

Privacy and the Internet of Things (IoT)

Leonie Huang, Esq.

Holland & Knight (Moderator)

Mark Melodia, Esq.

Partner, Holland & Knight

Jessica Lee, Esq.

Partner, Loeb & Loeb

Anthony Ford, Esq.

Senior Data Privacy Counsel, Medidata Solutions, Inc.

Manas Mohapatra, Esq.

Chief Privacy Officer at Viacom

The Internet of Things (“IoT”) – Background Information

Compiled by Leonie Huang, Holland & Knight

I. What is the IoT?

A. Where did the term come from?: Kevin Ashton is often credited with coining the term in 1999, while working as a brand manager at Procter & Gamble and working on early RFID technology. (Kevin Ashton is a cofounder of the Auto-ID Center at Massachusetts Institute of Technology, a precursor to the Auto-ID Lab at MIT— which is part of an independent network of seven academic research labs conducting research and development of new technologies with a goal of creating new consumer benefits and revolutionizing global commerce.)

1. Sources:

- a. Internet of things (IoT) History, Postscapes (Aug. 20, 2018), <https://www.postscapes.com/internet-of-things-history/> (“1999 - A big year for the IoT and MIT. The Internet of Things term is coined by Kevin Ashton executive director of the Auto-ID Center”).
- b. Kevin Ashton, “*That “Internet of Things” Thing*,” RFID Journal (June 22, 2009), available at <https://www.rfidjournal.com/articles/view?4986> (“I could be wrong, but I’m fairly sure the phrase “Internet of Things” started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999.”)
- c. Arik Gabbai, *Kevin Ashton Describes “the Internet of Things”*, Smithsonian Magazine (January 2015), available at <https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/#i6DUCkEK2jE8yH6V.99>
- d. Kevin Maney and Alison Maney, *Kevin Ashton, Father of the Internet of Things & Network Trailblazer*, Cisco - The Network (Dec. 8, 2014), available at <https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1558161> (“It all started with lipstick. A particularly popular color of Oil of Olay lipstick that Kevin Ashton had been pushing as a brand manager at Procter & Gamble was perpetually out of stock. He decided to find out why, and found holes in data about the supply chain that eventually led him to drive the early deployment of RFID chips on inventory. Asked by the Massachusetts Institute of Technology to start a group -- the Auto-ID Center -- that would research RFID technology, he found a way to talk about RFID to a less-than-computer-savvy crowd – by coining the phrase the Internet of Things or IoT.”).

- i. RFID: “Radio Frequency Identification is a technology that allows almost any object to be wirelessly identified using data transmitted via radio waves.” Suzanne Smiley, *What is RFID*, RFID Insider (Feb. 21, 2017), available at https://blog.atlasrfidstore.com/what-is-rfid?utm_source=Quick-Start&utm_medium=Link&utm_campaign=Content&utm_content=What-is-RFID

B. How do people define IoT?: There are many definitions and descriptions. Commenters say there is no generally or universally agreed definition. Here are some recent definitions excerpted from the source documents noted at the end of each excerpt:

1. “Internet of Things” (IoT) refers to networks of objects that communicate with other objects and with computers through the Internet. The objects that are not themselves computers but have embedded components that connect to the Internet.

- a. Things” may include virtually any object for which remote communication, data collection, or control might be useful, such as smart meters, fitness trackers, smart clothing, vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, or building systems.

- i. In other words, the IoT potentially includes huge numbers and kinds of interconnected objects.

- b. Two features makes objects part of the IoT—a unique identifier and Internet connectivity.

- i. Such “smart” objects each have a unique Internet Protocol (IP) address to identify the object sending and receiving information.

- ii. Smart objects can form systems that communicate among themselves, usually in concert with computers, allowing automated and remote control of many independent processes and potentially transforming them into integrated systems.

- c. Source: Eric A. Fischer, *The Internet of Things: Frequently Asked Questions*, Congressional Research Service Report (October 13, 2015), available at <https://crsreports.congress.gov/product/pdf/R/R44227>

2. Although there is no single, universal definition for IoT, the term generally refers to a network of ordinary objects that are embedded with Internet-connected electronics, sensors, or software that can capture, exchange, and receive data.

- a. These “things” include items sold to and used by consumers, as well as broader cloud-enabled machine-to-machine communications that enable businesses and organizations to track energy use, functionality, or efficiency.
- b. IoT technology enables the creation, transmission, communication, and analysis of data generated by embedded sensors.
- c. See Table ES-1 at page 2 for an overview of technologies facilitating IoT information exchange.
- d. Source: Federal Transit Administration, Report to Congress on Internet of Things, FTA Report No. 0099 (Feb. 2017), available at <https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/research-innovation/60436/ftareportno0099.pdf>

II. When did the IoT really take off?

A. According to Cisco Internet Business Solutions Group, there came a point in time (sometime between 2008 and 2009) when more things than people were connected to the internet, and the IoT was “born.”

Source: Dave Evans, *The Internet of Things, How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper 3 (April 2011), available at https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

B. More recently, with 5G wireless capability people are again talking about a takeoff of IoT.

Examples:

- Hatem Zeine, What The Future Of IoT And 5G May Look Like, Forbes.com (Nov. 1, 2018), available at <https://www.forbes.com/sites/forbestechcouncil/2018/11/01/what-the-future-of-iot-and-5g-may-look-like/#48341af0629b>
- Corrine Reichert, *CES 2019: Sprint pairs Curiosity IoT with 5G to power smart cities, autonomous vehicles*, ZDNet (Jan. 9, 2019), available at <https://www.zdnet.com/article/ces-2019-sprint-pairs-curiosity-iot-with-5g-to-power-smart-cities-autonomous-vehicles/>

III. How many things or devices are we talking about now?

A. Estimates vary widely, for example, ranging from 8.4 billion to 18 billion connected things in 2017 and projections of around 20 to 50 billion by 2020.

1. Sources:

- a. Cisco: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc529314172
- b. Ericsson: <https://www.ericsson.com/en/mobility-report/internet-of-things-forecast>
- c. Gartner: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>

IV. IoT in the News – For some recent headlines detailing public concern with privacy and security issues related to the IoT see these examples:

- Laura Hautala, *Blackberry Wants to Make the Internet of Things Safe for You*, CNet (Jan. 6, 2019), available at <https://www.cnet.com/news/blackberry-wants-to-make-the-internet-of-things-safe-for-you/>
- Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), available at <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>
- Farhad Manjoo, *A Future Where Everything Becomes a Computer Is as Creepy as You Feared*, N.Y. Times (Oct. 10, 2018), available at <https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html>
- Derek Hawkins, *The Cybersecurity 202: California's New Internet of Things Law Only Protects Against a Small Portion of Cyberthreats*, Washington Post (Oct. 8, 2018) available at https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/10/08/the-cybersecurity-202-california-s-new-internet-of-things-law-only-protects-against-a-small-portion-of-cyberthreats/5bba75781b326b7c8a8d1885/?utm_term=.5c55aec4735e
- Lily Hay Newman, *The Sensors that Power Smart Cities are Aa Hacker's Dream*, Wired (Aug. 9, 2018), available at <https://www.wired.com/story/sensor-hubs-smart-cities-vulnerabilities-hacks/>

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with
Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

The people of the State of California do enact as follows:

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. SECURITY OF CONNECTED DEVICES

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

- (1) Appropriate to the nature and function of the device.

- (2) Appropriate to the information it may collect, contain, or transmit.
- (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:

- (1) The preprogrammed password is unique to each device manufactured.
- (2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

1798.91.05. For the purposes of this title, the following terms have the following meanings:

(a) “Authentication” means a method of verifying the authority of a user, process, or device to access resources in an information system.

(b) “Connected device” means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.

(c) “Manufacturer” means the person who manufactures, or contracts with another person to manufacture on the person’s behalf, connected devices that are sold or offered for sale in California. For the purposes of this subdivision, a contract with another person to manufacture on the person’s behalf does not include a contract only to purchase a connected device, or only to purchase and brand a connected device.

(d) “Security feature” means a feature of a device designed to provide security for that device.

(e) “Unauthorized access, destruction, use, modification, or disclosure” means access, destruction, use, modification, or disclosure that is not authorized by the consumer.

1798.91.06. (a) This title shall not be construed to impose any duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications that a user chooses to add to a connected device.

(b) This title shall not be construed to impose any duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications, to review or enforce compliance with this title.

(c) This title shall not be construed to impose any duty upon the manufacturer of a connected device to prevent a user from having full control over a connected device, including the ability to modify the software or firmware running on the device at the user’s discretion.

(d) This title shall not apply to any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority.

(e) This title shall not be construed to provide a basis for a private right of action. The Attorney General, a city attorney, a county counsel, or a district attorney shall have the exclusive authority to enforce this title.

(f) The duties and obligations imposed by this title are cumulative with any other duties or obligations imposed under other law, and shall not be construed to relieve any party from any duties or obligations imposed under other law.

(g) This title shall not be construed to limit the authority of a law enforcement agency to obtain connected device information from a manufacturer as authorized by law or pursuant to an order of a court of competent jurisdiction.

(h) A covered entity, provider of health care, business associate, health care service plan, contractor, employer, or any other person subject to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) or the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) shall not be subject to this title with respect to any activity regulated by those acts.

(i) This title shall become operative on January 1, 2020.

SEC. 2. This act shall become operative only if Assembly Bill 1906 of the 2017–18 Regular Session is also enacted and becomes effective.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

BRIAN FLYNN, GEORGE BROWN,
KELLY BROWN, and MICHAEL
KEITH, *on behalf of themselves and all
others similarly situated,*

Plaintiffs,

vs.

FCA US LLC, and HARMAN
INTERNATIONAL INDUSTRIES, INC.,

Defendants.

Case No. 15-cv-855-MJR-DGW

MEMORANDUM & ORDER

REAGAN, Chief Judge:

Before the Court is a motion to dismiss for lack of personal jurisdiction (Doc. 407) filed by Defendant FCA US LLC on August 22, 2018. Defendant Harman International Industries, Inc. moved to join in the motion on August 24, 2018 (Doc. 408). Plaintiffs responded to the motion to dismiss on September 12, 2018 (Doc. 409), and FCA filed a reply on September 14, 2018. For good cause shown, the motion for joinder (Doc. 408) is **GRANTED**, and the Court considers the arguments in the motion to dismiss with respect to both Defendants.

BACKGROUND

On August 4, 2015, Plaintiffs Brian Flynn, Kelly and George Brown, and Michael Keith filed suit, on behalf of themselves and all others similarly situated, alleging a number of claims related to a design flaw in the uConnect system, which was manufactured by Harman and installed in certain 2013-2015 Chrysler vehicles. The

putative class action sought to certify both a nationwide class and state-based classes, including classes of Michigan consumers and of Missouri consumers. In September 2015, Defendants filed motions to dismiss for failure to state a claim and for lack of standing pursuant to Federal Rules of Civil Procedure 12(b)(6) and Rule 12(b)(1). (Docs. 23, 28). The motions were rendered moot by Plaintiffs' first amended complaint (Doc. 49), but new motions directed at that complaint were filed in February 2016. (Docs. 68, 71). The Court granted the motions in part and denied them in part in September 2016 (Doc. 115), withholding ruling on any arguments brought against the Browns' claims, as they were ordered to arbitrate certain warranty claims.

The Browns decided not to arbitrate, and their warranty claims were dismissed for failure to prosecute. (Doc. 149). Defendants then moved to dismiss the Browns' remaining claims, renewing challenges under Rules 12(b)(1) and 12(b)(6). (Docs. 152, 154, 158). The motions were granted in part and denied in part on August 21, 2017. (Doc. 236). The Court directed Plaintiffs to file a second amended complaint, which Defendants moved to dismiss. (Docs. 249, 254).

In October 2017 and January 2018, Defendants filed seven motions for summary judgment (Docs. 256, 257, 264, 267, 346, 348, 350). Both Harman and FCA filed lengthy oppositions to Plaintiffs' motion to certify class (Docs. 318, 321) and argued against class certification during a January 11, 2018 hearing on Plaintiffs' motion. At the hearing, Defendants also renewed their standing challenge. Following briefing on the renewed challenge, the Court found that Plaintiffs have standing to pursue their claims. Defendants moved the Court to certify the order denying their standing challenge for

interlocutory appeal. The request was granted, and Defendants filed a petition for leave to appeal with the Seventh Circuit Court of Appeals. The Seventh Circuit denied the petition on May 4, 2018. On July 5, 2018, the Court granted in part and denied in part the seven motions for summary judgment and Plaintiffs' motion to certify class. (Doc. 399). Three classes were certified: an Illinois class, a Michigan class, and a Missouri class.

At no point prior to class certification did Defendants challenge, or suggest that they might challenge, the exercise of personal jurisdiction over them. Instead, they raised the issue for the first time in the petition for leave to appeal the class certification order filed with the Seventh Circuit Court of Appeals in July 2018. The Seventh Circuit denied the petition for leave to appeal the class certification order, and Defendants now raise their objection to personal jurisdiction before this Court. For the reasons delineated below, the Court **FINDS** that Defendants waived any objection to personal jurisdiction, and the motion to dismiss for lack of jurisdiction is **DENIED**.

ANALYSIS

A defense based on personal jurisdiction "may be waived if a defendant gives a plaintiff a reasonable expectation that he will defend the suit on the merits or where he causes the court to go to some effort that would be wasted if personal jurisdiction is subsequently found lacking." *Hedeen Intern., LLC v. Zing Toys, Inc.*, 811 F.3d 904, 906 (7th Cir. 2016). Here, the parties have litigated this case fervently for more than three years, and Defendants seemingly acknowledge that the defense is waived as to the named Missouri and Michigan class representatives, Kelly and George Brown and

Michael Keith, by arguing their motion as to the unnamed class members only.. *See Continental Bank, N.A. v. Meyer*, 10 F.3d 1293, 1296-97 (7th Cir. 1993)(**finding personal jurisdiction defense waived where defendants fully participated in litigation for over two and a half years**). Defendants gave Plaintiffs a reasonable expectation that they would defend this action on the merits by failing to object to personal jurisdiction until after the class certification stage. They also caused the Court to go to some effort that would be wasted if personal jurisdiction now is found to be lacking by pursuing several rounds of motions to dismiss and standing challenges in addition to significant briefing related to summary judgment and class certification before raising the objection.

Defendants attempt to skirt past the waiver issue with an argument that unnamed class members were not parties to the litigation prior to the order certifying classes in this case, suggesting that they could not have challenged personal jurisdiction any earlier than they did. As a preliminary note, the party-status of unnamed class members is not as clear cut as Defendants state it is. *See e.g., Smith v. Bayer Corp.*, 564 U.S. 299, 313 (2011)(**noting that unnamed members of a proposed but uncertified class are not parties when considering preclusion and relitigation exception to Anti-Injunction Act**); *Pearson v. Target Corp.*, 893 F.3d 980, 984 (7th Cir. 2018)(**acknowledging that “party” does not indicate an absolute characteristic, as absent class members may be parties for some, but not all, purposes**). When it comes to the question of whether Defendants waived their objection to the exercise of personal jurisdiction with respect to the certified Michigan and Missouri classes, the issue of party-status and the recentness of the addition of unnamed class members to this action

is not determinative. Instead, the question of waiver is weighed against the entire course of this litigation, not just with respect to post-certification events.

Defendants' argument that they had to await a ruling on class certification before raising a challenge to personal jurisdiction relies on cases considering the issue at or before the class certification stage. In *Biffar v. Pinnacle Foods*, Judge Herndon denied a motion to dismiss for lack of personal jurisdiction over non-Illinois putative class members as premature, noting that the issues should be addressed "at the class certification stage." *Biffar v. Pinnacle Foods*, 2016 WL 7429130, *6 (S.D. Ill. 2016)(Herndon, J.). Defendants draw from that comment that the issue cannot be raised until after a ruling on class certification, which is plainly different than the language in the order. Defendants also cite to class certification order in *Practice Mgmt. Support Servs., Inc. v. Cirque du Soleil*, 301 F.Supp.3d 840, 861-64 (N.D. Ill. 2018)(Durkin, J.), which considered the issue of personal jurisdiction simultaneously with the issue of class certification. Unlike this case, the objection to personal jurisdiction was raised and briefed prior to the ruling on class certification. Defendants cite no cases directly in support of their contention that they had to wait until after class certification to raise personal jurisdiction challenges, and the undersigned finds that they now raise their objection too late.

Litigation of this action has progressed past the class certification stage without any hint of a challenge to personal jurisdiction prior to certification of classes with out-of-state plaintiffs, and the Court is not persuaded by Defendants' suggestion that their delay in raising the issue does not waive their ability to raise the challenge post-

certification. By proceeding through several motions to dismiss, seven motions for summary judgment, and a vigorous defense to class certification without mention of personal jurisdiction, Defendants gave Plaintiffs a reasonable impression that they would defend this suit on the merits. They have fully participated in this action for over three years and have caused the Court to expend more than “some effort” that would be wasted by a finding at this stage that personal jurisdiction is lacking. Accordingly, the Court **FINDS** that Defendants waived any objection to the exercise of personal jurisdiction as to all out-of-state plaintiffs, including the unnamed class members.

CONCLUSION

For the above-stated reasons, Defendant Harman International Industries, Inc.’s motion for joinder (Doc. 408) is **GRANTED** and Defendants’ motion to dismiss for lack of jurisdiction (Doc. 407) is **DENIED**.

On July 23, 2018, the Court exercised its discretionary powers and stayed this action in its entirety. The Court hereby **LIFTS the STAY** and sets this case for trial at 9:00 a.m. on Monday, March 11, 2019. A final pretrial conference is set for 10:00 a.m. on Thursday, March 7, 2019.

The parties shall confer regarding class notice and shall file a status report (not to exceed 6 pages) with their joint proposal or competing proposals for notice on or before October 19, 2018.

IT IS SO ORDERED.

DATED: October 9, 2018

s/ Michael J. Reagan
MICHAEL J. REAGAN
United States District Judge

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET AND TECHNOLOGY

In the Matter of

Assurance No. 17-056

**Investigation by ERIC T. SCHNEIDERMAN,
Attorney General of the State of New York, of**

**SAFETECH PRODUCTS, LLC, and RYAN HYDE, as an
individual,**

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("NYAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") §§ 349 and 350 into the security of Safetech Products LLC, and its owner Ryan Hyde ("Respondents"), Bluetooth-enabled locks. This Assurance of Discontinuance ("Assurance") contains the findings of the NYAG's investigation and the relief agreed to by NYAG and Respondents.

FINDINGS OF NYAG

1. Safetech Products, LLC ("Safetech") is a limited liability corporation with a principal place of business at 1601 North State Street, Lehi, Utah. It is owned by Ryan Hyde.
2. Safetech sells Bluetooth-enabled locks to customers through its website <https://www.thequicklock.com/> with the promise "Privacy When You Want It, Security When You Need It." With Bluetooth-enabled locks, the user may control the locks with an application ("app") installed on a smartphone.
3. Bluetooth is a wireless technology standard for exchanging data over short distances of up to 300 feet. It uses short-wavelength UHF radio waves in the ISM band from 2.4

to 2.485 GHz. To operate the Bluetooth-enabled lock, the smartphone and the lock must have their Bluetooth antennas turned on at the same frequency band and broadcast their identifiers to each other. A default password is used to secure the connection and exchange data.

4. In August 2016, independent security researchers reported that Respondents' Bluetooth-enabled locks transmitted passwords between the locks and the user's smartphone in plain text and without encryption. The researchers reported that a wrong-doer could intercept the passwords and proceed to unlock the locks. The researchers also reported that the locks contained weak default passwords that were not secure and could be guessed or discovered through brute force attacks (i.e., automated software used to generate a large number of consecutive guesses).

5. In October 2016, the NYAG contacted Respondents about the findings of the researchers and the security of the locks. Just prior to being contacted by the NYAG, Respondents voluntarily placed the following warning on the <https://www.thequicklock.com/> website:

SECURITY WARNING...Bluetooth keys for the hardware are passed
"unencrypted" on all current products.

We also strongly recommend the default password be changed at initial
setup. Please read "Security Risks Explained."

Upon clicking the "Security Risks Explained" hyperlink, the user is taken to a webpage that explains the risks identified above.

6. Respondents' locks limited the Bluetooth range to approximately 50 feet. Thus, a wrongdoer would need to be in close proximity to the lock to intercept the Bluetooth passwords. Additionally, the locks shutdown for 2 minutes with two failed password attempts. Thus, a brute force attack would be limited by the locks 2-minute lock-out feature.

7. By violating express and implied representations of reasonable data security, Respondents violated New York Executive Law § 63(12) and New York General Business Law §§ 349 and 350.

PROSPECTIVE RELIEF

WHEREAS, Respondents admit NYAG Findings (1)-(6) above;

WHEREAS, NYAG is willing to accept the terms of this Assurance pursuant to Executive Law § 63(15) and to discontinue its investigation into Respondents' representations concerning the security of its Bluetooth-enabled locks; and

WHEREAS, the parties each believe that the obligations imposed by this Assurance are prudent and appropriate;

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the parties, that:

8. This Assurance shall apply to Respondent Safetech Products LLC, and any officers, directors, servants, agents, employees, assignees, and any individual, subsidiary, division, or other entity through which the company may now or hereafter act, as well as any successors-in-interest, and Ryan Hyde, as an individual.

9. Respondents shall comply with Executive Law § 63(12), and GBL §§ 349 and 350, and shall not misrepresent, expressly or by implication, the security of its locks, or the security, confidentiality, or integrity of any data these devices transmit via Bluetooth or other radio frequencies.

10. Respondents shall encrypt all passwords, electronic keys or other credentials ("Security Information") in their locks and other Bluetooth-enabled devices that Respondents market or sell to individual consumers and the general public. Respondents' Bluetooth-enabled

devices shall prompt users to change the default password upon the customer's initial setup of wireless communication.

11. Within 30 days of the execution of this Assurance, Respondents shall establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing devices that use Security Information, and (2) protect the privacy, security, confidentiality, and integrity of Security Information. Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards appropriate to company's size and complexity, the nature and scope of the company's activities, and the sensitivity of the device's function or the information it collects, transmits or processes, including:

- a. The designation of an employee or employees to coordinate and be accountable for the security program;
- b. The identification of material internal and external risks to (1) the security of the devices that could result in unauthorized access to or unauthorized modification of the device and (2) the privacy, security, confidentiality, and integrity of Security Information;
- c. The risk assessments required by subpart b must include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing; (4) review, assessment, and response to third party security vulnerability

reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

- d. The design and implementation of reasonable safeguards to control the risks identified through risk assessment;
- e. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures including reasonable and appropriate security testing techniques such as vulnerability and penetration testing, security architecture reviews and code reviews;
- f. The development and use of reasonable steps to select and retain service providers (if any are hired) capable of maintaining security practices consistent with this Assurance, and requiring service providers by contract to implement and maintain appropriate safeguards consistent with this Assurance; and
- g. The evaluation and adjustment of Respondents' security program in light of the results of the testing and monitoring required by subpart e, any material changes to Respondents' operations or business arrangements, or any other circumstances that Respondents' knows or has reason to know may have a material impact on the effectiveness of the security program.

12. Respondents shall, within 10 business days of receiving a written request from NYAG, make available for NYAG review a copy of Respondents' written policies and procedures adopted pursuant to this Assurance or otherwise.

Miscellaneous

13. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondents and its counsel and NYAG's own factual

investigation as set forth in Findings (1)-(6) above. To the extent that any of Respondents' representations are later found to be inaccurate or misleading, this Assurance is voidable by the NYAG in its sole discretion.

14. If the Assurance is voided or breached, Respondents agree that any statute of limitations or other time-related defenses applicable to the subject of the Assurance and any claims arising from or relating thereto are tolled from and after the date of this Assurance. In the event the Assurance is voided or breached, Respondents expressly agree and acknowledge that this Assurance shall in no way bar or otherwise preclude NYAG from commencing, conducting or prosecuting any investigation, action or proceeding, however denominated, related to the Assurance, against the Respondents, or from using in any way any statements, documents or other materials produced or provided by Respondents prior to or after the date of this Assurance.

15. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondents in agreeing to this Assurance.

16. Respondents represent and warrant, through the signatures below, that the terms and conditions of this Assurance are duly approved, and execution of this Assurance is duly authorized. Respondents shall not take any action or make any statement denying, directly or indirectly, the propriety of this Assurance or expressing the view that this Assurance is without factual basis. Nothing in this paragraph affects Respondents' (i) testimonial obligations or (ii) right to take legal or factual positions in defense of litigation or other legal proceedings to which NYAG is not a party. This Assurance may not be used and is not intended for use by any third party in any other proceeding.

17. This Assurance may not be amended except by an instrument in writing signed on

behalf of all the parties to this Assurance.

18. This Assurance shall be binding on and inure to the benefit of the parties to this Assurance and their respective successors and assigns, provided that no party, other than NYAG, may assign, delegate, or otherwise transfer any of his rights or obligations under this Assurance without the prior written consent of NYAG.

19. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the NYAG such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

20. To the extent not already provided under this Assurance, Respondents shall, upon request by NYAG, provide documentation and information necessary for NYAG to verify compliance with this Assurance.

21. All notices, reports, requests, and other communications to any party pursuant to this Assurance shall be in writing and shall be directed as follows:

If to Respondents:

SafeTech Products, LLC
TheQuickLock LLC
1601 North State Street]
Lehi, Utah 84043

If to the NYAG, to:

Attorney General of the State of New York
120 Broadway
New York, New York 10271
Attention: Chief, Bureau of Internet and Technology

22. Acceptance of this Assurance by NYAG shall not be deemed approval by NYAG of any of the practices or procedures referenced herein, and Respondents shall make no

representation to the contrary.

23. Pursuant to Executive Law § 63(15), evidence of a violation of this Assurance shall constitute *prima facie* proof of violation of the applicable law in any action or proceeding thereafter commenced by NYAG.

24. If a court of competent jurisdiction determines that Respondents have breached this Assurance, Respondents shall pay to NYAG the cost, if any, of such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

25. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. The NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding.

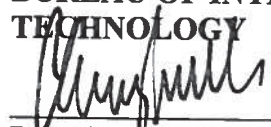
26. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

27. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

28. This Assurance may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

**ERIC T. SCHNEIDERMAN
NEW YORK ATTORNEY GENERAL
BUREAU OF INTERNET AND
TECHNOLOGY**


By: Clark Russell
Deputy Bureau Chief

5/9/17
Date

**SAFETECH PRODUCTS LLC AND RYAN
HYDE**


By:

May 3, 2017
Date

New York Attorney General's Office
120 Broadway
New York, NY 10271-0332
Phone: (212) 416-8433
Fax: (212) 416-8369

Privacy and the Internet of Things (IoT)

NYSBA IP Section / January 15, 2019 Annual Meeting

Mark S. Melodia, Partner, NY / Mark H. Francis, Partner, NY

1. UNDERSTANDING THE RISKS

- a. Data privacy risks typically stem from two key issues:
 - i. Data misuse such as the unauthorized collection and use an individual's personal information; and
 - ii. Data breach that compromises an individual's personal information due to insufficient security measures.
- b. "Internet of Things" ("IoT") devices present a bigger challenge than traditional systems such as computers for a number of reasons, for example:
 - i. Poor software patching practices by manufacturers and users result in IoT vulnerabilities being common and easily exploited;
 - ii. Manufacturers may not provide long-term support for IoT devices (*e.g.*, beyond 1-3 years) while they may be in use for much longer periods;
 - iii. Many IoT devices incorporate open source software that is not properly understood or secured when adopted by manufacturers (*e.g.*, Linux O/S); and
 - iv. Manufacturers compete on price for low-cost IoT devices and security is not a significant consideration in product development.
- c. IoT devices therefore present a number of heightened security risks, such as:
 - i. Enabling unauthorized access and misuse of users' sensitive personal information maintained or accessible by the IoT device;
 - ii. Facilitating attacks on other systems, such as (1) using a compromised IoT device to move laterally to other systems on the network, or (2) using thousands of compromised IoT devices and to facilitate botnet attacks; and
 - iii. Creating safety risks and potentially physical harm, such as damaging medical devices (insulin pumps, pacemakers), or taking over vehicle controls.

- d. IoT devices also collect more sensitive personal information that traditional computers in many respects—for example, they may have access to precise geolocation data, detailed health information (e.g., fitness trackers) and highly-personal audio and video feeds.

2. REGULATORY GUIDANCE

- a. U.S. Department of Homeland Security (“DHS”) issued the *Strategic Principles For Securing The Internet Of Things (IoT)* on November 15, 2016,¹ promoting six key practices:
 - i. Incorporate security at the design phase;
 - ii. Advance security updates and vulnerability management;
 - iii. Build on proven security practices;
 - iv. Prioritize security measures according to potential impact;
 - v. Promote transparency across IoT; and
 - vi. Connect carefully and deliberately.
- b. Federal Trade Commission (“FTC”) Staff Report *internet of things: Privacy & Security in a Connected World* released in January 2015² focused on three areas: data security, data minimization, and consumer notice and choice.
- c. Also in January 2015, the FTC also released a short summary on IoT Security entitled *Careful Connections: Building Security in the Internet of Things*,³ promoting adoption of many security concepts for IoT including a culture of security, security by design, defense-in-depth, risk-based approaches and avoidance of default passwords.

¹ <https://www.dhs.gov/securingtheIoT>.

² <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

³ <https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things>.

- d. The National Institute of Standards and Technology (“NIST”) has been a leading influencer in cybersecurity standards and best practices, most notably the *NIST Cybersecurity Framework*⁴
- e. In November 2018, NIST published an *Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)*⁵ to inform and support policymakers, businesses, and other interested participants on development and use of cybersecurity standards for IoT components, systems, and related services. The report focuses on five IoT areas: connected vehicles, consumer devices, health devices, smart buildings and smart manufacturing.

3. APPLICABLE LAWS (EXEMPLARY)

- a. FTC Authority and Oversight
 - i. The FTC’s enforcement authority is derived from over 70 different statutes, including the Federal Trade Commission Act.⁶ Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (“Section 5”), authorizes the FTC to bring actions—in both judicial and administrative forums—against entities engaging in “unfair or deceptive acts or practices in or affecting commerce.”⁷
 - ii. The FTC interprets its Section 5 authority as allowing it to regulate—and to bring enforcement actions related to—allegedly unfair or deceptive acts or practices in the data privacy and security arena. The FTC has become the leading federal regulatory authority on privacy and security, and has brought many cases against companies allegedly engaged in unfair or deceptive practices that put consumers’ personal data at unreasonable risk.
 - iii. An August 24, 2015 decision by the Third Circuit Court of Appeals in *FTC v. Wyndham Worldwide Corporation*⁸ recognized—for the first time by a U.S.

⁴ <https://www.nist.gov/cyberframework>.

⁵ <https://doi.org/10.6028/NIST.IR.8200>.

⁶ 15 U.S.C. §§ 41-58.

⁷ See generally *In the Matter of CardSystems Solutions, Inc. et al.*, FTC Dkt. No. C-4168 (Sept. 5, 2006) (complaint); *In the Matter of DSW, Inc.*, FTC Dkt. No. C-4157 (Mar. 7, 2006) (complaint); *United States v. ChoicePoint, Inc.*, No. 106-cv-0198, Dkt. No. 5 (N.D. Ga. Feb. 15, 2006) (stipulated judgment); *In the Matter of BJ’s Wholesale Club, Inc.*, FTC Dkt. No. C-4148 (Sept. 20, 2005) (complaint).

⁸ *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

appellate court—that the FTC has authority to regulate “unfair” or “deceptive” cybersecurity practices under Section 5.

- iv. On June 6, 2018, the Eleventh Circuit in *LabMD, Inc. v. Federal Trade Commission* vacated a cease and desist order by the FTC Commission directing LabMD to create and implement a variety of protective measures.⁹ The Court did not question the FTC’s authority under Section 5 to oversee cybersecurity and privacy practices, but it challenged the FTC’s practice of demanding that defendants institute “reasonable” security practices, and found that such orders must “enjoin a specific act or practice.”
- v. The FTC also has specific enforcement authority for data privacy under statutes such as COPPA, FCRA, HITECH (breach notice). In June 2017, the FTC updated its COPPA Guidance to explicitly note that the statutes reference to “[w]ebsite or online service” includes “connected toys or other Internet of Things devices.”¹⁰

b. U.S. Consumer Product Safety Commission (“CPSC”)

- i. The CPSC held a hearing in May 2018 on IoT product safety, but focused on risks of physical injury rather than data privacy.¹¹ The hearing followed a 2017 staff report on the safety risks associated with many new technologies, including IoT.¹²

c. State laws

- i. Consumer Protection: States have broad consumer protection statutes, typically in the form of Unfair and Deceptive Trade Practices Acts (“UDTPAs”). These laws are often modeled after Section 5(a) of the FTC Act, prohibiting trade practices that are “unfair” or “deceptive.” Like the FTC, state attorneys general (“AGs”) leverage these laws to pursue companies

⁹ *LabMD, Inc. v. Federal Trade Commission*, 894 F.3d 1221 (11th Cir. 2018).

¹⁰ FTC, *Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* (June 2017), <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>.

¹¹ CPSC, *The Internet of Things and Consumer Products Hazards*, 83 Fed. Reg. 13122 (Mar. 27, 2018).

¹² CPSC, Staff Report, *Potential Hazards Associated with Emerging and Future Technologies* (Jan. 19, 2017), <https://www.cpsc.gov/content/potential-hazards-associated-with-emerging-and-future-technologies>.

for unsatisfactory data privacy and security practices, frequently after a reported data incident. UDTPAs can provide a variety of remedies to state attorneys general such as injunctions, restitution, and civil penalties. Similarly, civil penalties can range up to \$50,000 per violation.¹³ Some jurisdictions have held that a civil penalty may be imposed *for each individual violation* of a consumer protection statute.¹⁴ In addition, at least 26 states and the District of Columbia permit an individual to bring a private right of action to recover damages or obtain equitable relief from businesses for injuries from a cyber-incident, for failure to notify customers of a breach in a timely manner, or under state consumer protection statutes such as UDTPAs.¹⁵ In some cases, prevailing plaintiffs are permitted to recover reasonable attorney's fees and court costs.

- ii. Data privacy: As of January 1, 2020, the California Consumer Privacy Act of 2018 ("CCPA") will create at least four core individual rights for consumers: (1) the right to know what PII is collected, sold, and disclosed (and to whom); (2) the right to opt-out of the sale of PII; (3) the right to deletion of PII; (4) and the right not to be discriminated against for exercising such rights. *It is unclear whether an employee will be deemed a "consumer" under the law*, but for now the statute is understood to include it. The CCPA is being viewed as "GDPR-lite" and adopts many of its concepts, including a broad definition of what constitutes PII. The CCPA is likely to undergo further revisions before 2020 and the California AG's office will be promulgating rules under the CCPA. Other states are expected to follow suit, and Congress is gearing up for a federal privacy law, but it remains unclear what that law will look like and to what extent it will preempt state laws.

¹³ See Cal. Bus. & Prof. Code § 17206(a) (California Attorney General may seek civil penalty not to exceed \$2,500 "for each violation"); 815 Ill. Comp. Stat. 505/7 (Illinois Attorney General can seek civil penalty not to exceed \$50,000.00 "against any person found to have engaged in any method, act or practice declared unlawful under this Act" when taken "with the intent to defraud."); Me. Rev. Stat. tit. 5, § 209 (Maine Attorney General can seek civil penalty of not more than \$10,000 for "each intentional violation"); Vt. Stat. Ann. tit. 9, § 2458(b)(1) (Vermont Attorney General may seek a civil penalty of not more than \$10,000 "for each violation").

¹⁴ See *McGraw v. Imperial Mktg.*, 203 W. Va. 203, 219 n.6 (W.Va. Sup. Ct. 1998) (Starcher, J. concurring) (listing various state imposed penalties).

¹⁵ For example, Florida and North Carolina, among others, have UDPTAs with private causes of action. See Fla. Stat. Ann. §§ 501.203, 501.211; N.C. Gen. Stat. § 75-1.1; see also *In re: Target Corp. Customer Data Security Breach Litig.*, 66 F.Supp.3d 1154 (D. Minn. Dec. 18, 2014) (addressing a number of state UDTPAs asserted in a class action stemming from a data breach).

- iii. *IoT laws*: On September 28, 2018, California’s governor signed into law the nation’s first IoT bill.¹⁶ The law will go into effect on January 1, 2020 and requires that manufacturers implement “reasonable security features” in IoT devices sold in California. The law provides certain specific requirements, such as rules for password and user authentication, its broad obligation for reasonable security presents some ambiguity for manufacturers, similar to the issues that manufacturers have complained about with respect to the FTC’s enforcement of alleged Section 5 violations for unreasonable practices. Notably, the This law does not provide a private right of action and vests exclusive authority to enforce the law with the state’s Attorney General and city/county prosecutors.

4. IoT ENFORCEMENT AND LEGAL ACTION (EXEMPLARY)

a. Regulatory Enforcement

i. FTC Activities

1. *TRENDnet and ASUSTeK*: The FTC has brought a number of enforcement actions for perceived failures to properly secure IoT devices. For example, it brought actions against a manufacturer of baby cameras in 2013¹⁷ and a router manufacturer in 2016. The agency resolved both actions through consent orders that required the businesses to (i) establish security programs designed to provide consumers with secure devices; (ii) conduct security audits for 20 years; and (iii) provide audit reports to the FTC upon request.¹⁸
2. *VTech*: In January 2018 the FTC brought an enforcement actions against Vtech for a connected toy app alleged to have collected children’s personal information without parental consent, in violation of COPPA and FTC Act—the parties entered into a stipulated order under which Vtech paid \$650,000 and agreed to a number of data privacy and security compliance and reporting obligations.¹⁹

¹⁶ Senate Bill 327; Assembly Bill 1906.

¹⁷ *In the Matter of TRENDnet INC.*, FTC Dkt. No. C-4426, Decision and Order (Jan. 16, 2014).

¹⁸ *In the Matter of ASUSTeK Computer Inc.*, FTC Dkt. No. C-4587, Decision and Order (July 18, 2016).

¹⁹ *USA v. Vtech Elec. Ltd. et al.*, No. 1:18-cv-114 (N.D. Ill. Jan. 8, 2018)

3. Vizio: On February 6, 2017, the FTC announced that Vizio would pay \$2.2 million to the FTC and State of New Jersey to settle charges it collected viewing histories on 11 million smart televisions without users' consent. The stipulated consent order also required Vizio to provide clear representations about its privacy practices, obtain affirmative consent for its data collection and sharing practices, delete data collected before March 1, 2016, and implement a comprehensive data privacy program with biennial assessments.²⁰
4. D-Link: In January 2017, the FTC sued D-Link under Section 5 for alleged failures to reasonably secure its routers and web cameras from widely known and reasonably foreseeable security risks. The Court dismissed some but not all of the FTC's claims on September 19, 2017 following D-Link's motion to dismiss. On September 21, 2018, the FTC and D-Link Systems Inc. each filed a motion for summary judgement.²¹ The dispute, which dates back to early 2017, concerns alleged may have widespread implications on companies' potential liability for lax security practices, even in the absence of actual consumer harm..

ii. State AGs

1. Safetech: On May 22, 2017, the New York Attorney General announced a settlement with Safetech over allegations that it sold insecure IoT door locks and padlocks. According to the agreement, Safetech would have to encrypt all passwords and other credentials in their IoT devices, prompt users to change default passwords upon setup, and implement a written comprehensive security program to address security in the products. At the time the NY AG noted it was the first AG enforcement action against a company for poor IoT security practices.²²

²⁰ *FTC. v. Vizio, Inc. et al.*, No. 2:17-cv-00758, Stipulated Order For Permanent Injunction and Monetary Judgment (D. N.J. Feb. 6, 2017); Press Release, VIZIO to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent (Feb. 6, 2017), <https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it>.

²¹ *FTC v. D-Link Systems Inc.*, No. 3:17-cv-00039 (N.D. Cal.)

²² Press Release, A.G. Schneiderman Announces Settlement With Tech Company Over Sale Of Insecure Bluetooth Door And Padlocks (May 22, 2017), <https://ag.ny.gov/press-release/ag->

5. CIVIL CASES AND CLASS ACTIONS

- i. *Kyle Zak et al v. Bose Corp.*: Class action filed against Bose on April 18, 2017 alleging its products collect users' music and audio selections and disclose it to a third party data miner for analysis. Bose's motion to dismiss is pending.²³
- ii. *P. v. Standard Innovation (US), Corp.*: In early 2017, a manufacturer of mobile app-controlled vibrator devices agreed to pay \$3.75 million to settle a privacy class action alleging that its devices secretly collected intimate information from users such as when and on what settings the device was used.²⁴ Standard also agreed to stop collecting the information and destroy the data it already collected.
- iii. *Ross v St Jude Medical Inc.*: One day after an infamous report from Muddy Water Capital was released with alleged "security vulnerabilities" in St Jude cardiac devices, a patient filed a class action based on the allegations.²⁵ The case was subsequently dropped by the plaintiff.
- iv. *ADT cases*: In 2014, home security company ADT was sued for allegedly insecure security systems that could be hacked and allow third parties to disable security features or "use customers' own security cameras to unknowingly spy on them."²⁶ The plaintiff alleged that his system was hacked at least twice. Rather than allege specific harm, the allegations focused on ADT's marketing statements and asserted claims for fraud, strict product liability and unjust enrichment. After lengthy discovery, various

[schneiderman-announces-settlement-tech-company-over-sale-insecure-bluetooth-door](#); *In the Matter of Investigation of Safetech Products, LLC et al.*, Assurance No. 17-056, Attorney General of the State of New York (May 9, 2017).

²³ *Kyle Zak et al v. Bose Corp.*, No. 1:17-cv-02928, Class Action Complaint (N.D. Ill. Apr. 18, 2017).

²⁴ *P. v. Standard Innovation (US), Corp.*, No. 1:16-cv-08655, DKt. 27, Plaintiffs' Motion For And Memorandum In Support Of Preliminary Approval Of Class Action Settlement (N.D. Ill. Mar. 9, 2017).

²⁵ *Ross v St Jude Medical Inc.*, No 2:16- cv-06465 (CD Cal 2016).

²⁶ *Baker v. The ADT Corporation et al.*, No. 2:15-cv-02038 (C.D. Ill.).

parties agreed to a nationwide settlement under which ADT would pay \$16 million for class counsel legal fees and customer awards of \$15 to \$45.²⁷

- v. *In re Vizio*: Concurrent with resolution of the FTC and state AG investigations concerning data-tracking software installed on Vizio smart TVs, on October 4, 2018 Vizio filed a motion for approval to settle the consumer class actions consolidated California federal court for \$17 million. Vizio also agreed to revise on-screen disclosures concerning its viewing data practices.²⁸
- vi. *Flynn v FCA US LLC*: Although more of a cybersecurity case than a privacy case, a federal court recently held that a class action case filed in 2015 and alleging that Fiat Chrysler designed and installed defective “Uconnect” infotainment systems that could be hacked and remotely controlled would proceed to trial.²⁹

6. IOT IN OTHER LEGAL CONTEXTS

- a. *Witness to murder?* On November 5, 2018, a court in New Hampshire ordered Amazon to produce two days of recordings from an Amazon Echo device suspected of capturing audio at the time a double murder occurred in the location.³⁰
- b. *Pacemaker subverts insurance fraud*: Police questioning an individual about a fire that caused about \$400,000 in damages at his home were told that when he

²⁷ *Edenborough et al. v. ADT, LLC et al.*, No. 3:16-cv-02233, Dkt. 94, Plaintiffs’ Notice Of Motion, Unopposed Motion, And Memorandum In Support Of Preliminary Approval Of Class Action Settlement (N.D. Cal. Mar. 23, 2017).

²⁸ *In Re: Vizio, Inc., Consumer Privacy Litigation*, No. 8:16-ml-02693, Dkt. 282-1 (C.D. Cal. Oct. 4, 2018).

²⁹ *Flynn v FCA US LLC*, No. 3:15-cv-00855, Dkt. 411, Memorandum & Order (S.D. Ill. Oct. 9, 2018). The Court previously found there existed a genuine dispute as to whether the class vehicles had defects, whether the alleged defects were remedied by the recall and whether additional measures were required to protect the vehicles from an unreasonable risk of hacking. Specifically, the plaintiffs’ warranty and fraudulent misrepresentation claims survived a summary judgment motion, and the Court granted class certification but limited it to the named plaintiffs’ states (Michigan, Illinois and Missouri). Another car hacking case filed around the same time was dismissed by the Court. *See Cahen v. Toyota Motor Corp.*, 3:15-cv-01104 (N.D. Cal. March 10, 2015).

³⁰ *State of New Hampshire v. Verrill*, No. 219-2017-cr-072, Order on Motion to Search in Lieu of Search Warrant (Sup. Ct. Nov. 5, 2018).

discovered the fire he gathered belongings, put them in various bags, broke out a bedroom window with his cane, threw his bags outside, and rushed out of the house. But when the police reviewed data from the 59-year old's pacemaker, it showed that his heart rate barely changed during the fire. After a cardiologist testified that the man's story was "highly improbable" under the circumstances he was charged with arson and insurance fraud.³¹

³¹ Journal News, *Data from man's pacemaker led to arson charges* (Jan 27, 2017), <https://www.journal-news.com/news/data-from-man-pacemaker-led-arson-charges/sDp2XXGPY1EKJkY57sureP/>; WLWT-TV, *Ross Compton indicted on charges of arson, insurance fraud* (Jan. 27, 2017), <https://www.wlwt.com/article/middletown-mans-electronic-heart-monitor-leads-to-his-arrest/8647942>.

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0

November 15, 2016



Homeland
Security

INTRODUCTION AND OVERVIEW

The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT)¹ creates immense opportunities and benefits for our society. IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks. This document explains these risks and provides a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate.

Growth and Prevalence of the Internet of Things

Internet-connected devices enable seamless connections among people, networks, and physical services. These connections afford efficiencies, novel uses, and customized experiences that are attractive to both manufacturers and consumers. Network-connected devices are already becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to our homes. The promise offered by IoT is almost without limit.

Prioritizing IoT Security

While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

The IoT ecosystem introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure.

Last year, in a cyber attack that temporarily disabled the power grid in parts of Ukraine, the world saw the critical consequences that can result from failures in connected systems. Because our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, IoT security is now a matter of homeland security.

¹ In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

It is imperative that government and industry work together, quickly, to ensure the IoT ecosystem is built on a foundation that is trustworthy and secure. In 2014, the President's National Security Telecommunications Advisory Committee (NSTAC) highlighted the need for urgent action.

IoT adoption will increase in both speed and scope, and [will] impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally.... there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.²

The time to address IoT security is right now. This document sets the stage for engagement with the public and private sectors on these key issues. It is a first step to motivate and frame conversations about positive measures for IoT security among IoT developers, manufacturers, service providers, and the users who purchase and deploy the devices, services, and systems. The following principles and suggested practices provide a strategic focus on security and enhance the trust framework that underpins the IoT ecosystem.

Overview of Strategic Principles

Many of the vulnerabilities in IoT could be mitigated through recognized security best practices, but too many products today do not incorporate even basic security measures. There are many contributing factors to this security shortfall. One is that it can be unclear who is responsible for security decisions in a world in which one company may design a device, another supplies component software, another operates the network in which the device is embedded, and another deploys the device. This challenge is magnified by a lack of comprehensive, widely-adopted international norms and standards for IoT security. Other contributing factors include a lack of incentives for developers to adequately secure products, since they do not necessarily bear the costs of failing to do so, and uneven awareness of how to evaluate the security features of competing options.

The following principles, set forth in the next section, offer stakeholders a way to organize their thinking about how to address these IoT security challenges:

Incorporate Security at the Design Phase

Advance Security Updates and Vulnerability Management

Build on Proven Security Practices

² National Security Telecommunications Advisory Committee Report to the President on the Internet of Things, November 19, 2014.

Prioritize Security Measures According to Potential Impact

Promote Transparency across IoT

Connect Carefully and Deliberately

As with all cybersecurity efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector. Companies and consumers are generally responsible for making their own decisions about the security features of the products they make or buy. The role of government, outside of certain specific regulatory contexts and law enforcement activities, is to provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security.

Scope, Purpose, and Audience

The purpose of these non-binding principles is to equip stakeholders with suggested practices that help to account for security as they develop, manufacture, implement, or use network-connected devices. Specifically, these principles are designed for:

1	IoT developers to factor in security when a device, sensor, service, or any component of the IoT is being designed and developed;
2	IoT manufacturers to improve security for both consumer devices and vendor managed devices;
3	Service providers , that implement services through IoT devices, to consider the security of the functions offered by those IoT devices, as well as the underlying security of the infrastructure enabling these services; and
4	Industrial and business-level consumers (including the federal government and critical infrastructure owners and operators) to serve as leaders in engaging manufacturers and service providers on the security of IoT devices.

STRATEGIC PRINCIPLES FOR SECURING IOT

The principles set forth below are designed to improve security of IoT across the full range of design, manufacturing, and deployment activities. Widespread adoption of these strategic principles and the associated suggested practices would dramatically improve the security posture of IoT. There is, however, no one-size-fits-all solution for mitigating IoT security risks. Not all of the practices listed below will be equally relevant across the diversity of IoT devices. These principles are intended to be adapted and applied through a risk-based approach that takes into account relevant business contexts, as well as the particular threats and consequences that may result from incidents involving a network-connected device, system, or service.

Incorporate Security at the Design Phase

Security should be evaluated as an integral component of any network-connected device. While there are exceptions, in too many cases economic drivers or lack of awareness of the risks cause businesses to push devices to market with little regard for their security. Building security in at the design phase reduces potential disruptions and avoids the much more difficult and expensive endeavor of attempting to add security to products after they have been developed and deployed. By focusing on security as a feature of network-connected devices, manufacturers and service providers also have the opportunity for market differentiation. The practices below are some of the most effective ways to account for security in the earliest phases of design, development, and production.

What are the potential impacts of not building security in during design?

Failing to design and implement adequate security measures could be damaging to the manufacturer in terms of financial costs, reputational costs, or product recall costs. While there is not yet an established body of case law addressing IoT context, traditional tort principles of product liability can be expected to apply.

SUGGESTED PRACTICES:

Enable security by default through unique, hard to crack default user names and passwords. User names and passwords for IoT devices supplied by the manufacturer are

often never changed by the user and are easily cracked. Botnets operate by continuously scanning for IoT devices that are protected by known factory default user names and passwords. Strong security controls should be something the industrial consumer has to deliberately disable rather than deliberately enable.

Build the device using the most **recent operating system** that is technically viable and economically feasible. Many IoT devices use Linux operating systems, but may not use the most up-to-date operating system. Using the current operating system ensures that known vulnerabilities will have been mitigated.

Use **hardware that incorporates security features** to strengthen the protection and integrity of the device. For example, use computer chips that integrate security at the transistor level, embedded in the processor, and provide encryption and anonymity.

Design with system and operational disruption in mind. Understanding what consequences could flow from the failure of a device will enable developers, manufacturers, and service providers to make more informed risk-based security decisions. Where feasible, developers should build IoT devices to fail safely and securely, so that the failure does not lead to greater systemic disruption.

Promote Security Updates and Vulnerability Management

Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies. In designing these strategies, developers should consider the implications of a device failure, the durability of the associated product, and the anticipated cost of repair. In the absence of the ability to deploy security updates, manufacturers may be faced with the decision between costly recalls and leaving devices with known vulnerabilities in circulation.

FOCUS ON: NTIA Multi-Stakeholder Process on Patching and Updating

The National Telecommunications and Information Administration (NTIA) has convened a multi-stakeholder process concerning the “Internet of Things Upgradability and Patching” to bring stakeholders together to share the range of views on security upgradability and patching, and to establish more concrete goals for industry-wide adoption.

SUGGESTED PRACTICES:

Consider ways in which to **secure the device over network connections or through automated means**. Ideally, patches would be applied automatically and leverage cryptographic integrity and authenticity protections to more quickly address vulnerabilities.

Consider **coordinating software updates among third-party vendors** to address vulnerabilities and security improvements to ensure consumer devices have the complete set of current protections.

Develop **automated mechanisms for addressing vulnerabilities**. In the software engineering space, for example, there are mechanisms for ingesting information from critical vulnerability reports sourced from the research and hacker communities in real time. This allows developers to address those vulnerabilities in the software design, and respond when appropriate.

Develop a policy regarding the **coordinated disclosure of vulnerabilities**, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT). The US Computer Emergency Readiness Team (US-CERT), Industrial Control Systems (ICS)-CERT, and other CSIRTs provide regular technical alerts, including after major incidents, which provide information about vulnerabilities and mitigation.

Develop an **end-of-life strategy** for IoT products. Not all IoT devices will be indefinitely patchable and updateable. Developers should consider product sunset issues ahead of time and communicate to manufacturers and consumers expectations regarding the device and the risks of using a device beyond its usability date.

Build on Recognized Security Practices

Many tested practices used in traditional IT and network security can be applied to IoT. These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices.

FOCUS ON: NIST Cybersecurity Risk Management Framework

The National Institute of Standards and Technology (NIST) published a framework for cybersecurity risk management that has been widely adopted by private industry, integrated across sectors, and within organizations. The framework is widely recognized as a comprehensive touchstone for organizational cyber risk management <https://www.nist.gov/cyberframework>. While not specific to IoT, the risk framework provides a starting point for considering risks and best practices.

SUGGESTED PRACTICES:

Start with **basic software security and cybersecurity practices** and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways.

Refer to relevant **Sector-Specific Guidance**, where it exists, as a starting point from which to consider security practices. Some federal agencies address security practices for the unique sectors that they regulate. For example, the National Highway Traffic Safety Administration (NHTSA) recently released guidance on [Cybersecurity Best Practices for Modern Vehicles](#) that address some of the unique risks posed by autonomous or semi-autonomous vehicles. Similarly, the Food and Drug Administration released draft guidance on [Postmarket Management of Cybersecurity in Medical Devices](#).

Practice defense in depth. Developers and manufacturers should employ a holistic approach to security that includes layered defenses against cybersecurity threats, including user-level tools as potential entry points for malicious actors. This is especially valuable if patching or updating mechanisms are not available or insufficient to address a specific vulnerability.

Participate in **information sharing platforms** to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise³. The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), as well as multi-state and sector-specific information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs), are examples.

³ ["Information Sharing,"](#) National Cybersecurity and Communications Information Center.

Prioritize Security Measures According to Potential Impact

Risk models differ substantially across the IoT ecosystem. For example, industrial consumers (such as nuclear reactor owners and operators) will have different considerations than a retail consumer. The consequences of a security failure across different customers will also vary significantly. Focusing on the potential consequences of disruption, breach, or malicious activity across the consumer spectrum is therefore critical in determining where particular security efforts should be directed, and who is best able to mitigate significant consequences.

Should IoT security measures focus on the IoT device?

Since the purpose of all IoT processes is to take in information at a physical point and motivate a decision based on that information (sometimes with physical consequences), security measures can focus on one or more parts of the IoT process. As noted earlier, the risks to IoT begin with the specific device, but are certainly not limited to it. Developers, manufacturers, and service providers should consider specific risks to the IoT device as well as process and service, and make decisions based on relative impact to all three as to where the most robust measures should be applied.

SUGGESTED PRACTICES:

Know a device's **intended use and environment**, where possible. This awareness helps developers and manufacturers consider the technical characteristics of the IoT device, how the device may operate, and the security measures that may be necessary.

Perform a “**red-teaming**” **exercise**, where developers actively try to bypass the security measures needed at the application, network, data, or physical layers. The resulting analysis and mitigation planning should help prioritize decisions on where and how to incorporate additional security measures.

Identify and authenticate the devices connected to the network, especially for industrial consumers and business networks. Applying authentication measures for known devices and services allows the industrial consumer to control those devices and services that are within their organizational frameworks.

Promote Transparency across IoT

Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Reliance on the many low-cost, easily accessible software and hardware solutions used in IoT can make this challenging. Because developers and manufacturers rely on outside sources for low-cost, easily accessible software and hardware solutions, they may not be able to accurately assess the level of security built into component parts when developing and deploying network-connected devices. Furthermore, since many IoT devices leverage open source packages, developers and manufacturers may not be able to identify the sources of these component parts.

Increased awareness could help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies. Depending on the risk profile of the product in question, developers, manufacturers, and service providers will be better equipped to appropriately mitigate threats and vulnerabilities as expeditiously as possible, whether through patching, product recall, or consumer advisory.

SUGGESTED PRACTICES:

Conduct end-to-end risk assessments that account for both internal and **third party vendor risks**, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded.

Consider creating a **publicly disclosed mechanism for using vulnerability reports**. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.

Consider developing and employing a **software bill of materials** that can be used as a means of building shared trust among vendors and manufacturers. Developers and manufacturers should consider providing a list of known hardware and software components in the device package in a manner which is mindful of the need to protect intellectual property issues. A list can serve as a valuable tool for others in the IoT ecosystem to understand and manage their risk and patch any vulnerabilities immediately following any incident.

Connect Carefully and Deliberately

IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption. IoT consumers can also help contain the potential threats posed by network connectivity by connecting carefully and deliberately, and weighing the risks of a potential breach or failure of an IoT device against the costs of limiting connectivity to the Internet.

In the current networked environment, it is likely that any given IoT device may be disrupted during its lifecycle. IoT developers, manufacturers, and consumers should consider how a disruption will impact the IoT device's primary function and business operations following the disruption.

Does every networked device need continuous, automated connection to the Internet?

In 2015, the Federal Trade Commission published a [guide](#) called "Start with Security: A Guide for Businesses" to help them determine this very question. While it may be convenient to have continuous network access, it may not be necessary for the purpose of the device – and systems; for example, nuclear reactors, where a continuous connection to the internet opens up the opportunity for an intrusion of potentially enormous consequences.

SUGGESTED PRACTICES:

Advise IoT consumers on the intended purpose of any network connections. Direct internet connections may not be needed to operate critical functions of an IoT device, particularly in the industrial setting. Information about the nature and purpose of connections can inform consumer decisions.

Make intentional connections. There are instances when it is in the consumer's interest not to connect directly to the Internet, but instead to a local network that can aggregate and evaluate any critical information. For example, Industrial Control Systems (ICS) should be protected through defense in depth principles as published by https://ics-cert.us-cert.gov/recommended_practices.

Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable **selective connectivity**. Depending on the purpose of the IoT device, providing the consumers with guidance and control over the end implementation can be a sound practice.

CONCLUSION

Our nation cannot afford a generation of IoT devices deployed with little consideration for security. The consequences are too high given the potential for harm to our critical infrastructure, our personal privacy, and our economy.

As DHS issues these principles, we recognize the efforts underway by our colleagues at other federal agencies, and the work of private sector entities to advance architectures and institute practices to address the security of the IoT. This document is a first step to strengthen those efforts by articulating overarching security principles. But next steps will surely be required.

DHS identifies four lines of effort that should be undertaken across government and industry to fortify the security of the IoT.

FOUR LINES OF EFFORT:

1



Coordinate across federal departments and agencies to engage with IoT stakeholders and jointly explore ways to mitigate the risks posed by IoT.

DHS with its federal partners will continue to engage with industry partners to determine approaches that can further enhance IoT security, and to promote understanding of evolving technology trends that may address IoT risks. Future efforts will also focus on updating and applying these principles, as best practices and approaches are further refined and understood.

2



Build awareness of risks associated with IoT across stakeholders.

It is important that stakeholders are aware of IoT risks so that they can position themselves to address them. DHS will accelerate public awareness, education, and training initiatives, in partnership with other agencies, the private sector, and international partners. DHS, together with other agencies, will also undertake initiatives more directly tailored to particular sectors and individual consumers.

3



Identify and advance incentives for incorporating IoT security.

Policymakers, legislators, and stakeholders need to consider ways to better incentivize efforts to enhance the security of IoT. In the current environment, it is too often unclear who bears responsibility for the security of a given product or system. In addition, the costs of poor security are often not borne by those best positioned to increase security. DHS and all other stakeholders need to consider

how tort liability, cyber insurance, legislation, regulation, voluntary certification management, standards-settings initiatives, voluntary industry-level initiatives, and other mechanisms could improve security while still encouraging economic activity and groundbreaking innovation. Going forward, DHS will convene with partners to discuss these critical matters and solicit ideas and feedback.

4



Contribute to international standards development processes for IoT.

IoT is part of a global ecosystem, and other countries and international organizations are beginning to evaluate many of these same security considerations. It is important that IoT-related activities not splinter into inconsistent sets of standards or rules. As DHS becomes increasingly focused on IoT efforts, we must engage with our international partners and the private sector to support the development of international standards and ensure they align with our commitment to fostering innovation and promoting security.

DHS looks forward to these next collaborative steps. Together, we can, and must, address these complex challenges. By doing so, we will ensure that our network-connected future is not only innovative, but also secure and built to last.

APPENDIX: GUIDANCE AND ADDITIONAL RESOURCES

The principles in this document have been developed based on information gathered from industry reports, and through discussions with private industry, trade associations, non-governmental entities, and Federal partners, especially with NIST and NTIA.

Department of Homeland Security

- <https://www.dhs.gov/sites/default/files/publications/draft-lces-security-comments-508.pdf>
- <https://www.dhs.gov/publication/security-tenets-lces>
- <https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf>

Other Federal Entities

- [National Security Telecommunications Advisory Committee](#)
 1. [Final NSTAC Internet of Things Report](#)
- [NTIA](#)
 1. [Notice and Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things](#)
 - a) [Comments](#)
 2. [Green Paper – Cybersecurity, Innovation and the Internet Economy, 2011](#)
 3. [New Insights into the Emerging Internet of Things](#)
 4. [Remarks of Deputy Assistant Secretary Simpson at Fostering the Advancement of the Internet of Things Workshop, 9/9/2016](#)
 - a) Announcement for [Fostering the Advancement of the Internet of Things Workshop](#)
 5. Internet Policy Task Force [resource/review/cataloging](#) of the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things.
- NIST
 1. Cybersecurity [Framework](#)
 2. [Cyber-Physical Systems \(CPS\) Program](#)
 - a) CPS Public Working Group (PWG) [draft Cyber-Physical Systems \(CPS\) Framework Release 1.0](#)
 - o [Comments accepted through 9/2/2015](#)

3. [Smart-Grid](#) Program
 4. International Technical Working Group on [IoT-Enabled Smart City Framework](#)
 5. NIST Special Publication (SP) [800-183](#), Network of Things, 7/28/2016.
 - a) NIST [news release](#)
- Federal Trade Commission
 1. FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January 2015.
 - United States Congress
 1. Senate Committee on Commerce, Science, and Transportation committee hearing, "[The Connected World: Examining the Internet of Things](#)."
 2. Senate unanimously bipartisan resolution ([S. Res. 110](#)) calling for a national strategy to guide the development of the Internet of Things.
 3. House Energy and Commerce Committee's "[The Internet of Things: Exploring the Next Technology Frontier](#)"
 - Government Accounting Office
 1. [GAO engagement with DHS](#): GAO is currently engaged with DHS on IoT, code 100435 [January 15, 2016 notification letter available via this [link](#)]
 - a) Status/entry in the most recent, June 3, 2016 [List of Active GAO Engagements Related to DHS](#)

External Sources

The list of additional resources is provided solely as a reference and does not constitute an endorsement by the Department of Homeland Security (DHS). DHS does not endorse any commercial product, service, or enterprise.

- Atlantic Council
 1. Smart Homes and the Internet of Things – <http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things>
- I Am The Cavalry
 1. Five Star Automotive Cyber Safety Framework – <https://iamthecavalry.org/5star>
 2. Hippocratic Oath for Connected Medical Devices – <https://iamthecavalry.org/oath>
- Online Trust Alliance
 1. [Consumer Best Practices](#)
- Industrial Internet Consortium: <http://www.iiconsortium.org/IISF.htm>
- Open Web Application Security Project (OWASP)

1. Internet of Things Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
 2. Internet of Things Security Guidance
https://www.owasp.org/index.php/IoT_Security_Guidance
- Safecode.org relevant industry best practices www.safecode.org
 - AT&T
 1. [Exploring IoT Security](#)
 - Symantec
 1. An Internet of Things Reference Architecture
<https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf>

1 Eric H. Gibbs (Bar No. 178658)
2 Andre M. Mura (Bar No. 298541)
3 Linda Lam (Bar No. 301461)
4 **GIBBS LAW GROUP LLP**
5 505 14th Street, Suite 1110
6 Oakland, CA 94612
7 Telephone: (510) 350-9700
8 Facsimile: (510) 350-9701
ehg@classlawgroup.com
amm@classlawgroup.com
lpl@classlawgroup.com

9 Joseph W. Cotchett (Bar No. 36324)
10 Adam J. Zapala (Bar No. 245748)
11 Adam J. Trott (Bar No. 275520)
12 **COTCHETT, PITRE & McCARTHY, LLP**
13 840 Malcolm Road, Suite 200
14 Burlingame, CA 94010
15 Telephone: 650-697-6000
16 Facsimile: 650-697-0577
jcotchett@cpmlegal.com
azapala@cpmlegal.com
atrott@cpmlegal.com

17 *Plaintiffs' Interim Co-Lead Counsel*

18 **UNITED STATES DISTRICT COURT FOR THE**
19 **CENTRAL DISTRICT OF CALIFORNIA**
20 **SANTA ANA DIVISION**

21 IN RE: VIZIO, INC., CONSUMER
22 PRIVACY LITIGATION

23 This document relates to:
24 ALL ACTIONS

Case No. 8:16-ml-02693- JLS (KESx)

**PLAINTIFFS' MEMORANDUM OF
POINTS AND AUTHORITIES IN
SUPPORT OF MOTION FOR
PRELIMINARY APPROVAL OF
PROPOSED CLASS ACTION
SETTLEMENT (UNOPPOSED)**

25 Date: December 7, 2018
26 Time: 10:30 a.m.
27 Dept: Courtroom 10-A
28 Judge: Hon. Josephine L. Staton

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Summary of Argument	2
III.	Overview of the Litigation	3
A.	The alleged circumstances that prompted these lawsuits.....	3
B.	An abbreviated history of these legal proceedings.	6
IV.	Terms of Proposed Settlement.....	9
A.	Proposed Settlement Class	9
B.	Settlement Fund.....	10
C.	Injunctive Relief.....	11
D.	Release	13
E.	Notice	13
F.	Administration.....	15
IV.	Argument	15
A.	Certification of the Proposed Settlement Class Is Appropriate.	16
1.	Rule 23(a) Is Satisfied.....	18
2.	Rule 23(b)(3) Is Satisfied.....	20
3.	Appointment of Class Counsel Is Merited.	22
B.	Preliminary Approval of the Settlement Is Warranted.	22
1.	Strength of Plaintiffs’ Case.....	24
2.	Risk, Complexity, Costs, and Likely Duration of Further Litigation, and Risk of Maintaining Class Certification	29
3.	Amount Offered in Settlement.....	30
4.	Method of Distributing Relief	33
5.	Attorneys’ Fees and Costs, and Service Awards	34
6.	Stage of the Proceedings and Extent of Discovery Completed	35
7.	Support of Experienced Counsel	36
8.	Positive Views of Class Members	36
9.	No Signs of Collusion	36

1	C. Approval of the Proposed Settlement Administrator.....	38
2	V. CONCLUSION.....	42

TABLE OF AUTHORITIES

	Page
Cases	
<i>Abdullah v. U.S. Sec. Assocs.</i> , 731 F.3d 952 (9th Cir. 2013)	20
<i>Acosta v. Trans Union, LLC</i> , 243 F.R.D. 377 (C.D. Cal. 2007)	24
<i>Amchem Prods. v. Windsor</i> , 521 U.S. 591 (1997)	20
<i>Astiana v. Kashi Co.</i> , 291 F.R.D. 493 (C.D. Cal. 2013)	19
<i>Brown v. Hain Celestial Group, Inc.</i> , 2016 WL 631880 (N.D. Cal. Feb. 17, 2016)	39
<i>Campbell v. Facebook Inc.</i> , 315 F.R.D. 250 (N.D. Cal. 2016)	28, 29
<i>Cf. Lee v. Enter. Leasing Co.-W.</i> , No. 3:10-CV-00326-LRH, 2015 WL 2345540 n.5 (D. Nev. May 15, 2015)	32
<i>Clesceri v. Beach City Investigations & Protective Servs., Inc.</i> , Case No. CV-10-3873-JLS (RZx), 2011 WL 320998 (C.D. Cal. Jan. 27, 2011)	36
<i>DiracTV, Inc. v. Huynh</i> , 2005 WL 5864467 (N.D. Cal. May 31, 2005)	28, 29
<i>Ehret v. Uber Techs., Inc.</i> , 148 F. Supp. 3d 884 (N.D. Cal. 2015)	20
<i>Eichenberger v. ESPN, Inc.</i> , 876 F.3d 979 (9th Cir. 2017)	26
<i>Evon v. Law Offices of Sidney Mickell</i> , 688 F.3d 1015 (9th Cir. 2012)	18
<i>Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.</i> , 528 U.S. 167 (2000)	30
<i>Gustafson v. BAC Home Loans Servicing, LP</i> , 294 F.R.D. 529 (C.D. Cal. 2013)	21
<i>Hanlon v. Chrysler Corp.</i> , 150 F.3d 1011 (9th Cir. 1998)	21, 22
<i>Hesse v. Sprint Corp.</i> , 598 F.3d 581 (9th Cir. 2010)	34
<i>In re Bluetooth Headset Prod. Liab. Litig.</i> , 654 F.3d 935 (9th Cir. 2011)	23, 35, 37
<i>In re Hyundai And Kia Fuel Econ. Litig.</i> , 897 F.3d 1003 (9th Cir. 2018)	21
<i>In re LinkedIn User Privacy Litig.</i> , 309 F.R.D. 573 (N.D. Cal. 2015)	31

1	<i>In re Mex. Money Transfer Litig.</i> , 267 F.3d 743 (7th Cir. 2001)	21
2	<i>In re Omnivision Techs., Inc.</i> , 559 F. Supp. 2d 1036 (N.D. Cal. 2008)	36
3	<i>In re Online DVD-Rental Antitrust Litig.</i> , 779 F.3d 934 (9th Cir. 2015)	35
4	<i>In re Tableware Antitrust Litig.</i> , 484 F. Supp. 2d 1078 (N.D. Cal. 2007)	24, 31
6	<i>In re TFT-LCD (Flat Panel) Antitrust Litig.</i> , 2011 WL 7575004 (N.D. Cal. Dec. 27, 2011)	39
7	<i>In re Vizio, Inc., Consumer Privacy Litig.</i> , 238 F. Supp. 3d 1204 (C.D. Cal. 2017)	21, 27
8	<i>In re Zynga Privacy Litigation</i> , 750 F.3d 1098 (9th Cir. 2014)	27
9	<i>Konop v. Hawaiian Airlines</i> , 302 F.3d 868 (9th Cir. 2002)	27
10	<i>Linney v. Cellular Alaska P'ship</i> , 151 F.3d 1234 (9th Cir. 1998)	36
11	<i>Linney v. Cellular Alaska P'ship</i> , Nos. C-96-3008 DLJ, 1997 WL 450064 (N.D. Cal. July 18, 1997)	37
12	<i>Los Angeles Cnty. Metro. Transp. Auth. v. Superior Court</i> , 123 Cal. App. 4th 261 (2004)	25
13	<i>Mullins v. Premier Nutrition Corp.</i> , No. 13-CV-01271-RS, 2016 WL 1535057 (N.D. Cal. Apr. 15, 2016)	22
14	<i>Munday v. Navy Fed. Credit Union</i> , No. SACV151629-JLS-KESx, 2016 WL 7655807 (C.D. Cal. Sept. 15, 2016)	17
15	<i>Munday v. Navy Federal Credit Union</i> , 2016 WL 7655796 (C.D. Cal. Sep. 15, 2016)	39
16	<i>Nat'l Rural Telecomms. Coop. v. DIRECTV, Inc.</i> , 221 F.R.D. 523 (C.D. Cal. 2004)	31, 36
17	<i>Nicholson v. UTI Worldwide, Inc.</i> , No. 3:09-cv-722-JPG-DGW, 2011 WL 1775726 (S.D. Ill. May 10, 2011)	20
18	<i>Officers for Justice v. Civil Serv. Comm'n of City & Cnty. of San Francisco</i> , 688 F.2d 615 (9th Cir. 1982)	24
19	<i>Pelzer v. Vassalle</i> , 655 Fed. App'x 352 (6th Cir. 2016)	38
20	<i>Ramos v. Capital One, N.A.</i> , No. 17-CV-00435-BLF, 2017 WL 3232488 (N.D. Cal. July 27, 2017)	25
21	<i>Rhom v. Thumbtack, Inc.</i> , No. 16-CV-02008-HSG, 2017 WL 4642409 (N.D. Cal. Oct. 17, 2017)	35
22	<i>Schuchard v. Law Office of Rory W. Clark</i> , No. 15-cv-01329-JSC, 2016 WL 232435 (N.D. Cal. Jan. 20, 2016)	31
23	<i>Smoot v. United Transp. Union</i> , 246 F.3d 633 (6th Cir. 2001)	28
24		
25		
26		
27		
28		

1	<i>Staton v. Boeing Co.</i> , 327 F.3d 938 (9th Cir. 2003)	passim
2	<i>Torres v. Mercer Canyons Inc.</i> , 835 F.3d 1125 (9th Cir. 2016)	17, 19
3	<i>Tyson Foods, Inc. v. Bouaphakeo</i> , 136 S. Ct. 1036 (2016)	29
4	<i>United States v. Szymuszkiewicz</i> , 622 F.3d 701 (7th Cir. 2010)	27
5	<i>Valentino v. Carter-Wallace, Inc.</i> , 97 F.3d 1227 (9th Cir. 1996)	22
6	<i>Vandervort v. Balboa Capital Corp.</i> , 8 F. Supp. 3d 1200 (C.D. Cal. 2014)	30
7	<i>Vandervort v. Balboa Capital Corp.</i> , 2013 WL 12123234 (C.D. Cal. Nov. 20, 2013)	38
8	<i>Wal-Mart Stores, Inc. v. Dukes</i> , 564 U.S. 338 (2011)	17, 18
9	<i>Wang v. Chinese Daily News, Inc.</i> , 737 F.3d 538 (9th Cir. 2013)	17
10	<i>In re Volkswagen “Clean Diesel” Mktg., Sales Practices, & Prod. Liab. Litig.</i> , 895 F.3d 597 (9th Cir. 2018)	23, 24, 25
11	<i>Yershov v. Gannett Satellite Info. Network, Inc.</i> , 820 F.3d 482 (1st Cir. 2016)	26
12	Statutes	
13	18 U.S.C. § 2520(a)	17, 27
14	18 U.S.C. § 2710	17
15	18 U.S.C. § 2710(c)(2)	28
16	28 U.S.C. 2072	16
17	28 U.S.C. § 1715(b)	42
18	28 U.S.C. § 1715(d)	42
19	N.Y. Gen. Bus. Law § 349	8
20	Rules	
21	Fed. R. Civ. P. 23(a)(1)	17, 18
22	Fed. R. Civ. P. 23(c)(b)(2)	39, 41
23	Fed. R. Civ. P. 30(b)(6)	36
24	Fed. R. Evid. 408	36
25	Rule 23(a)	17
26	Rule 23(a)(2)	18
27	Rule 23(a)(3)	19

1	Rule 23(a)(4)	19
2	Rule 23(b)	17
3	Rule 23(b)(3)	17, 18, 20, 22
4	Rule 23(c)(2)(B)	40, 42
5	Rule 23(e)	23
6	Rule 23(e)(1)	40
7	Rule 23(e)(2)	22
8	Rule 23(e)(3)	24
9	Rule 23(g)	22
10	Other Authorities	
11	Duke Law School, <i>Implementing 2018 Amendments to Rule 23</i>	23, 24, 39
12	Manual for Complex Litigation, Fourth § 21.63 (2004)	16
13	<i>The End of Objector Blackmail?</i>	
14	62 Vand. L. Rev. 1623 (2009)	38
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 **I. Introduction**

2 Plaintiffs seek preliminary approval of a settlement agreement providing monetary
3 and injunctive relief for all individuals in the United States who purchased a Vizio Smart
4 Television for personal or household use, and not for resale, that was subsequently
5 connected to the Internet at any time between February 1, 2014 and February 6, 2017.
6 The nationwide relief negotiated at arm's length and under the supervision of a retired
7 federal judge, after years of intensive litigation and probing discovery, would end this
8 multi-district litigation against Vizio on the following terms:

9 *First*, Vizio will establish a non-reversionary \$17 million fund for proportional
10 monetary payments for settlement class members who submit a claim. The fund will cover
11 any court-approved expenses, costs, and attorneys' fees.

12 *Second*, beginning in December 2016, after this lawsuit was filed and in substantial
13 part because of it, Vizio revised its on-screen disclosures regarding its viewing-data
14 collection and sharing practices, in a stand-alone, on-screen disclosure, and asked for
15 permission to collect and share viewing data. Under this settlement, Vizio will make
16 additional changes to its on-screen disclosure for new customers and will add a disclosure
17 to a "quick start" guide that accompanies new Smart TVs.

18 *Third*, Vizio will delete all viewing data collected during the class period which it
19 possesses. An independent auditor will confirm that this deletion is successful.

20 Plaintiffs and class counsel are proud to present this settlement agreement to the
21 Court because it is restorative. The revenue that Vizio obtained from the collection and
22 licensing of viewing data during the class period will be fully disgorged; and in turn
23 settlement class members will receive compensation comfortably within the range of
24 reasonableness for their claims. Just as important, Vizio's collection of viewing data by
25 default ended as of February 2017. Vizio's disclosures were revamped—and will be
26 further revised as a result of this settlement. And Vizio will destroy the remaining
27 contested viewing data in its possession.

28 Given the settlement's many strengths and the real risk of achieving far less after

1 trial, the Court should grant this unopposed motion to begin the settlement approval
2 process.

3 **II. Summary of Argument**

4 All of the factors this Court must consider in determining whether to grant a
5 motion for preliminary approval are met here.

6 *First*, it is appropriate to conditionally certify a nationwide settlement class of all
7 individuals who purchased affected Smart TVs that were subsequently connected to the
8 Internet during the class period. Millions of consumers purchased the affected TVs and
9 connected them to the Internet (numerosity); questions common to all settlement class
10 members, including whether Vizio disclosed information that would readily permit an
11 ordinary person to identify a specific individual's video-watching behavior, are answerable
12 through common proof (commonality); the harm that Plaintiffs have suffered is identical
13 to the harm suffered by all settlement class members (typicality); and Plaintiffs and class
14 counsel will continue to vigorously prosecute this litigation on behalf of the settlement
15 class, as they have to date (adequacy).¹

16 In addition, common questions predominate over any individual ones because
17 Vizio engaged in a uniform course of conduct applicable to all settlement class members.
18 This includes the core allegation that Vizio collected and shared viewing data during the
19 class period without consumers' knowledge or consent. The proposed settlement class is
20 thus sufficiently cohesive to warrant adjudication by representation. And here, because
21 conditional certification of a single nationwide class would be based on alleged violations
22 of federal law, there can be no argument that differences in state law defeat
23 predominance.

24 Further, class adjudication is superior to other available methods of adjudication,
25 such as individual litigation, for two reasons. The high cost of litigating this case involving
26 complex technology overwhelms Vizio's potential liability per consumer. And the only
27 economically rational way for litigants and the courts to resolve millions of such claims is

28 ¹ Vizio does not oppose class certification solely for the purposes of settlement only.

1 through the class device.

2 *Second*, the proposed settlement is fair, reasonable, and adequate, and will likely be
3 granted final approval. It is the product of serious, informed, non-collusive negotiations,
4 before a former federal judge, after considerable litigation and discovery. It does not
5 improperly grant preferential treatment to class representatives or segments of the class. It
6 falls within the range of possible approval. And it has no obvious deficiencies. To assure
7 the Court that preliminary approval is appropriate and final approval likely, Plaintiffs
8 discuss herein the class definition, benefits, claims process, distribution plan (including for
9 unclaimed funds), the scope of the release, the range of litigated outcomes, the extent of
10 discovery, the views of Plaintiffs and counsel, the manner in which attorneys' fees will be
11 addressed, and demonstrate there are no signs, explicit or subtle, of collusion between the
12 parties. Plaintiffs will also seek the Court's approval of a settlement administrator.

13 *Third*, the proposed content and method of the class notice plan is sufficient. The
14 notice program is tailored to this case and designed to maximize the number of claims
15 from approximately 16 million class members. Affected Smart TVs that remain connected
16 to the Internet will display a clear, concise, and plain notice to an estimated 6 million class
17 members. That same notice will be e-mailed to an estimated 9 million class members. A
18 custom digital and print media campaign accounting for class demographics further
19 pushes the reach of this notice program well past the constitutional line. A long-form
20 notice will also be available, in English and Spanish, at www.VizioTVsettlement.com, and
21 it will answer typical questions and provide important information. Not only is this digital
22 notice program the best practicable under the circumstances, it avoids the sizeable
23 expense that attends first-class mail notice.

24 **III. Overview of the Litigation**

25 **A. The alleged circumstances that prompted these lawsuits.²**

26 Based in Irvine, California, Vizio has designed and sold televisions in the United
27

28 ² Vizio's current disclosures concerning viewing data collection and licensing, which were implemented in early 2017, are described in more detail in Section IV.C.

1 States since 2002. This includes Internet-connected televisions, or “Smart” TVs, a key
2 feature of which is the TV’s ability to access online media content, including movies and
3 music.

4 Beginning in February 2014, Vizio remotely installed automated (or automatic)
5 content recognition software on Smart TVs that had already been sold and that did not
6 have such software when sold. In about August 2014, Vizio began selling Smart TVs with
7 this software pre-installed.

8 This technology monitors the video stream of all physical inputs and certain
9 streamed content, by capturing real-time or near real-time data to construct a historical
10 record of the content displayed on-screen with one-second granularity. A mathematical
11 representation of a subsample of the viewing data, along with a unique identification
12 number assigned to the TV, are sent to a server that operates as a match database.

13 More simply: Say you own a Smart TV with this software and it is connected to the
14 Internet. You are watching a cable news program. As the program plays, the software
15 captures certain pixels that appear on your screen and sends the mathematical
16 representation and a unique number assigned to your TV to a computer server in the
17 cloud. If the server has in its library this particular program,³ then what you’re watching
18 on your Smart TV is identified; but if not, not. If there is no match, the viewing
19 information is discarded. But if there is a match, a summary of the viewing information is
20 stored.

21 In addition to capturing information about what is displayed, the software collects
22 the TV’s Internet-protocol address and WiFi signal strength, among other information.
23 This information facilitates the delivery of advertisements to other electronic devices
24 connected to the same network, such as a mobile device.

25 Why is “viewing data”—information about the content viewed on a TV and reports
26 or data derived therefrom or combined with such data—collected? According to public

27
28 ³ The server ingests certain types of content and certain services but not pornographic material.

1 statements by Vizio, “the collection of viewing data can be used to generate intelligent
2 insights for advertisers and media content providers and to drive their delivery of more
3 relevant, personalized content to Smart TVs.” Vizio, *Form S-1 Registration Statement* (July
4 24, 2015), at *2.⁴ At one point, Vizio stated that its tracking software captures up to 100
5 billion data points each day from more than 10 million televisions, and “provides highly
6 specific viewing behavior data on a massive scale with great accuracy, ...” *Id.*

7 Vizio earns revenue by licensing this data to third parties. Decl. of Wilda Siu
8 (identifying specific amount). Between February 1, 2014 and February 6, 2017, Vizio
9 earned revenue that is less than the settlement amount.

10 During this time, the data was licensed to third parties under contracts that purport
11 to bar them from associating viewing data with individuals or households by name or
12 physical addresses. (Vizio does not itself associate viewing data with individuals or
13 households by name or physical address, or share information such as name or physical
14 address with third parties.) The contracts, however, allow third parties to associate viewing
15 data with demographic information such as sex, age, income, marital status, and
16 education.

17 Between February 2014 and February 2017, third parties licensed viewing data for
18 three purposes: to determine in the aggregate what consumers watch and how they watch
19 it; to analyze the effectiveness of advertising; and, starting in 2016 (after a notification was
20 displayed on-screen referencing explicitly the delivery of target advertisements based on
21 the collection of viewing data), to enable ad retargeting.

22 Consumers who purchased Smart TVs that received this tracking software through
23 a software update were presented with a message on the TV that said:

24 The VIZIO Privacy Policy has changed. Smart Interactivity has been enabled
25 on your TV, but you may disable it in the settings menu. See
26 www.vizio.com/privacy for more details. This message will time out in 1
minute.

27 ⁴ Available at
28 <https://www.sec.gov/Archives/edgar/data/1648158/000119312515262817/d946612ds1.htm>.

1 Consumers who purchased Smart TVs with this software pre-installed also received this
2 notice.

3 “Smart Interactivity” referred to the collection of viewing data. The software was
4 on by default and operated continuously unless it was turned off by the consumer.

5 The settings menu of these TVs included the setting “Smart Interactivity” and the
6 description, “Enables program offers and suggestions.” Although Vizio maintains that it
7 intended to and worked to develop certain program offers and suggestions during the
8 class period, no program offers or suggestions were enabled for more than two years.

9 To turn “Smart Interactivity” off, a consumer would have had to find this setting in
10 the menu, click on it, and then click again to disable it.

11 Between approximately Fall 2015 and Summer 2016, consumers whose Smart TVs
12 had ACR software installed received a new notice stating:

13 Select Reset & Admin in System to disable the collection and analysis of
14 viewing history from this television (“Smart Interactivity”). NEW: Smart
15 Interactivity may enable the delivery of tailored ads based upon viewing
16 history to smartphones or other devices that share an IP address or other
non-personal identifiers with the television.

17 **B. An abbreviated history of these legal proceedings.**

18 In November 2015, investigative journalists at ProPublica reported that Vizio
19 Smart TVs collect and share customers’ viewing habits with advertisers. Class action
20 complaints were filed apace and later centralized for pre-trial proceedings in this Court.

21 Upon centralization here, the Court appointed interim co-lead counsel and a
22 steering committee for Plaintiffs, as well as lead counsel for Defendants; denied a request
23 by Vizio to stay discovery until the pleadings were set; and issued a case management
24 schedule.

25 In August 2016, Plaintiffs filed a consolidated class action complaint against several
26 Vizio entities on behalf of a nationwide class of individuals who purchased affected Smart
27 TVs, and on behalf of subclasses of individuals from California, Florida, Massachusetts,
28 New York, and Florida. The complaint asserted a variety of federal and state privacy

1 claims, and state consumer protection claims. The common thread linking all of these
2 claims was the allegation that “Vizio offered Smart TVs equipped with automatic content
3 recognition software that collected consumers’ viewing histories and then sold that
4 information—along with ‘highly specific’ information about consumers’ digital
5 identities—to third parties, without consumers’ knowledge or consent.” Order Denying
6 Mot. for Interlocutory Appeal at 2.

7 Vizio responded to the complaint by moving to dismiss. After the Court received
8 outsized briefing and held oral argument, it granted and denied the motion in part,
9 allowing Plaintiffs the opportunity to replead any dismissed claim.

10 In March 2017, Plaintiffs filed a second consolidated complaint. Vizio again moved
11 to dismiss. It argued that Plaintiffs’ claims for injunctive relief were moot because Vizio
12 had entered into a consent decree with the Federal Trade Commission in February 2017
13 that required Vizio to change its business practices relating to the collection of viewing
14 data. Vizio also contested certain legal claims as insufficiently pleaded, and it asked the
15 Court to strike the class definition in the second consolidated complaint because it
16 included consumers who might be bound by arbitration agreements that forbid class
17 proceedings in any forum.

18 After briefing and oral argument, the Court denied Vizio’s motion in full. Vizio
19 then filed an answer to the second consolidated complaint in August 2017. A few months
20 later, the Court refused Vizio’s separate request to certify an immediate appeal on
21 questions of law pertaining to Vizio’s liability under the federal Video Privacy Protection
22 Act.

23 As things stand, Dicisha Hodges and Rory Zufolo of California; John Walsh of
24 Massachusetts; Chris Rizzitello of New York; Linda Thomson of Washington; and Mark
25 Queenan of Florida are named Plaintiffs for the nationwide class and their respective state
26 sub-classes.

27 The Defendants named in the operative pleadings are Vizio, Inc., Vizio Holdings,
28 Inc., Vizio Inscape Technologies, LLC; and Vizio Inscape Services, LLC. Their roles are

1 as follows. Vizio, Inc. is the primary Vizio entity for consumer electronics, such as Smart
2 TVs. Vizio Holdings, Inc. was established as a holding company pending a public offering
3 that was initiated with the filing of an S1 in July 2015 but did not advance.

4 Inscape Data, Inc. (formerly Vizio Inscape Technologies, LLC) (hereinafter
5 “Inscape”) develops the software on Vizio units that can recognize onscreen content, and
6 selectively maintains a record of viewing history associated with the television. Inscape
7 also owns the underlying automated content recognition technology, which recognizes
8 onscreen content.⁵ And Vizio Services, LLC (formerly Vizio Inscape Services, LLC) is the
9 entity that enters into contracts with customers for Inscape viewing data.⁶

10 As for the parties’ respective legal theories, Plaintiffs have proceeded to discovery
11 under the Video Privacy Protection Act, Wiretap Act, California Invasion of Privacy Act,
12 California Consumer Legal Remedies Act, California Unfair Competition Law, Florida
13 Deceptive and Unfair Trade Practices Act, N.Y. Gen. Bus. Law § 349, Massachusetts
14 Unfair and Deceptive Trade Practices Statute, Massachusetts Privacy Act, Washington
15 Consumer Protection Act, unjust enrichment, intrusion upon seclusion, and fraudulent
16 omission claims.

17 Vizio has denied Plaintiffs’ allegations and has raised thirty-seven affirmative
18 defenses. Vizio takes the position that it properly disclosed the collection of viewing data
19 to consumers; that consumers consented to or had knowledge of Vizio’s collection and
20 sharing of viewing data; that the data collected by Vizio does not constitute personally
21 identifiable information; that consumers must arbitrate their claims and cannot maintain
22 class actions; and consumers’ damages are speculative or must be judicially limited by law
23 which proscribes damages awards that exceed actual harm.

24 _____
25 ⁵ Inscape is the original Cognitive Media Networks Inc. entity. It was converted to an LLC
26 when acquired by Vizio, Inc., and all Vizio-owned viewing data was transferred to this
27 entity.

28 ⁶ The second consolidated complaint named Vizio Inscape Technologies, LLC and Vizio
Inscape Services, LLC. The Defendants’ answer to this complaint recognizes that the
former is now Vizio Services, LLC, and the latter is now Inscape Data, Inc. We thus refer
to these Vizio entities by their current corporate names in settlement documents and this
motion.

1 **IV. Terms of Proposed Settlement⁷**

2 **A. Proposed Settlement Class**

3 If approved, the settlement would offer relief to the following proposed class:

4 All individuals in the United States who purchased a VIZIO Smart
5 Television for personal or household use, and not for resale, that was
6 subsequently connected to the Internet at any time between February 1, 2014
and February 6, 2017.

7 Joint Decl. in Support of Motion for Preliminary Approval, Ex. 1 (hereinafter,
8 “Settlement”) ¶ I.32.

9 The time frame proposed corresponds with when Vizio first implemented
10 automatic content recognition technology (February 1, 2014), and when Vizio stopped
11 collecting viewing data through this software from Vizio Smart TVs unless the consumer
12 affirmatively consented (February 6, 2017). Settlement ¶¶ Recitals B.10-14. Note that
13 “viewing data” is defined in the settlement agreement to correspond with the definition of
14 viewing data in the consent decree with the Federal Trade Commission.

15 All Vizio Smart TVs, including the SmartCast product line, were pre-installed with
16 this software, or the software was installed remotely through an over-the-air update. The
17 number of TVs with this software which connected to Vizio’s servers during the class
18 period is approximately 16 million. Assuming one purchaser per TV per household, the
19 proposed class covers approximately 16 million individuals

20 The proposed settlement class definition parallels the nationwide class definition
21 pleaded in the operative Second Consolidated Complaint (which is identical to the
22 definition pleaded in the Consolidated Complaint). The definition proposed in these
23 pleadings was:

24 All individuals in the United States who purchased a VIZIO Smart TV with
25 Smart Interactivity capability for personal or household use, and not for
resale, during the applicable statute of limitations period.

26 Second Consol. Compl., Doc. 136 at ¶ 102.

27 ⁷ For readability, defined terms are not capitalized in the motion or memorandum, unless
28 in quoted material or in the conclusion. The proposed order, by contrast, capitalizes
defined terms as they appear in the settlement agreement.

1 The parties have made two changes to the proposed nationwide settlement class
2 definition, neither of which affects the scope of the class. First, the proposed class
3 definition now includes a specific date range. Second, the proposed class definition no
4 longer refers to “Smart Interactivity capability,” the Vizio’s name for the automated
5 content recognition software. Because Vizio’s entire Smart TV line had this software
6 during the class period, it is unnecessary to mention the software by name for purposes of
7 class identification. The time period specified is sufficient to identify who is in, and who is
8 outside of, the proposed class. The deletion of this language also improves clarity.

9 **B. Settlement Fund**

10 The proposed settlement contemplates a settlement fund in the amount of
11 \$17,000,000. After payment of attorneys’ fees and expenses to Class Counsel, payment of
12 the settlement administration costs, and payment of service awards, the remaining balance
13 will be distributed proportionally to all settlement class members who submit valid claims.

14 The settlement fund is non-reversionary, meaning, Vizio will not be entitled to
15 retain any part of the settlement amount that is not paid out or distributed as part of the
16 administration of the settlement for any reason. Any part of the settlement amount that
17 cannot feasibly be distributed to the class will be subject to a cy pres distribution to be
18 proposed by Plaintiffs and approved by the Court.

19 Plaintiffs will ask the Court to award each named plaintiff up to \$5,000 from the
20 settlement fund in recognition of the time, effort, and expense they incurred pursuing
21 claims against Vizio, which ultimately benefited the entire class. Vizio will not oppose this
22 request. The settlement agreement preserves the Court’s supervisory authority to
23 determine the appropriateness of any service award.

24 Counsel will petition the Court for an award of attorneys’ fees and reimbursement
25 of costs or expenses from the settlement fund. Vizio will not oppose a request that does
26 not exceed 33 percent of the settlement fund. The settlement agreement also preserves the
27 Court’s supervisory authority to determine the appropriateness of any such award or
28 reimbursement.

1 **C. Injunctive Relief**

2 The proposed settlement provides several different forms of injunctive relief in the
3 form of business practice changes that correspond with changes which took place during
4 the class period pursuant to a consent decree between Vizio and the Federal Trade
5 Commission. *See* Settlement, §§ VI, XII.

6 Under this consent order, Vizio agreed to display a prominent and detailed
7 notification on the TV screen, separate and apart from any privacy policy, terms of use
8 page, or other similar document. As part of this notification, Vizio gave consumers the
9 option to accept viewing data collection. If a consumer opted not to accept viewing data
10 collection, then no viewing data would be collected from the Smart TV.

11 Professor Joseph Turow, a leading privacy expert, was asked to review the
12 disclosures Vizio has used since February 2017 and the disclosures proposed here, as well
13 as contemporaneous on-screen disclosures of other smart television manufacturers whose
14 TV sets have software that collect viewing data. He concluded that only the revised Vizio
15 on-screen disclosures implemented with the FTC agreement:

16 prominently and collectively disclose to the customer—separate from any
17 privacy policy, terms of use page, or other similar document— four
18 categories of information: the types of viewing data that are collected and
19 used; the types of viewing data that will be shared with third parties; specific
categories of such third parties; and purposes for sharing such information.

20 Turow Decl. ¶ 32.⁸ Professor Turow also concluded that these revised disclosures “are
21 reasonably informative,” and “[a]s compared to the previous disclosures, this presentation
22 gives readers a useful overview of what the viewing data collection yields Vizio and
23 possibly them.” *Id.* ¶ 28.

24 Vizio’s imposition of prominent and clear disclosures in February 2017, and its
25 shift to an affirmative consent model, is a significant change which resolves a central
26 concern that motivated this lawsuit and the Federal Trade Commission’s investigation.

27
28 ⁸ The disclosures negotiated by the parties also address these categories of information. *See id.*

1 Vizio acknowledges that “Plaintiffs’ filing of this Action was a substantial cause of
2 VIZIO’s implementation of the Disclosures.” Settlement ¶ A.12.

3 The parties have negotiated further changes to the on-screen disclosure for new
4 customers and have secured an agreement that Vizio will disclose viewing data collection
5 in a “quick-start” guide. Turow Decl. ¶¶ 5, 7, 31-33. The disclosures will be displayed in
6 substantially the same form for the next five years. *Id.* ¶ 5.

7 The changes to the on-screen disclosure are two-fold. First, a “Decline” button will
8 now appear next to an “Accept” button. *Id.* ¶ 31. The “Decline” button replaces the
9 Settings button and different process for declining data collection, which Professor Turow
10 describes in his declaration. *Id.*

11 Second, the disclosure now explicitly states that “Declining Viewing Data collection
12 will not change the functionality of your device.” *Id.* Disabling viewing data collection on
13 Smart TVs of other manufacturers can change the functionality of the TV, including key
14 features. The language to be added effectively informs consumers of Vizio Smart TVs
15 “that there have not been adverse consequences in terms of functionality if viewing data
16 collection is declined.” *Id.*

17 In addition to the on-screen disclosure, Vizio will include additional language in the
18 device’s quick start guide . . . [that] alerts the customer to the right and ability to make a
19 decision during installation about allowing Vizio’s viewing data sharing[,] . . . [and]
20 increases the chances that customers will pause and think about what choice is best for
21 them.” *Id.*

22 Professor Turow concludes, based on his evaluation of these disclosures and the
23 disclosures of other manufacturers, “that the result is far superior to the disclosures (or
24 non-disclosures) that prompted this litigation and will be among the best in the industry.”
25 *Id.* ¶ 34.. He further writes:

26 This court proceeding is to be commended for setting a precedent of
27 significance. Its resolution signals to the industry the importance of
28 obtaining affirmative consent from a consumer before viewing data is
collected, and it provides a template for a prominent and clear disclosure that

1 allows a consumer to make an informed decision. Equally significant, this
2 precedent is being set at a time when the Smart TV viewing-data collection
3 industry is emerging.

4 *Id.* ¶ 8.

5 The final business practice change we will mention here is Vizio's agreement to
6 delete the remaining contested viewing data in its possession. Under the governmental
7 consent decree, Vizio was obligated to destroy viewing data that was collected prior to
8 March 1, 2016, unless a user of the television subsequently affirmatively consented to
9 viewing data collection when presented with the revised notices.

10 Under the settlement agreement, Vizio will extend the deletion period to
11 correspond with the class period and will destroy all viewing data collected during the
12 class period without exception. A third party will verify that the viewing data has been
13 successfully destroyed and will report to class counsel. If class counsel does not receive
14 such verification within the time specified by agreement, it is obligated to inform this
15 Court, which retains continuing jurisdiction to address any issues with the enforcement of
16 the settlement agreement.

17 These changes will take place after the effective date of finality.

18 **D. Release**

19 In exchange for the benefits provided under the settlement, the Plaintiffs and
20 settlement class members will release any legal claims that may arise from or relate to the
21 facts alleged or that could have been alleged in this action. This release is appropriately
22 tailored to the claims litigated to date in this multi-district litigation in that it extends only
23 to the "Vizio Released Parties" and does not include any other individual or entity.

24 **E. Notice**

25 The settlement proposes notice by electronic means.

26 First, notice will be provided directly to Vizio Smart TVs three separate times,
27 unless a person viewing the notice selects to dismiss the notice, in which case it will only
28 appear one more time (for a total of two times). The notice will time out after 45 seconds.
It tells class members that this is a class action; it references the class definition

1 (“Purchased a VIZIO Smart TV Connected to the Internet Between February 1, 2014 and
2 February 6, 2017? You Could Get Money From a \$17 Million Class Action Settlement”).
3 And it informs the reader that the class alleges privacy and consumer protection claims;
4 that a class member may appear through an attorney if the member wants; that class
5 members can be excluded; the time and manner for requesting exclusion; and the binding
6 effect of a class judgment. It includes the date by which to file a claim and provides the
7 address for a settlement website, which hosts the Long Form notice and important
8 pleadings and other filings. This notice is estimated to reach 6 million Smart TVs.

9 Second, a substantially similar notice will also be sent to approximately 9 million
10 potential class members via e-mail. The settlement administrator will use best practices to
11 increase deliverability and verify the number of e-mails successfully delivered

12 The sample notices do not yet include estimated compensation but an appropriate
13 estimated range for the notices would be \$13 to \$31, which assumes a 2 percent to 5
14 percent claims rate.

15 Third, a digital media campaign will supplement the TV and e-mail notices. As
16 explained further in the Declaration of Eric Schacter of A.B. Data, this campaign will
17 execute digital banners ads through the Google Display Network, Facebook (which
18 includes a settlement-specific Facebook page) and Google AdWords/Search platforms. A
19 minimum of 62 million impressions will be delivered. The campaign will also include a
20 notice through a press release over PR Newswire’s US1 and Hispanic Newslines. After the
21 press release is disseminated, both A.B. Data and PR Newswire will post the press release
22 on their respective Twitter pages. A copy of a digital banner ad is attached to the
23 Declaration of Eric Schacter of A.B. Data.

24 Lastly, the settlement administrator will set up a case-specific webpage for a long
25 form notice in English and Spanish, to host pleadings, to provide case updates, contact
26 information for the settlement administrator, as well as other information. The English
27 version of the long form notice is attached to the settlement agreement as an exhibit.

28 The notice and notice plan is further described below in Section V.C-D, the

1 Declaration of Eric Schachter of A.B. Data, and the settlement agreement.

2 **F. Administration**

3 The settlement agreement provides that payment will issue upon finality to class
4 members who submit valid a valid claim form. The claim form is attached to the
5 Declaration of Eric Schachter of A.B. Data, which describes the plan of allocation.

6 The settlement agreement also provides that the Settlement Administrator shall
7 disseminate the notice and implement the notice. And it provides procedures for
8 exclusion from the settlement class or to comment on or opt out of the settlement class.

9 Deadlines for these events and also the final approval hearing are proposed as
10 follows, under the assumption that an order granting preliminary approval issues on or
11 soon after December 7, 2018:

12

<u>Event</u>	<u>Date</u>
Notice of Class Action Settlement completed per Notice Plan	February 26, 2019
Deadline for Class Counsel to File Motion for Final Approval	March 19, 2019
Deadline for Class Counsel to File Motion for Attorney's Fees and Costs	March 19, 2019
Opt-Out and Objection Deadline	April 12, 2019
Reply in Support of Motions for Final Approval and Attorney's Fees and Costs	May 3, 2019
Final Approval Hearing	May 31, 2019

23

24 **IV. Argument**

25 The procedure for judicial approval of a proposed class action settlement under
26 Rule 23(e) typically involves three main steps:

- 27 (1) Certification of a settlement class and preliminary approval of the proposed
28 settlement after submission to the Court of a written motion for preliminary

1 approval.

2 (2) Dissemination of notice of the proposed settlement to the class members.

3 (3) A hearing at which evidence and argument concerning the fairness,
4 adequacy, and reasonableness of the proposed settlement may be presented.

5 *See* Federal Judicial Center, Manual for Complex Litigation, Fourth § 21.63 (2004).

6 Plaintiffs respectfully request that the Court begin this process by provisionally
7 certifying the proposed settlement class, granting preliminary approval of the proposed
8 settlement, and directing that notice be provided.

9 At the outset, we note that pending before Congress are amendments to Federal
10 Rule of Civil Procedure 23 that have been adopted by the Supreme Court of the United
11 States pursuant to 28 U.S.C. 2072. “Among other things, the amendments require lawyers
12 to provide additional information up front for the court to preliminarily approve
13 settlements (“frontloading”), permit notice by electronic means, impose limitations on
14 compensating objectors, and clarify final-settlement criteria.” Bolch Judicial Institute,
15 *Guidelines and Best Practices Implementing 2018 Amendments to Rule 23 Class Action Settlement*
16 *Provisions*, Duke Law School (August 2018), at *ii.⁹

17 The amendments will take effect on December 1, 2018, absent action by Congress,
18 and will “govern in all proceedings in civil cases thereafter commenced and, insofar as just
19 and practicable, all proceedings then pending.” April 26, 2018 Order of Supreme Court.¹⁰
20 Because Congress rarely takes such action, we apply here the soon-to-be-amended Rule 23
21 because this proceeding (and possibly this motion) will be pending when the new rule
22 takes effect in December, and because it is not impracticable or unjust to apply the new
23 rule to this case.

24 **A. Certification of the Proposed Settlement Class Is Appropriate.**

25 The Court should conditionally certify the settlement class for settlement purposes

26 _____
27 ⁹ Available at <https://judicialstudies.duke.edu/wp-content/uploads/2018/09/Class-Actions-Best-Practices-Final-Version.pdf>.

28 ¹⁰ www.supremecourt.gov/orders/courtorders/frcv18_5924.pdf (page 3 of 18). A copy of the amendments to this rule is available at this link.

1 under Rule 23(a) and 23(b)(3) based on violations of the federal Video Privacy Protection
2 Act, 18 U.S.C. § 2710, and Wiretap Act, *see* 18 U.S.C. § 2520(a).

3 “When conditionally certifying a class for settlement purposes, the Court ‘must pay
4 undiluted, even heightened, attention to class certification requirements.’” *Munday v. Navy*
5 *Fed. Credit Union*, No. SACV151629-JLS-KESx, 2016 WL 7655807, at *2 (C.D. Cal. Sept.
6 15, 2016) (citing *Staton v. Boeing Co.*, 327 F.3d 938, 952-53 (9th Cir. 2003) (internal
7 quotation marks omitted). “A party seeking class certification must satisfy the
8 requirements of Federal Rule of Civil Procedure 23(a) and the requirements of at least one
9 of the categories under Rule 23(b).” *Wang v. Chinese Daily News, Inc.*, 737 F.3d 538, 542 (9th
10 Cir. 2013). Rule 23 does not set forth a mere pleading standard,” but rather requires the
11 movant to be “prepared to prove that there are in fact sufficiently numerous parties,
12 common questions of law or fact, etc.” *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350
13 (2011) (emphasis removed). The Court, in turn, must engage in a “rigorous analysis” of
14 Rule 23 criteria, which frequently overlaps with the merits. *Id.* That said, the Court can
15 “consider merits questions at the class certification stage only to the extent they are
16 relevant to whether Rule 23 requirements have been met.” *Torres v. Mercer Canyons Inc.*, 835
17 F.3d 1125, 1133 (9th Cir. 2016).

18 “Rule 23(a) ensures that the named plaintiffs are appropriate representatives of the
19 class whose claims they wish to litigate.” *Dukes*, 564 U.S. at 349. It sets forth four
20 requirements a party seeking class certification must satisfy: numerosity, commonality,
21 typicality, and adequacy. Fed. R. Civ. P. 23(a).

22 “A proposed class must also satisfy the requirements for at least one of the three
23 types of class actions enumerated in Rule 23(b).” *Munday*, 2016 WL 7655807, at *3. Here,
24 Plaintiffs seek certification under Rule 23(b)(3), which authorizes a class proceeding if
25 “the court finds that the questions of law or fact common to class members predominate
26 over any questions affecting only individual members, and that a class action is superior to
27 other available methods for fairly and efficiently adjudicating the controversy.” Fed. R.
28 Civ. P. 23(b)(3).

1 **1. Rule 23(a) Is Satisfied.**

2 **a. The Class Members Are Too Numerous to Be Joined.**

3 The proposed class is so numerous that joinder of all members is impracticable. *See*
4 Fed. R. Civ. P. 23(a)(1). Vizio collected viewing data from Smart TVs that were connected
5 to the Internet between February 1, 2014 and February 6, 2017. All such TVs had
6 automated content recognition software installed, including the SmartCast product line.¹¹
7 Vizio estimates that 16 million TVs connected to its servers during the settlement class
8 period. Because the class is defined as one purchaser per household per television,
9 numerosity is plainly met.

10 **b. The Action Involves Common Questions of Law or Fact.**

11 Under Rule 23(a)(2)’s requirement that there be “questions of law or fact common
12 to the class,” the claims “must depend upon a common contention” such that
13 “determination of [their] truth or falsity will resolve an issue that is central to the validity
14 of each one of the claims in one stroke.” *Dukes*, 564 U.S. at 350. “What matters to class
15 certification . . . is not the raising of common ‘questions’—even in droves—but, rather the
16 capacity of a classwide proceeding to generate common answers apt to drive the
17 resolution of the litigation.” *Id.* (internal citation omitted, emphasis removed).

18 Here, commonality is satisfied because the “circumstances of each particular class
19 member . . . retain a common core of factual or legal issues with the rest of the class.”
20 *Evon v. Law Offices of Sidney Mickell*, 688 F.3d 1015, 1029 (9th Cir. 2012) (citations and
21 quotations omitted). Plaintiffs’ claims center on whether Vizio collected and shared what
22 Plaintiffs consider to be personally identifiable viewing data without consumers’
23 knowledge or consent. Because the core issues of Vizio’s nondisclosure and the collection
24 and sharing of viewing data is common to the claims, Plaintiffs have met their “minimal”
25 burden of demonstrating commonality. *See Astiana v. Kashi Co.*, 291 F.R.D. 493, 502 (C.D.
26 Cal. 2013).

27 ¹¹ Viewing data was not collected from a small percentage of SmartCast TVs during the
28 class period; however, it would be administratively difficult to exclude purchasers of such
TVs during the class period.

1 **c. Plaintiffs' Claims Are Typical of Those of the Class.**

2 “[R]epresentative claims are ‘typical’ [under Rule 23(a)(3)] if they are reasonably
3 coextensive with those of absent class members.” *Torres*, 835 F.3d at 1141. “Measures of
4 typicality include ‘whether other members have the same or similar injury, whether the
5 action is based on conduct which is not unique to the named plaintiffs, and whether other
6 class members have been injured in the same course of conduct.’” *Id.* (citation omitted).

7 Here, the claims of Plaintiffs and all class members arise out of the same course of
8 conduct—the alleged collection and sharing of personally identifiable viewing data
9 without consumers’ knowledge or consent—and assert the same theories of liability. As a
10 result, the typicality requirement is satisfied.

11 **d. Plaintiffs and Their Counsel Will Fairly and Adequately**
12 **Protect the Interests of Class Members.**

13 The test for evaluating adequacy of representation under Rule 23(a)(4) is: “(1) Do
14 the representative plaintiffs and their counsel have any conflicts of interest with other
15 class members; and (2) will the representative plaintiffs and their counsel prosecute the
16 action vigorously on behalf of the class?” *Staton*, 327 F.3d at 957.

17 In this instance, there is no conflict between Plaintiffs and the settlement class
18 members. Plaintiffs were allegedly harmed in the same way as all class members when
19 their personally identifiable viewing data was collected without their consent or
20 knowledge. In light of this common injury, the named Plaintiffs have every incentive to
21 vigorously pursue the class claims. And in fact, each has done so: Plaintiffs have made
22 important contributions to the case, including by preparing and sitting for depositions.
23 Each Plaintiff has agreed to undertake the responsibilities of serving as a class
24 representative, and each has sworn that he or she will continue to act in the class
25 members’ best interests.

26 Class counsel likewise are qualified to continue representing the class. The Court
27 appointed us as interim co-lead class counsel because of our experience in data privacy
28 and consumer class actions. Since then, this Court and Magistrate Judge Scott have had an

1 opportunity to review class counsel’s written work and oral presentations, including the
2 work of Andre Mura and Adam Zapala. The results obtained in the course of litigation
3 and settlement negotiations confirm counsel’s adequacy.

4 **2. Rule 23(b)(3) Is Satisfied.**

5 **a. Common Questions of Fact and Law Predominate.**

6 Predominance analysis under Rule 23(b)(3) “focuses on the relationship between
7 the common and individual issues in the case, and tests whether the proposed class is
8 sufficiently cohesive” *Ehret v. Uber Techs., Inc.*, 148 F. Supp. 3d 884, 894-95 (N.D. Cal.
9 2015) (quoting *Abdullah v. U.S. Sec. Assocs.*, 731 F.3d 952, 964 (9th Cir. 2013)). “When a
10 proposed class challenges a uniform policy, the validity of that policy tends to be the
11 predominant issue in the litigation.” *Nicholson v. UTI Worldwide, Inc.*, No. 3:09-cv-722-JPG-
12 DGW, 2011 WL 1775726, at *7 (S.D. Ill. May 10, 2011) (citation omitted). Further, when
13 a settlement class is proposed, the manageability criteria of Rule 23(b)(3) do not apply.
14 *Amchem Prods. v. Windsor*, 521 U.S. 591, 620 (1997).

15 This case involves an alleged uniform policy of Vizio to equip its Smart TVs with
16 software that collects viewing data to license to third parties, in order to create an
17 additional revenue stream for Vizio. The common thread running through Plaintiffs’
18 federal privacy claims—the Video Privacy Protection Act, and the Wiretap Act—is that
19 Vizio allegedly collected (or intercepted) personally identifiable viewing data, without
20 consumers’ consent or knowledge, as this viewing data was communicated on the TV
21 screen.¹² Plaintiffs allege Vizio then licensed this sensitive viewing data to third parties—
22 along with information about their digital identities—thus allegedly enabling these third
23 parties to connect viewing data with individuals on a personal, or household, level.

24 Because the technology at issue operated uniformly across Vizio’s TVs, legal and
25

26 ¹² This is likewise a core allegation for Plaintiffs’ state-law privacy claims. These state laws
27 are closely related to federal privacy law. *See In re Vizio, Inc., Consumer Privacy Litig.*, 238 F.
28 Supp. 3d 1204, 1215 (C.D. Cal. 2017) (“Plaintiffs’ federal claims under the Wiretap Act
bear a ‘close relationship’ to the tort of invasion of privacy.”). Also, this allegation
addresses issues important to the consumer protection claims, which ask whether Vizio
adequately informed consumers of this data collection and licensing.

1 factual issues respecting collection and disclosure may be resolved for all in a single
2 adjudication. Issues of consent or knowledge may also be answered for all on a class-wide
3 basis, because arguably there is no evidence of any adequate disclosure of the collection of
4 viewing data during the class period. Consequently, central issues common to the class
5 predominate over any individual considerations that might arise.

6 Finally, because conditional certification of a single nationwide class is based on
7 violations of federal law, there can be no argument that differences in state law defeat
8 predominance.¹³ See *Gustafson v. BAC Home Loans Servicing, LP*, 294 F.R.D. 529, 544 (C.D.
9 Cal. 2013); see also *In re Mex. Money Transfer Litig.*, 267 F.3d 743, 747 (7th Cir. 2001) (class
10 representatives can meet the predominance requirement by limiting their legal theories to
11 aspects of law that are uniform).

12
13 **b. A Class Action Is the Superior Method for Resolving**
14 **These Claims.**

15 A class action is superior under Rule 23(b)(3) because it represents the only realistic
16 means through which purchasers of affected Smart TVs may obtain relief. See, e.g.,
17 *Valentino v. Carter-Wallace, Inc.*, 97 F.3d 1227, 1234 (9th Cir. 1996) (explaining that a class
18 action may be superior where “classwide litigation of common issues will reduce litigation
19 costs and promote greater efficiency”). Even assuming class members could recover
20 statutory damages, they nonetheless would lack an incentive to bring their own cases given
21 the high expert costs involved in litigating a case such as this concerning complex
22 technology. *Mullins v. Premier Nutrition Corp.*, No. 13-CV-01271-RS, 2016 WL 1535057, at
23

24 ¹³ Such an argument would fail on its own terms. “Variations in state law do not
25 necessarily preclude a 23(b)(3) action,” and would not do so here if conditional
26 certification of consumer claims were sought, because of “the commonality of substantive
27 law applicable to all class members.” *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1022 (9th Cir.
28 1998); *id.* at 1022-23 (concluding “the idiosyncratic differences between state consumer
protection laws are not sufficiently substantive to predominate over the shared claims”); *In re Hyundai And Kia Fuel Econ. Litig.*, 897 F.3d 1003, 1007 (9th Cir. 2018) (granting en banc review of this issue). In any event, here the issue is academic, because conditional certification of a nationwide class is based on federal law, which fully suffices for purposes of preliminary and final approval of this settlement.

*8 (N.D. Cal. Apr. 15, 2016) (“Cases, such as this, ‘where litigation costs dwarf potential recovery’ are paradigmatic examples of those well-suited for classwide prosecution.”) (quoting *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1023 (9th Cir. 1998)).

3. Appointment of Class Counsel Is Merited.

Under Rule 23(g), “a court that certifies a class must appoint class counsel.” Fed. R. Civ. P. 23(g). As discussed above in addressing the adequacy requirement of Rule 23(a), Eric Gibbs and Andre Mura of Gibbs Law Group LLP, and Joseph Cotchett and Adam Zapala of Cotchett, Pitre, McCarthy LLP, each possesses the necessary skill and expertise to ably represent the class, as each has to date. The Court should thus appoint these four lawyers as class counsel.

* * *

For all these reasons, the proposed settlement class merits provisional certification.

B. Preliminary Approval of the Settlement Is Warranted.

“To preliminarily approve a proposed class action settlement, Rule 23(e)(2) requires the Court to determine whether the proposed settlement is fair, reasonable, and adequate.” *Oda v. DeMarini Sports, Inc.*, No. 8:15-cv-2131-JLS-JCGx, slip op. at 13 (C.D. Cal. June 6, 2018) (Doc. 157) (citing Fed. R. Civ. P. 23(e)(2)). If preliminary approval is granted, the Court will examine many of the same procedural and substantive factors at the approval stage that it is now considering at this notice stage. *Id.*

“A proposed settlement that is ‘fair, adequate and free from collusion’ will pass judicial muster.” *In re Volkswagen “Clean Diesel” Mktg., Sales Practices, & Prod. Liab. Litig.*, 895 F.3d 597, 610 (9th Cir. 2018). “To determine whether a settlement agreement meets these standards, a district court must consider a number of factors, including: the strength of plaintiffs’ case; the risk, expense, complexity, and likely duration of further litigation; the risk of maintaining class action status throughout the trial; the amount offered in settlement; the extent of discovery completed, and the stage of the proceedings; the experience and views of counsel; the presence of a governmental participant; and the reaction of the class members to the proposed settlement.” *Staton*, 327 F.3d at 959

1 (internal citation and quotation marks omitted).

2 In addition, “[w]hen, as here, the settlement was negotiated before the district court
3 certified the class, ‘there is an even greater potential for a breach of fiduciary duty’ by class
4 counsel, so we require the district court to undertake an additional search for ‘more subtle
5 signs that class counsel have allowed pursuit of their own self-interests and that of certain
6 class members to infect the negotiations.’” *In re Volkswagen*, 895 F.3d at 610–11. “Such
7 signs include (1) when counsel receive a disproportionate distribution of the settlement,
8 (2) when the parties negotiate a clear sailing arrangement providing for the payment of
9 attorneys’ fees separate and apart from class funds, and (3) when the parties arrange for
10 fees not awarded to revert to defendants rather than be added to the class fund.” *Oda*, No.
11 8:15-cv-2131-JLS-JCGx, slip op. at 14 (citing *In re Bluetooth Headset Prod. Liab. Litig.*, 654
12 F.3d 935, 946-47 (9th Cir. 2011)).

13 The 2018 amendments to Rule 23(e) similarly require counsel to provide additional
14 information up front at the preliminary approval stage, so that the court can determine
15 whether it “will likely be able to [finally] approve” it. Duke Law School, *Implementing 2018*
16 *Amendments to Rule 23*, *supra*, at *2. This information must address the adequacy of class
17 representatives and class counsel; whether the settlement proposal was negotiated at arm’s
18 length; the relief provided to the class, in view of a variety of factors, including the costs,
19 risks, and delay of trial and appeal; the effectiveness of any proposed method of
20 distributing relief to the class, including the method of processing class-member claims;
21 the terms of any proposed award of attorney’s fees, including timing of payment; and any
22 agreement required to be identified under Rule 23(e)(3); and lastly whether the proposal
23 treats class members equitably relative to each other.

24 Ultimately, however, the factors are “guideposts. ‘The relative degree of importance
25 to be attached to any particular factor will depend upon . . . the unique facts and
26 circumstances presented by each individual case.’” *In re Volkswagen*, 895 F.3d at 611 (citing
27 *Officers for Justice v. Civil Serv. Comm’n of City & Cnty. of San Francisco*, 688 F.2d 615, 625 (9th
28 Cir. 1982). “Deciding whether a settlement is fair is ultimately an amalgam of delicate

1 balancing, gross approximations and rough justice,” that is “best left” to the sound
2 discretion of the trial judge. *Id.* (internal citation and quotation marks omitted).

3 Furthermore, “[a]t this preliminary stage and because Class Members will receive an
4 opportunity to be heard on the Settlement Agreement, a full fairness analysis is
5 unnecessary.” *Oda*, No. 8:15-cv-2131-JLS-JCGx, slip op. at 14 (citation and quotation
6 marks omitted). The 2018 amendments to Rule 23 do not change this law. Despite
7 requiring courts to ask whether a proposed settlement is likely to win final approval, the
8 preliminary approval standard remains “more lenient than the eventual standard required
9 to grant final approval.” Duke Law School, *Implementing 2018 Amendments to Rule 23, supra*,
10 at *2.

11 As such, “preliminary approval and notice of the settlement terms to the proposed
12 Class are appropriate where [1] the proposed settlement appears to be the product of
13 serious, informed, non-collusive negotiations, [2] has no obvious deficiencies, [3] does not
14 improperly grant preferential treatment to class representatives or segments of the class,
15 and [4] falls within the range of *possible* approval” *Oda*, No. 8:15-cv-2131-JLS-JCGx,
16 slip op. at 15 (citing *In re Tableware Antitrust Litig.*, 484 F. Supp. 2d 1078, 1079 (N.D. Cal.
17 2007) (emphasis supplied by *Oda*); *see also Acosta v. Trans Union*, LLC, 243 F.R.D. 377, 386
18 (C.D. Cal. 2007) (“To determine whether preliminary approval is appropriate, the
19 settlement need only be *potentially* fair, as the Court will make a final determination of its
20 adequacy at the hearing on the Final Approval, after such time as any party has had a
21 chance to object and/or opt out.”) (emphasis in original).

22 After evaluating the “lengthy but non-exhaustive list of [overlapping fairness]
23 factors,” *In re Volkswagen*, 895 F.3d at 610, the Court should preliminarily approve the
24 settlement agreement because it is fair, reasonable, and adequate, and will likely be granted
25 final approval.

26 **1. Strength of Plaintiffs’ Case**

27 As mentioned, the principal claims at issue here involve Vizio’s alleged collection
28 and licensing of viewing data without consumers’ knowledge or consent. The collection of

1 the content of this communication in real time (Wiretap Act) for purposes of licensing to
2 third parties (VPPA) without consumers' knowledge or consent (Wiretap, VPPA) are core
3 issues that unite Plaintiffs' federal privacy claims, and are similarly critical to the resolution
4 of Plaintiffs' state-law privacy claims (the scope of the intrusion and the sensitivity of the
5 information obtained) and consumer-protection claims (whether these practices were
6 adequately disclosed in marketing materials or privacy policies). If these legal theories were
7 proven at summary judgment or trial, Plaintiffs could theoretically be entitled to liquidated
8 or statutory damages under the VPPA or Wiretap Act, for \$2,500 and \$10,000,
9 respectively.¹⁴

10 Plaintiffs allege that the viewing data is sensitive and personally identifies them.
11 Vizio disputes the sensitive and personal nature of the data collected and shared. The
12 recent decision in *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 981 (9th Cir. 2017), throws a
13 wrench in the gears of Plaintiffs' case. There, the Ninth Circuit held that "personally
14 identifiable information" under the VPPA includes only information that readily permits
15 an ordinary person to identify a particular individual as having watched certain videos. *Id.*
16 at 985. This is a less forgiving legal standard than that applied by the First Circuit in
17 *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016), and adopted
18 by this Court: "whether a video tape service provider can escape liability for disclosures
19 that would reasonably and foreseeably result in identifying a specific person as watching a
20 particular program merely because an 'ordinary person' would not be able, on her own, to
21 identify the consumer." Order Denying Mot. for Interlocutory Appeal, Doc 224 at 12
22

23 ¹⁴ For almost the entire class period, the California wiretap act authorized a single \$5,000
24 award of statutory damages per individual, rather than an award per violation. *See Ramos v.*
25 *Capital One, N.A.*, No. 17-CV-00435-BLF, 2017 WL 3232488, at *5-7 (N.D. Cal. July 27,
26 2017), *appeal dismissed*, No. 17-16723, 2017 WL 5891737 (9th Cir. Nov. 14, 2017). Still,
27 because the elements of the federal and state wiretap claims are essentially the same, and
28 because these two laws arguably serve the same remedial purpose, courts applying
California law might not allow a California plaintiff to recover multiple statutory penalties
for the same wiretap. *See Los Angeles Cnty. Metro. Transp. Auth. v. Superior Court*, 123 Cal.
App. 4th 261, 267 (2004). We thus consider the federal Wiretap Act claim only, though it
hardly matters whether we consider only one wiretap act or both; either way, any such
award of statutory damages would be colossal and could never be recovered from Vizio.

1 n.4.¹⁵

2 Applied here, *Eichenberger*'s more restrictive standard for "personally identifiable
3 information" under the VPPA would be difficult to meet. Put simply, whether the
4 information Vizio discloses would require too much detective work for an ordinary
5 person to link an individual to viewing data is a factual matter that could be challenging
6 for Plaintiffs to establish under Ninth Circuit law. We say this recognizing that the Ninth
7 Circuit itself left the open the possibility that "modern technology may indeed alter—or
8 may already have altered—what qualifies under the statute" as personally identifiable. 876
9 F.3d at 986.

10 The Wiretap Act claim also raises issues of first impression in this circuit. The
11 statute authorizes "any person whose wire, oral, or electronic communication is
12 intercepted, disclosed, or intentionally used in violation of this chapter" to sue for
13 damages. 18 U.S.C. § 2520(a). Vizio has argued that it does not "intercept" any electronic
14 communications, and the messages it collects do not constitute the "contents" of an
15 electronic communication. Plaintiffs, in turn, believe there is favorable evidence
16 supporting the real-time nature of the interception of the contents of a communication.

17 Even so, whether information qualifies as having been "intercepted" within the
18 meaning of the Wiretap Act, if it is acquired simultaneously with its arrival on the Smart
19 TV, has not been established. The Ninth Circuit in *Konop v. Hawaiian Airlines* suggested in
20 dicta that the Wiretap Act might not be implicated by such facts, but it did not resolve the
21 issue. 302 F.3d 868, 878 (9th Cir. 2002).

22 This Court identified legal authority to support the view that such an acquisition
23 "satisfies the contemporaneous interception requirement." *In re Vizio*, 238 F. Supp. 3d at

24 ¹⁵ While *Yershov* sets forth a more forgiving legal standard, it was nonetheless
25 insurmountable in that case. See *Yershov*, Joint Stipulation of Dismissal With Prejudice,
26 Case No. 1:14-cv-13112-FDS (D. Mass. March 27, 2017) (Doc. 83 at 1) ("the Parties agree
27 that Plaintiff lacks sufficient evidence to support his allegation that Defendant violated the
28 Video Privacy Protection Act by 'disclosing his PII—in the form of the title of the videos
he watched [on the USA Today App], his unique Android ID, and his GPS coordinates—to
third party analytics company Adobe Systems Inc.' from which Adobe identified
Yershov and attributed his video viewing records to an individualized profile of Plaintiff
Yershov in its databases.") (brackets and internal quotation marks removed).

1 1226 (citing *United States v. Szymuszkiewicz*, 622 F.3d 701, 706 (7th Cir. 2010)). Plaintiffs
2 would defend that view. But *Szymuszkiewicz* has been criticized by a leading Fourth
3 Amendment scholar who claims the Seventh Circuit misread the Wiretap Act. Orin Kerr,
4 *The Perils of Interpreting Statutes With Multiple Remedial Schemes: A Comment on the Dicta in*
5 *United States v. Szymuszkiewicz*, The Volokh Conspiracy blog.¹⁶ The professor's arguments
6 have some force, so it is not free from doubt that Plaintiffs could prevail on their Wiretap
7 Act claim.¹⁷

8 As for Plaintiffs' remaining claims, their strength on the merits may largely turn on
9 whether consumers were adequately advised that their viewing data would be collected
10 and shared. The parties disagree on this point, because Plaintiffs believe there is evidence
11 that Vizio's disclosures in marketing materials and privacy policies during the class period
12 were inadequate.

13 In addition, the remaining claims may turn on whether the information collected is
14 deemed sensitive. This matters both for purposes of materiality under the consumer-
15 protection claims and the state privacy claims, which may be actionable when community
16 norms are violated. Again, the parties disagree on the degree of risk for these claims. If the
17 named Plaintiffs' negative reaction to Vizio's conduct is any indication, however,
18 likeminded jurors could resolve these factual questions favorably for Plaintiffs.

19 Finally, even if Plaintiffs are able to establish that Vizio violated these federal
20 privacy laws, "statutory damages are not to be awarded mechanically." *Campbell v. Facebook*
21 *Inc.*, 315 F.R.D. 250, 268 (N.D. Cal. 2016). The Wiretap Act, for instance, "makes the
22 decision of whether or not to award damages subject to the court's discretion." *DirecTV,*
23 *Inc. v. Huynh*, 2005 WL 5864467, at *8 (N.D.Cal. May 31, 2005), *aff'd*, 503 F.3d 847 (9th
24 Cir. 2007). This is apparent in the text of the Wiretap Act, "which was amended in 1986

25 _____
26 ¹⁶ <http://volokh.com/2010/09/10/the-perils-of-interpreting-statutes-with-multiple-remedial-schemes-a-comment-on-the-dicta-in-united-states-v-szymuszkiewicz/>.

27 ¹⁷ Citing *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1106 (9th Cir. 2014), Vizio has argued
28 that Wiretap Act claim should fail because the information Vizio collects from Smart TVs
does not constitute the "contents" of an electronic communication. Plaintiffs disagree
with Vizio's reading of *In re Zynga*.

1 to state that the court ‘may’ award damages, rather than stating that it ‘shall’ award
2 damages.” *Campbell*, 315 F.R.D. at 268. The Court’s “discretion is limited to deciding
3 whether to ‘either award the statutory sum or nothing at all,’ it ‘may not award any
4 amount between those two figures.’” *Id.* (quoting *Huynh*, 2005 WL 5864467, at *8).¹⁸

5 In authorizing liquidated damages under the VPPA, Congress employed similar
6 language—“The court may award . . . actual damages but not less than liquidated damages
7 in an amount of \$2,500,” or punitive damages, 18 U.S.C. § 2710(c)(2)—rather than
8 directing that a court “shall” award such damages. *See id.*

9 When exercising such discretion, courts consider “(1) whether the defendant
10 profited from his violation; (2) whether there was any evidence that the defendant actually
11 used his pirate access devices; (3) the extent of [plaintiff’s] financial harm; (4) the extent of
12 the defendant’s violation; (5) whether the defendant had a legitimate reason for his
13 actions; (6) whether an award of damages would serve a legitimate purpose; and (7)
14 whether the defendant was also subject to another judgment based on the same conduct.”
15 *Huynh*, 2005 WL 5864467 at *8.¹⁹ If this Court were to conclude that some or many class
16 members suffered little monetary harm from the collection and disclosure of viewing data,
17 it could conclude that any liquidated, statutory, or punitive damages would
18 disproportionately penalize Vizio.²⁰

19 For all these reasons, while aspects of Plaintiffs’ claims are strong, Plaintiffs may
20 face considerable headwinds in seeking to establish new law in these complex areas and to

21 ¹⁸ The \$10,000 lump sum for liquidated damages is limited to a single award per victim as
22 long as the violations are “interrelated and time compacted.” *Smoof v. United Transp. Union*,
246 F.3d 633, 642-645 (6th Cir. 2001).

23 ¹⁹ We see no sensible reason why such factors would not also be germane to the VPPA.

24 ²⁰ In *Campbell*, the court declined to certify a Rule 23(b)(3) litigation class because it
25 concluded that “sorting out those disproportionate damages awards would require
26 individualized analyses that would predominate over common ones.” 315 F.R.D. at 269.
27 Plaintiffs believe this analysis of predominance clashes with *Tyson Foods, Inc. v. Bonaphakeo*,
28 which recognized: “When one or more of the central issues in the action are common to
the class and can be said to predominate, the action may be considered proper under Rule
23(b)(3) even though other important matters will have to be tried separately, such as
damages or some affirmative defenses peculiar to some individual class members.” 136 S.
Ct. 1036, 1045 (2016) (internal quotation marks and citation omitted). Therefore, Plaintiffs
have not mentioned this case as posing a risk to class certification.

1 recover more in the way of monetary relief. *See also* Section IV.B.2 (explaining that further
2 litigation could extinguish Plaintiffs’ legal entitlement to, and ability to negotiate for,
3 injunctive relief). Overall, then, this factor weighs in favor of preliminary approval.

4 **2. Risk, Complexity, Costs, and Likely Duration of Further**
5 **Litigation, and Risk of Maintaining Class Certification**

6 This litigation is complex because it “involves several intricate technologies”; it is
7 risky because it requires Plaintiffs to establish new law; and it is expensive because it
8 requires intensive work by qualified experts familiar with the data industry, tracking
9 software, and privacy practices in the digital sphere. Order Denying Mot. for Interlocutory
10 Appeal, Doc. 224 at 5. Neither party is likely to accept a dispositive, adverse ruling
11 without an appeal. The litigation has been intensive to date, and would only become more
12 so, and increasingly costly, if litigation were to continue.

13 More critically, if this settlement is not approved, it is unlikely that further litigation
14 would lead to a better settlement. This is evident for two reasons. One, there is the risk
15 that Vizio will again seek to limit Plaintiffs’ injunctive relief based on its compliance with
16 the consent decree with the Federal Trade Commission. The Court previously denied such
17 a request by Vizio—an important ruling which allowed Plaintiffs to negotiate the
18 injunctive relief in this case. But it did so without prejudice, noting Vizio could yet satisfy
19 its “formidable burden” of demonstrating that “subsequent events make it absolutely clear
20 that the allegedly wrongful behavior could not reasonably be expected to recur.” *Friends of*
21 *the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 189 (2000) (citation
22 omitted).

23 Two, if Plaintiffs were to succeed in certifying a litigation class, Vizio would then
24 press the Court to “definitively adjudicate the enforceability of the arbitration agreement.”
25 Order Denying Mot. to Dismiss and Strike. The arbitration agreement that applies to such
26 class members does not, by its terms, permit class proceedings, and it does not allow the
27 arbitrator to award equitable relief. *See* Brinkman Decl., Exs. A-B, Docs. 142-3, 142-4.
28 Also, monetary relief in arbitration may be limited to actual damages. *Id.*

1 If either of these two events were to occur, Plaintiffs would be diminished in their
2 ability to negotiate settlement terms as favorable as those in the proposed settlement.

3 Costs will increase substantially if the litigation continues through class certification,
4 *Daubert* motions, summary judgment, trial, and appeals. Expert costs in particular would
5 be high. Plaintiffs have been judicious in their use of experts to date, but class certification
6 and trial will require considerable work by experts.

7 Plaintiffs do not see serious obstacles to obtaining and maintaining class
8 certification. Even so, Vizio would vigorously resist class certification, before this Court
9 and on appeal. Even a “small” risk that class certification is not achievable “weigh(s) in
10 favor of granting final approval, as the settlement would eliminate the risk.” *Vandervort v.*
11 *Balboa Capital Corp.*, 8 F. Supp. 3d 1200, 1206 (C.D. Cal. 2014).

12 This settlement, by comparison, “eliminates the risks inherent in certifying a class,
13 prevailing at trial, and withstanding any subsequent appeals, and it may provide the last
14 opportunity for class members to obtain” monetary and injunctive relief. *Oda*, No. 8:15-
15 cv-2131-JLS-JCGx, slip op. at 16. This factor therefore weights in favor of settlement
16 approval. *See Nat’l Rural Telecomms. Coop. v. DIRECTV, Inc.*, 221 F.R.D. 523, 526 (C.D.
17 Cal. 2004) (“In most situations, unless the settlement is clearly inadequate, its acceptance
18 and approval are preferable to lengthy and expensive litigation with uncertain results.”
19 (citation omitted)).

20 **3. Amount Offered in Settlement**

21 “To determine whether a settlement ‘falls within the range of possible approval,’
22 courts focus on ‘substantive fairness and adequacy’ and ‘consider plaintiffs’ expected
23 recovery balanced against the value of the settlement offer.’” *Schuchard v. Law Office of Rory*
24 *W. Clark*, No. 15-cv-01329-JSC, 2016 WL 232435, at *10 (N.D. Cal. Jan. 20, 2016)
25 (quoting *Tableware*, 484 F. Supp. 2d at 1080). “Immediate receipt of money through
26 settlement, even if lower than what could potentially be achieved through ultimate success
27 on the merits, has value to a class, especially when compared to risky and costly continued
28 litigation.” *In re LinkedIn User Privacy Litig.*, 309 F.R.D. 573, 587 (N.D. Cal. 2015).

1 The class benefits offered in this settlement—both monetary and injunctive
2 relief—represent an excellent outcome for the class. To begin, the settlement establishes a
3 cash fund of \$17,000,000. This is more than the revenue Vizio obtained from licensing
4 viewing data during the class period. *See* *Siu Decl.* ¶ 11. Plaintiffs’ expert calculates that
5 actual harm per consumer is in the range of \$0.78 and \$4.76. *See* *Egelman Rep.* at 12.
6 There are approximately 16 million class members. After payment of notice and
7 administration costs and any approved award of attorneys’ fees, costs, and service awards,
8 all funds remaining in the settlement fund will be distributed to the class (*i.e.*, “the net
9 settlement fund”).

10 In addition to the monetary benefits obtained through the settlement, Plaintiffs
11 have obtained extensive injunctive relief. Plaintiffs’ expert has opined that the value of the
12 injunctive relief is, conservatively, \$6 to \$8 million. *See* *Egelman Rep.* at 3, 12. Thus, even
13 assuming that 100 percent of the class submits a claim for payment from the Settlement
14 Fund, each member of the class would theoretically receive up to \$0.62 in direct
15 compensation (assuming \$10,000,000 in a Net Settlement Fund made available to 16
16 million class members), plus the value of injunctive relief per class member, which is
17 approximately \$0.50. Thus, in a scenario where 100 percent of the class make claims, each
18 class member would receive \$1.12 in settlement benefits, which is above 100 percent of
19 the damages a class member could expect to receive at trial at the lower bounded range of
20 the maximum amount recoverable. Assuming a more realistic claims rate of 5 percent—
21 which is still considered on the high end of claims rates for consumer class actions—
22 Plaintiffs estimate that the per class member recovery would be \$13.00 (\$12.50 from the
23 settlement fund and \$0.50 in injunctive relief). These amounts greatly exceed the
24 maximum value of actual harm per consumer, per TV.

25 Because Plaintiffs’ expert estimates that average damages for actual harm from the
26 collection and sharing of viewing data is between \$0.78 and \$4.76, the ranges that class
27 counsel anticipate as direct payment to class members represents a highly favorable
28 recovery on a per-TV basis. *See* *Egelman Rep.* at 12. And it is more favorable still once the

1 value of injunctive relief is considered, as it must be. *Cf. Lee v. Enter. Leasing Co.-W.*, No.
2 3:10-CV-00326-LRH, 2015 WL 2345540, at *5 n.5 (D. Nev. May 15, 2015) (“[T]he Ninth
3 Circuit considers the value available to the class in determining total value, rather than
4 merely the amount redeemed.”) (emphasis removed).

5 An examination of settlements in similar consumer privacy cases, where parties
6 pleaded claims for statutory damages under the VPPA or Wiretap Act, further confirms
7 the reasonableness of the proposed settlement in this case. *Perkins v LinkedIn*, which
8 concerned the collection and dissemination of user e-mails and address book contents,
9 settled for \$13 million. No. 5:13-cv-04303-LHK (N.D. Cal.), Doc. 134 at 4. *Google Referrer*
10 *Header Privacy Litigation*, which concerned the collection and use of users’ search terms,
11 settled for \$8.5 million. No. 5:10-cv-04809-EJD (N.D. Cal.), Doc. 85 at 10, *aff’d*, 869 F.3d
12 737 (2017), *cert. granted*, 138 S. Ct. 1697 (2018). *Sony Gaming Networks*, which concerned the
13 disclosure of Sony PlayStation account holder information, settled for \$15 million. No.
14 3:11-md-02258 (S.D. Cal.), Doc. 204-1 at 6-10. *In re Netflix Privacy Litigation*, which
15 concerned the collection and retention of users’ viewing and personal information, settled
16 for \$9 million plus injunctive relief valued at \$4.65 million. No. 5:11-cv-00379 (N.D. Cal.),
17 Doc. 256 at 10. *Fraley v. Facebook*, which concerned the collection of names and likenesses
18 for promotional purposes, settled for \$20 million. No. 3:11-cv-01726 (N.D. Cal.),
19 Doc. 359 at 5. And *Lane v. Facebook*, which concerned the public dissemination of
20 information about members’ online activities, settled for \$9.5 million. No. 5:08-cv-03845
21 (N.D. Cal.), Doc. 108 at 4.

22 Several of the settlements just mentioned—*In re Netflix*, *Google Referrer Header*, and
23 *Lane*—resolved the claims of significantly larger classes. The amounts achieved in those
24 settlements were so small per class member that courts concluded compensation could
25 not feasibly be distributed to class members, and thus directed funds to *cy pres* recipients.
26 This fact further confirms the reasonableness of the settlement benefits achieved in this
27 case.

28 The reasonableness of the settlement is further supported by the Declaration of

1 Wilda Siu, senior director of accounting at Vizio, Inc. In this declaration, Ms. Siu discusses
2 Vizio's financial position in relation to the settlement amount, and she confirms the
3 revenue received during the class period from the licensing of viewing data. This
4 evidentiary submission demonstrates that "the aggregate size of the settlement—and,
5 relatedly, each individual claimant's recovery—is fully supported by the reality of
6 Defendants' financial position." *Etter v. Thetford Corp.*, NO. SACV 13-00081-JLS (RNBx),
7 slip op. at 20 (C.D. Cal. Mar. 29, 2016) (Doc. 468) (order granting plaintiffs' renewed
8 motion for preliminary approval of class action settlement).

9 Finally, the amount of the settlement is fair in view of the claims released by
10 Plaintiffs and the class. Each class member will release claims that were or could have
11 been asserted in this action, and the release does not extend beyond the Vizio released
12 parties. Settlement § XVII.1. Because the release mirrors those that have won approval in
13 other similar cases, its scope supports the conclusion that the amount offered in this
14 settlement is fair. *See Hesse v. Sprint Corp.*, 598 F.3d 581, 590 (9th Cir. 2010) ("A settlement
15 agreement may preclude a party from bringing a related claim in the future even though
16 the claim was not presented and might not have been presentable in the class action, but
17 only where the released claim is based on the identical factual predicate as that underlying
18 the claims in the settled class action." (internal quotation marks and citation omitted)).

19 **4. Method of Distributing Relief**

20 The 2018 amendments to Rule 23 instruct that the effectiveness of any proposed
21 method of distributing relief to the class, including the method of processing class-
22 member claims, should be considered as part of the fairness inquiry. This factor supports
23 approval for several reasons.

24 For one, A.B. Data will distribute relief directly from the settlement fund to all
25 settlement class members who submit valid claims. The settlement class will have the
26 option to receive payment immediately through electronic payment systems (such as
27 PayPal) or by printed check.

28 For another, the claims process is not unduly demanding, burdensome, or

1 oppressive. A claimant need not submit a receipt but must state under oath that he or she
2 is a class member based on the objective criteria set forth in the class definition. *See*
3 Schachter Decl. ¶ 17.

4 Further, the claims process facilitates the filing of claims. Claimants can complete a
5 claim form on a website or on a paper form, and the case-specific website answers
6 frequently asked questions through a long-form notice and provides a toll-free telephone
7 number with an automated interactive voice response system.

8 Finally, the claims process will also deter unjustified claims and has appropriate
9 security for electronic payment methods. The e-mail notice will provide a unique pin that
10 is associated with an e-mail address. A.B. Data also employs fraud-detection techniques.
11 The electronic payment walls, in turn, are operated by the payment systems themselves,
12 such as PayPal, and thus have advanced security in place. The class member is simply
13 directed to the platforms of these systems. A.B. Data does not receive any log in or
14 password information.

15 For all these reasons, the method of distributing relief is reasonable and supports
16 preliminary approval.

17 **5. Attorneys' Fees and Costs, and Service Awards**

18 At this stage, courts do not formally consider whether to approve attorneys' fees or
19 service payments for named Plaintiffs. Nevertheless, in light of the amendments to Rule
20 23, we forecast the application for such payments.

21 In the Ninth Circuit, when the percentage-of-recovery method is employed, 25
22 percent of a common fund is a presumptively reasonable amount of attorneys' fees. *See In*
23 *re Bluetooth*, 654 F.3d at 942. Here, counsel will not ask for more than 25 percent of the
24 total value of the settlement for monetary *and* injunctive relief. *See Staton*, 327 F.3d at 974
25 ("where the value to individual class members of benefits deriving from injunctive relief
26 can be accurately ascertained [] courts [may] include such relief as part of the value of a
27 common fund for purposes of applying the percentage method of determining fees.").

28 Plaintiffs will seek service awards of \$5,000. This enhancement is set at the Ninth

Circuit’s benchmark award for representative plaintiffs. *See In re Online DVD-Rental Antitrust Litig.*, 779 F.3d 934, 947-48 (9th Cir. 2015). It is an appropriate enhancement in this case because the representative Plaintiffs actively participated in the litigation and sat for depositions, and because the cumulative awards sought will constitute a small fraction (0.18 percent) of the total settlement fund. *Rhom v. Thumbtack, Inc.*, No. 16-CV-02008-HSG, 2017 WL 4642409, at *8 (N.D. Cal. Oct. 17, 2017) (“A \$5,000 award also equals approximately 1–2% of the total settlement fund, which is consistent with other court-approved enhancements.”).

6. Stage of the Proceedings and Extent of Discovery Completed

In order to settle a class action, the parties must have “sufficient information to make an informed decision about settlement.” *Linney v. Cellular Alaska P’ship*, 151 F.3d 1234, 1239 (9th Cir. 1998). This information can be obtained through formal or informal discovery. *See Clesceri v. Beach City Investigations & Protective Servs., Inc.*, No. CV-10-3873-JLS (RZx), 2011 WL 320998, at *9 (C.D. Cal. Jan. 27, 2011).

Plaintiffs have engaged in extensive discovery, formally and informally, including the production and review of voluminous documents, interrogatories, depositions of all of the Plaintiffs, and one non-party deposition. Further, Plaintiffs took three Fed. R. Civ P. 30(b)(6) depositions of Vizio and served additional interrogatories in the course of crafting injunctive relief. During this period, Vizio also shared information memorializing business-practice changes that Vizio had made pursuant to its consent decree with the government. The report was provided to Plaintiffs under Fed. R. Evid. 408.

Plaintiffs consulted with leading technologists and privacy experts about the strengths and weaknesses of this case. What’s more, Plaintiffs’ legal theories were put to adversarial testing through two motions to dismiss, a motion for interlocutory appeal, and numerous discovery motions before Magistrate Judge Scott.

Although the parties are proposing to settle before class certification, they possess sufficient information to make an informed decision about the settlement. This factor, then, weighs in favor of granting preliminary approval.

1 **7. Support of Experienced Counsel**

2 “The recommendations of plaintiffs’ counsel should be given a presumption of
3 reasonableness.” *In re Omnivision Techs., Inc.*, 559 F. Supp. 2d 1036, 1043 (N.D. Cal. 2008)
4 (citation omitted). In fact, experienced counsel’s judgment in this respect carries
5 considerable weight. *See Nat’l Rural Telcoms. Coop. v. DIRECTV, Inc.*, 221 F.R.D. 523, 528
6 (C.D. Cal. 2004) (“‘Great weight’ is accorded to the recommendation of counsel, who are
7 most closely acquainted with the facts of the underlying litigation.”) (citation omitted).

8 Class counsel wholeheartedly endorse the settlement agreement as fair, reasonable,
9 and adequate. That endorsement is the product of arm’s length negotiations before a
10 former federal judge and following relevant discovery. The Court should therefore credit
11 counsel’s recommendation that the settlement warrants preliminary approval. *See Linney v.*
12 *Cellular Alaska P’ship*, Nos. C-96-3008 DLJ, 1997 WL 450064, at *5 (N.D. Cal. July 18,
13 1997), *aff’d*, 151 F.3d 1234 (9th Cir. 1998) (“The involvement of experienced class action
14 counsel and the fact that the settlement agreement was reached in arm’s length
15 negotiations, after relevant discovery had taken place create a presumption that the
16 agreement is fair.”).

17 **8. Positive Views of Class Members**

18 The named Plaintiffs have all submitted declarations summarizing their individual
19 views of the settlement. *See* Hodges Decl., Zufolo Decl., Walsh Decl., Rizzitello Decl.,
20 Thomson Decl., and Queenan Decl. All are excited by the benefits achieved for the class
21 and support settlement approval. As the views of other class members are known, the
22 Court may take them into account as well. At this stage, however, all indications are that
23 the class is reacting positively to the proposed settlement.

24 **9. No Signs of Collusion**

25 When, as here, a class settlement is reached before class certification, courts are
26 “particularly vigilant” in searching for signs of collusion. *In re Bluetooth*, 654 F.3d at 946–
27 47. Courts must look for explicit collusion and “more subtle signs that class counsel have
28 allowed pursuit of their own self-interests and that of certain class members to infect the

1 negotiations.” *Id.* at 947. Such signs include “when the parties arrange for fees not
2 awarded to revert to defendants rather than be added to the class fund,” disproportionate
3 distributions of settlement funds to counsel, and clear-sailing arrangements. *Id.*

4 There are no signs, explicit or subtle, of collusion between the parties here. First,
5 settlement funds will not revert to Vizio under any circumstances. Settlement funds will
6 go to class members, and the use of electronic payment methods will increase the chances
7 that even small dollar amounts can be distributed to the class. These payments will be
8 divided proportionally among purchasers per TV per household, and thus all class
9 members are treated equitably. The same may be said for the injunctive relief which
10 admits no distinctions among class members. The named Plaintiffs, moreover, have stated
11 under oath that they understand they are not legally entitled to any benefits other than
12 those available to all settlement class members.

13 Any amount that is not feasibly distributable to the class will be split by next-best
14 recipients. Plaintiffs propose that the next-best recipients should be: Electronic Privacy
15 Information Center, Privacy Rights Clearinghouse, and World Privacy Forum. Any
16 residual would be divided evenly. These organizations submitted applications in which
17 they explained how they would commit to use distributed funds in a specified way that
18 benefits the class or substantial portions of it and addresses issues related to the basis of
19 the lawsuit. And each was asked to confirm that the organization is independent of the
20 parties, their counsel, and the district court. The applications which Plaintiffs received are
21 being submitted to the Court so that it can independently determine the suitability of
22 these next-best recipients. *See* Joint Decl., Ex. 4. This process further confirms that there
23 is no collusion.

24 Second, there will not be a disproportionate distribution of the settlement fund to
25 counsel.

26 Third, under the settlement agreement, attorneys’ fees are to be awarded from the
27 settlement fund. Although Vizio informed Plaintiffs, after all material class settlement
28 benefits had been negotiated, that it would not oppose an application for fees that does

1 not exceed 33% of \$17,000,000, the settlement agreement explicitly says that the Court is
2 to determine the proportion of the settlement fund that will be awarded as attorneys' fees.
3 Thus, the agreement does not in any way affect the Court's "supervisory discretion" in
4 approving fees. *See Vandervort v. Balboa Capital Corp.*, 2013 WL 12123234, at *5 (C.D. Cal.
5 Nov. 20, 2013) (quoting *Staton*, 327 F.3d at 970).

6 The timing of the payment of attorneys' fees—shortly after the final approval of
7 fees by this Court—is not controversial, either. *Pelzer v. Vassalle*, 655 Fed. App'x 352, 365
8 (6th Cir. 2016) ("Quick-pay provisions are common.") (citing Brian T. Fitzpatrick, *The*
9 *End of Objector Blackmail?*, 62 Vand. L. Rev. 1623, 1643 (2009), which found over one-third
10 of federal class action settlement agreements in 2006 included quick-pay provisions);
11 *Brown v. Hain Celestial Group, Inc.*, 2016 WL 631880, at *10 (N.D. Cal. Feb. 17, 2016)
12 ("Courts . . . approve these 'quick pay' provisions routinely.") (citation omitted); *In re TFT-*
13 *LCD (Flat Panel) Antitrust Litig.*, 2011 WL 7575004, at *1 (N.D. Cal. Dec. 27, 2011) (same).

14 Lastly, there is no undisclosed agreement made in connection with the settlement
15 proposal.

16 For all these reasons, there is no cause for concern that the settlement is the
17 product of collusion.

18 * * *

19 Considering all these guideposts, the Court should preliminarily conclude that the
20 proposed settlement is fair, reasonable, and adequate, and likely to receive final approval.

21 **C. Approval of the Proposed Settlement Administrator**

22 Plaintiffs propose, and Vizio does not oppose, the appointment of A.B. Data, Ltd.
23 as settlement administrator. Documentation of A.B. Data's competence is included in the
24 Declaration of Eric Schacter, vice-president of this company. Notably, this Court has
25 previously approved of A.B. Data as a settlement administrator in another class action
26 settlement. *Munday v. Navy Federal Credit Union*, 2016 WL 7655796, at *9 (C.D. Cal. Sep. 15,
27 2016) (*Staton*, J.) (order granting renewed joint motion for preliminary approval of class
28 action settlement). For these reasons, the Court should appoint A.B. Data to serve in this

1 capacity in this case.²¹

2 **D. Preliminary Approval of Class Notice Form and Method**

3 Even as amended in 2018, Fed. R. Civ. P. 23(c)(b)(2) requires the “best notice that
4 is practicable under the circumstances, including individual notice to all members who can
5 be identified through reasonable effort” for certified (b)(3) litigation classes. S. Ct., *Proposed*
6 *Amendments to the Fed. R. Civ. P.*, at *6.²² The 2018 amendments apply the requirements of
7 subdivision (c)(2)(B) to the notice of class-action settlements for (b)(3) classes. The
8 settlement agreement contemplates a single, combined notice advising the class of the
9 proposed certification and settlement of (b)(3) classes under both Rule 23(e)(1) and
10 (c)(2)(B).

11 Rule 23(c)(2)(B) was amended because means of communication have evolved and
12 permitting notice by *electronic* means, including e-mails, digital media, and social media, may
13 provide the best practicable notice under the circumstances. Duke Law School,
14 *Implementing 2018 Amendments to Rule 23, supra*, Rules Appendix C, at *17-18.²³ Specifically,
15 the amended language expressly provides that notice can be made by one or a
16 combination of means, including “United States mail, electronic means, or other
17 appropriate means.” See S. Ct., *Proposed Amendments, supra*, at *6.

18 The Committee Note to amended Rule 23 advises: “Counsel should consider which
19 method or methods of giving notice will be most effective; simply assuming that the
20 ‘traditional’ methods are best may disregard contemporary communication realities.”
21 Duke Law School, *Implementing 2018 Amendments to Rule 23, supra*, Rules Appendix C, at
22 *19. Consistent with that directive, counsel for the parties and the settlement
23 administrator have carefully considered cost, customer preference, and effectiveness, in
24 determining the best practicable means of communicating the settlement benefits and
25

26 ²¹ Plaintiffs will apply for an award of costs to A.B. Data for settlement administration
concurrently with their application for attorneys’ fees and service payments.

27 ²² Available at https://www.fjc.gov/sites/default/files/materials/58/frcv18_5924.pdf.

28 ²³ Available at <https://judicialstudies.duke.edu/wp-content/uploads/2018/09/Class-Actions-Best-Practices-Final-Version.pdf>.

1 rights of exclusion (among other matters) to the class.

2 Vizio has communicated with its customers directly through affected TVs to
3 provide disclosures during and after the class period. Working with the settlement
4 administrator, the parties and the Court will know precisely the number of affected Smart
5 TVs which successfully display the on-screen notice.

6 The parties have a solid sense of the number of Smart TVs capable of displaying
7 the notice based upon the number of TVs which have communicated with Vizio's servers
8 within the last 3 months and 6 months. Based on these estimates, notice will be sent
9 through the Internet directly to approximately 6,000,000 Vizio TVs purchased by potential
10 Settlement Class Members. As such, the notice will effectively reach the class.

11 The notice will display three times for 45 seconds, unless the option to dismiss the
12 notice is selected, in which case it will display a second time but not a third time. The easy-
13 to-remember settlement website address—www.VizioTVsettlement.com—is displayed
14 prominently in the center of the screen and in large font. Because of the frequency of the
15 TV notice, there is assurance that the notice will actually come to the attention of the
16 class.

17 Lastly, the TV notice is informative, engaging, and easy to understand. And it
18 allows class members to learn of their rights and options, and to act on them by visiting
19 the settlement website.

20 In *Hinshaw v. Vizio*, the court preliminarily approved a class action settlement and
21 notice plan which authorized Vizio to display a class action notice on Vizio TVs, among
22 other notice. *See* No. 8:14-cv-00876-DOC (C.D. Cal.), Doc. 56 at § 7.3. Subsequently, the
23 court granted final approval. *Hinshaw*, Doc. 69 at 3-4. Under that notice plan, the TV
24 notice displayed a total of two times for 30 seconds unless the class member selected a
25 command button to remove it. *Hinshaw*, Doc. 56 at § 7.3.

26 The TV Notice presented in this case is superior in that it will display more
27 frequently for longer intervals. The TV Notice here also has the information demanded by
28 Rule 23(c)(B)(2). And in contrast with the *Hinshaw* TV notice, the text of which is

1 represented in a single font-size, the text in the TV notice here is formatted to enhance
2 class member engagement. We draw these comparisons not to diminish the TV Notice in
3 *Hinsshaw*, which satisfied Rule 23, but to explain the reasons why the design of the TV
4 Notice in this case will be particularly effective.

5 Notice is also accomplished through a combination of e-mail, and digital and print
6 media. Vizio has a large number of e-mail addresses. This reflects the manner in which
7 customers engage Vizio. It also reflects “contemporary communication realities” of this
8 particular demographic. Approximately 9,000,000 potential Settlement Class Members will
9 receive the notice via e-mail. A.B. Data implements certain best practices to increase
10 deliverability and bypass SPAM and junk filters and can verify the number of e-mails
11 successfully delivered.²⁴

12 Other forms of notice, such as the digital and print media campaign, will provide
13 more than adequate coverage in the event that the outreach of the e-mail and TV notice
14 reaches fewer settlement class members than estimated. Digital banners ads through the
15 Google Display Network, Facebook (which includes a settlement-specific Facebook page)
16 and Google AdWords/Search platforms will yield a minimum of 62 million impressions.
17 Utilizing the known contact information and demographics of the settlement class, the
18 digital banner ads will be specifically targeted to settlement class members and likely
19 settlement class members.

20 Notice of the proposed settlement will be sent to relevant state and federal
21 authorities per the terms of 28 U.S.C. § 1715(b) at least 90 days prior to the date for the
22 final fairness hearing. 28 U.S.C. § 1715(d). A declaration attesting to this fact will be
23 submitted to the Court.

24 Under Rule 23, the notice must include, in a manner that is understandable to
25 potential class members: “(i) the nature of the action; (ii) the definition of the class
26 certified; (iii) the class claims, issues, or defenses; (iv) that a class member may enter an

27 ²⁴ Plaintiffs have provided the Court with mock ups of the TV and e-mail notice, so that
28 the Court can review the notice in a similar manner in which it will be presented to the
class.

1 appearance through an attorney if the member so desires; (v) that the court will exclude
2 from the class any member who requests exclusion; (vi) the time and manner for
3 requesting exclusion; and (vii) the binding effect of a class judgment on members under
4 Rule 23(c)(3).” Fed. R. Civ. P. 23(c)(2)(B). This information is included in each of the
5 notices in language that is easy to understand.

6 Because the class notices and notice plan set forth in the settlement agreement
7 satisfy the requirements of due process and Federal Rule of Civil Procedure 23, and
8 provide the best notice practicable under the circumstances, the Court should direct the
9 parties and the Settlement Administrator to proceed with providing notice to settlement
10 class members pursuant to the terms of the settlement agreement and its order granting
11 preliminary approval.

12 **V. CONCLUSION**

13 For the foregoing reasons, Plaintiffs respectfully request that the Court enter the
14 proposed Preliminary Approval Order, thereby:

- 15 (1) preliminarily approving the proposed Settlement;
- 16 (2) provisionally certifying the proposed Settlement Class;
- 17 (3) appointing Plaintiffs as Class Representatives;
- 18 (4) appointing Class Counsel as Settlement Class Counsel;
- 19 (5) approving Plaintiffs’ proposed notice program and directing that the notice
20 be carried out under that program;
- 21 (6) appointing A.B. Data, Ltd. as Settlement Administrator and directing it to
22 carry out the duties and responsibilities stated in the Settlement;
- 23 (7) approving Electronic Privacy Information Center, Privacy Rights
24 Clearinghouse, and World Privacy Forum as next-best recipients of residual
25 funds that cannot feasibly be distributed to class members; and
- 26 (8) setting a Final Approval Hearing and certain other dates in connection with
27 the settlement approval process.

Respectfully submitted,

GIBBS LAW GROUP LLP

/s/ Andre M. Mura

Eric H. Gibbs
ehg@classlawgroup.com
Andre M. Mura
amm@classlawgroup.com
Linda Lam
lpl@classlawgroup.com
505 14th Street, Suite 1110
Oakland, CA 94612
Tel: (510) 350-9700
Fax: (510) 350-9701

COTCHETT, PITRE & MCCARTHY, LLP

/s/ Adam J. Zapala

Joseph W. Cotchett
jcotchett@cpmlegal.com
Adam J. Zapala
azapala@cpmlegal.com
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577

Interim Co-Lead Counsel for Plaintiffs

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION**

KYLE ZAK, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

BOSE CORP., a Delaware corporation,

Defendant.

Case No. 17-cv-2928

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Kyle Zak (“Zak” or “Plaintiff”) brings this Class Action Complaint and Demand for Jury Trial against Defendant Bose Corp. (“Bose” or “Defendant”) for secretly collecting, transmitting, and disclosing its customers’ private music and audio selections to third parties, including a data mining company. Plaintiff, for his Complaint, alleges as follows upon personal knowledge as to himself and his own acts and experiences, and as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Defendant Bose manufactures and sells high-end wireless headphones and speakers. To fully operate its wireless products, customers must download Defendant’s “Bose Connect” mobile application from the Apple App or Google Play stores and install it on their smartphones. With Bose Connect, customers can “pair” their smartphones with their Bose wireless products, which allows them to access and control their settings and features.

2. Unbeknownst to its customers, however, Defendant designed Bose Connect to (i) collect and record the titles of the music and audio files its customers choose to play through their Bose wireless products and (ii) transmit such data along with other personal identifiers to third-parties—including a data miner—without its customers’ knowledge or consent.

3. Though the data collected from its customers' smartphones is undoubtedly valuable to the company, Defendant's conduct demonstrates a wholesale disregard for consumer privacy rights and violates numerous state and federal laws.

4. Indeed, one's personal audio selections – including music, radio broadcast, Podcast, and lecture choices – provide an incredible amount of insight into his or her personality, behavior, political views, and personal identity. In fact, numerous scientific studies show that musical preferences reflect explicit characteristics such as age, personality, and values, and can likely even be used to identify people with autism spectrum conditions.¹ And that's just a small sampling of what can be learned from one's music preferences. When it comes other types of audio tracks, the personality, values, likes, dislikes, and preferences of the listener are more self-evident. For example, a person that listens to Muslim prayer services through his headphones or speakers is very likely a Muslim, a person that listens to the Ashamed, Confused, And In the Closet Podcast is very likely a homosexual in need of a support system, and a person that listens to The Body's HIV/AIDS Podcast is very likely an individual that has been diagnosed and is living with HIV or AIDS. None of Defendant's customers could have ever anticipated that these types of music and audio selections would be recorded and sent to, of all people, a third party data miner for analysis.

5. As such, Plaintiff brings this suit individually and on behalf of all others similarly situated and seeks (i) an injunction prohibiting Bose from collecting, transmitting, and disclosing consumers' music and audio selections, (ii) actual and statutory damages arising from the invasion of their privacy, and (iii) actual damages arising from their purchase of the Bose

¹ Greenberg DM, Baron-Cohen S, Stillwell DJ, Kosinski M, Rentfrow PJ (2015) Musical Preferences are Linked to Cognitive Styles. PLoS ONE 10(7): e0131151. <https://doi.org/10.1371/journal.pone.0131151>.

Wireless Products, including the return of the purchase price of the product and disgorgement of profits.

PARTIES

6. Plaintiff Kyle Zak is a natural person and a citizen of the State of Illinois.

7. Defendant Bose Corporation is a corporation organized and existing under the laws of the State of Delaware with its principal place of business located at The Mountain, Framingham, Massachusetts 01701.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over Plaintiff's claim under the Wiretap Act, 18 U.S.C. § 2510, a federal statute, and supplemental jurisdiction over Plaintiff's state law claims because they are so related to Plaintiff's federal claim that they form part of the same case or controversy under Article III of the United States Constitution. The Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (i) at least one member of the Class is a citizen of a different state than the Defendant, (ii) the amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and (iii) none of the exceptions under that subsection apply to this action.

9. This Court has personal jurisdiction over Defendant because it conducts business in the State of Illinois and because the events giving rise to this lawsuit occurred, in substantial part, in the State of Illinois.

10. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred, in substantial part, in this District and Plaintiff resides in this District.

COMMON FACTUAL ALLEGATIONS

A Brief Overview of Defendant Bose and The Bose Connect App

11. In 2016, Bose introduced a new feature for some of its products that enabled customers to remotely control certain Bose headphones and speakers from their smartphones, including the QuietComfort 35, SoundSport Wireless, Sound Sport Pulse Wireless, QuietControl 30, SoundLink Around-Ear Wireless Headphones II, and SoundLink Color II (“Bose Wireless Products”).

12. Bose customers could download Defendant’s proprietary Bose Connect app from the Apple App Store or the Google Play Store and install it on their smartphones to take advantage of this new remote control feature.

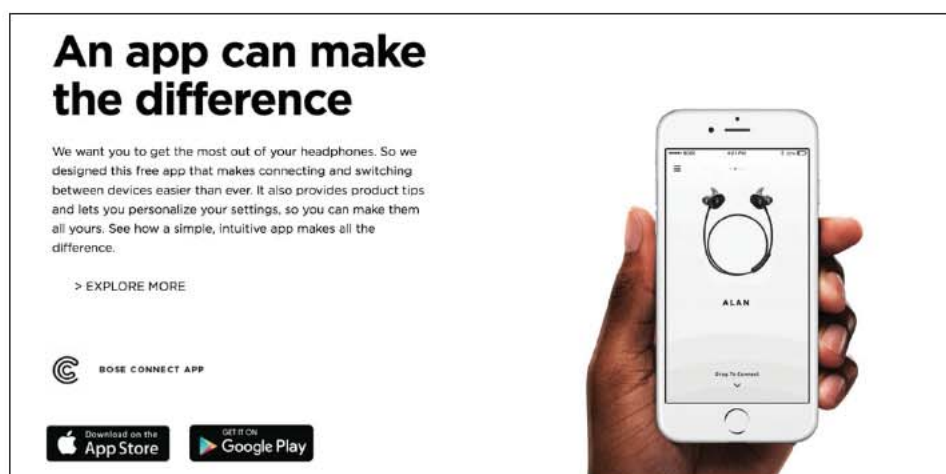
13. Once downloaded, the Bose Connect app allows customers to “pair” (i.e., connect) their Bose Wireless Products to their smartphones using a Bluetooth connection, and access essential product functionality. Specifically, through the Bose Connect app, customers can (i) download and install firmware updates to the Bose Wireless Products, (ii) manage the connections between the Bose Wireless Products and mobile devices, (iii) adjust the Bose Wireless Products’ noise cancellation settings, (iv) customize the Bose Wireless Products’ “Auto-Off” settings (for purposes of conserving the product’s battery life), and (v) share music between two Bose Wireless Products.²

14. Users can utilize the Bose Connect app to pause, resume, rewind, and skip songs already playing on their smartphones. The Bose Connect app is not a music player like the iTunes or Podcast players found on Apple devices—it is simply a companion app that allows customers to remotely control their Bose Wireless Products.

² *Bose Connect on the App Store*, <https://itunes.apple.com/us/app/bose-connect/id1046510029> (last visited April 18, 2017).

15. Defendant advertised the Bose Connect app functionality on the outside packaging of all Bose Wireless Products. For instance, the packaging of its SoundSport wireless headphones states in multiple languages: “[t]he Bose Connect app unlocks current and future headphone features. Download now.”

16. Likewise, Defendant touts the functionality Bose Connect on its website, and invites consumers to download the app to “get the most out of your headphones.” Defendant explains that Bose Connect “makes connecting and switching between devices easier than ever. It also provides product tips and lets you personalize your settings.” *See Figure 1.*



(Figure 1.)³

17. Defendant also encourages its customers to register their Bose Wireless Products with Bose. Registered product owners will receive “confirmation of ownership” and “important updates for products.”⁴ During product registration, consumers provide their Bose Wireless Product’s serial number, full name, email address, and phone number.

³ *QC35 Wireless Noise Cancelling Headphones* | Bose, https://www.bose.com/en_us/products/headphones/over_ear_headphones/quietcomfort-35-wireless.html (last visited April 18, 2017).

⁴ *Product registration*, https://www.bose.com/en_us/support/product_registration.html (last visited April 18, 2017).

Defendant Designed the Bose Connect App to Secretly Collect Consumers' Usage Data

18. As described above, customers must download and install Bose Connect to take advantage of the Bose Wireless Products' features and functions. Yet, Bose fails to notify or warn customers that Bose Connect monitors and collects—in real time—the music and audio tracks played through their Bose Wireless Products. Nor does Bose disclose that it transmits the collected listening data to third parties.

19. Indeed, Defendant programmed its Bose Connect app to continuously record the contents of the electronic communications that users send to their Bose Wireless Products from their smartphones, including the names of the music and audio tracks they select to play along with the corresponding artist and album information, together with the Bose Wireless Product's serial numbers (collectively, "Media Information").

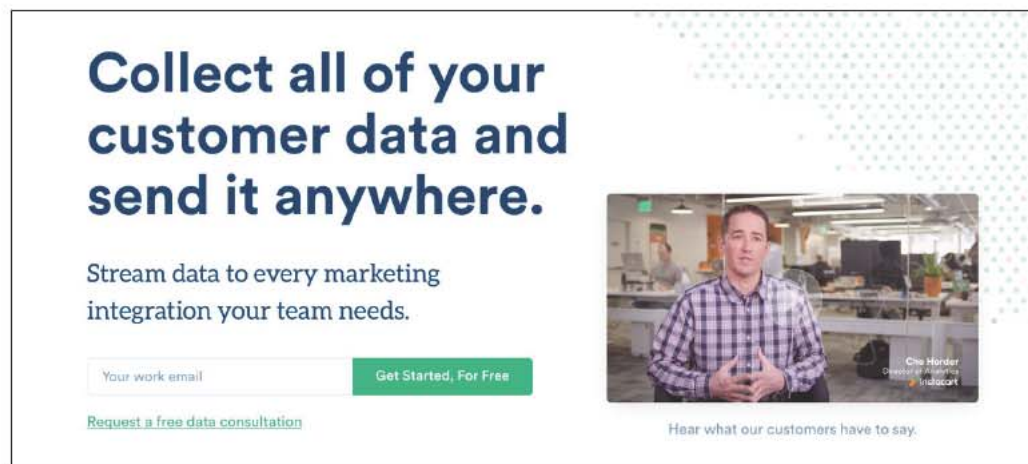
20. As mentioned above, Bose solicits registration information (name and email address) and collects that information with the product's serial number. And by collecting the Bose Wireless Products' serial numbers along with Media Information, Bose is able to link the Media Information to any individual that has registered or will register their products, thus enabling Bose to create detailed profiles about its users and their music listening histories and habits.

21. To collect customers' Media Information, Defendant designed and programmed Bose Connect to continuously and contemporaneously intercept the content of electronic communications that customers send to their Bose Wireless Products from their smartphones, such as operational instructions regarding the skipping and rewinding audio tracks and their corresponding titles. In other words, when a user interacted with Bose Connect to change their audio track, Defendant intercepted the content of those electronic communications.

22. Defendant also intentionally designed and programmed its Bose Connect app to automatically disclose and transmit its customers' Media Information to third party companies, including a data miner called Segment.io, Inc. ("Segment.io").

23. According to its homepage, Segment.io is a sophisticated data mining and analysis company that can be used to "Collect all of your customer data and send it anywhere."

See Figure 2.



(Figure 2.)⁵

24. The music and audio tracks that people listen to (i.e., Media Information) reveal sensitive information about themselves that suggests their politics, religious views, thoughts, sentiments, and emotions. In other words, knowing what music, radio broadcasts, lectures, and Podcasts a person chooses to listen to is enough to make accurate judgments and predictions about their personalities and behaviors.⁶

⁵ *Analytics API and Customer Data Platform | Segment*, <https://segment.com/> (last visited April 18, 2017).

⁶ *Music and Personality*, <https://www.verywell.com/music-and-personality-2795424> (last visited April 18, 2017) ("researchers found that people could make accurate judgments about an individual's levels of extraversion, creativity and open-mindedness after listening to ten of their favorite songs.")

25. Defendant never obtained consent from any of its customers before intercepting, monitoring, collecting, and transmitting their Media Information. To the contrary, Defendant concealed its actual data collection policies from its customers knowing that (i) a speaker or headphone product that monitors, collects, and transmits users' private music and audio tracks to any third party—let alone a data miner—is worth significantly less than a speaker or headphone product that does not, and (ii) few, if any, of its customers would have purchased a Bose Wireless Product in the first place had they known that it would monitor, collect, and transmit their Media Information.

FACTS SPECIFIC TO PLAINTIFF ZAK

26. On or around March 2017, Plaintiff Zak purchased Bose QuietComfort 35 wireless headphones for \$350.

27. Immediately after he purchased the headphones, Plaintiff registered his product with Bose and downloaded the Bose Connect app onto his smartphone in order to access the headphone's full array of features. During the registration process, Plaintiff provided Bose with his product's unique serial number, as well as his full name and email address.

28. Plaintiff uses his smartphone several times each day to select music tracks to play through his Bose wireless headphones, and often opens the Bose Connect app while such music is playing to configure the settings, access additional features, and to skip and pause audio tracks.

29. Unbeknownst to Plaintiff, each and every time he opened Bose Connect, Defendant intercepted and collected all available Media Information from his smartphone—including the names of any music and audio tracks he played through his wireless headphones and his personally identifiable serial number—and transmitted such information to third parties, including to data miner Segment.io.

30. Plaintiff Zak never provided his consent to Bose to monitor, collect, and transmit his Media Information. Nor did Plaintiff ever provide his consent to Bose to disclose his Media Information to any third party, let alone data miner Segment.io.

31. Likewise, Defendant never informed Plaintiff Zak that it would monitor, collect, transmit, and disclose his Media Information.

32. Plaintiff Zak would never have purchased his Bose Wireless Product had he known that Defendant would use Bose Connect (which was necessary to access the product's full array of functions and features) to collect, transmit, and disclose his Media Information.

CLASS ALLEGATIONS

33. **Class Definitions:** Plaintiff brings this action pursuant to the Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of himself and a class and subclass of similarly situated individuals as follows:

Class: All individuals in the United States who purchased a Bose Wireless Product and installed the Bose Connect mobile app.

Illinois Subclass: All members of the Class who are domiciled in the State of Illinois.

The following people are excluded from the Classes: (1) any Judge or Magistrate presiding over this action and the members of their family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

34. **Numerosity:** The exact number of members of the Classes is unknown, but

individual joinder in this case is impracticable. The Classes likely consist of tens of thousands of individuals. Members of the Classes can be easily identified through Defendant's records and/or Defendant's retail partners' records.

35. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include but are not limited to the following:

- (a) Whether Defendant's conduct constitutes a violation of the Wiretap Act;
- (b) Whether Defendant's conduct constitutes a violation of the Illinois Eavesdropping Statute;
- (c) Whether Defendant's conduct constitutes an intrusion upon seclusion;
- (d) Whether Defendant was unjustly enriched through its conduct; and
- (e) Whether Defendant's conduct constitutes a violation of the Illinois Consumer Fraud and Deceptive Business Practice Act.

36. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Classes in that Plaintiff and the members of the Classes sustained damages arising out of Defendant's uniform wrongful conduct.

37. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Classes, and they have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Classes.

38. **Superiority:** This class action is also appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. The damages suffered by the individual members of the Classes will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION
Violation of the Federal Wiretap Act
18 U.S.C. § 2510 *et seq.*
(On behalf of Plaintiff and the Class)

39. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

40. The Wiretap Act generally prohibits the intentional "interception" of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1)(a). The Act also prohibits the intentional disclosure of such communications. 18 U.S.C. § 2511(1)(c).

41. By designing the Bose Connect app to contemporaneously and secretly collect Media Information—including details about the music played by Plaintiff and the Class members—Defendant Bose intentionally intercepted and/or endeavored to intercept the contents of "electronic communications" in violation of 18 U.S.C. § 2511(1)(a).

42. Further, by automatically and contemporaneously transmitting and disclosing the content of an electronic communication it collected from Plaintiff and the Class members to a third-party company while knowing or having reason to know that the data was obtained through the interception of an electronic communication, Defendant violated 18 U.S.C. § 2511(1)(c).

43. No party to the electronic communications alleged herein consented to Defendant's collection, interception, use, or disclosure of the contents of the electronic communications. Nor could they—Defendant never sought to obtain Plaintiff's and the Class's consent, nor did Defendant obtain the consent of the other party, such as Spotify or other media providers. Moreover, Defendant was not a party to any of the electronic communications sent and/or received by Plaintiff and members of the Class.

44. Plaintiff and the Class suffered harm as a result of Defendant's violations of the Wiretap Act, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Violation of the Illinois Eavesdropping Statute
720 ILCS 5/14-1 *et seq.*
(On behalf of Plaintiff and the Illinois Subclass)

45. Plaintiff incorporates the foregoing allegation as if fully set forth herein.

46. A person violates the Illinois Eavesdropping Statute when he or she knowingly and intentionally “[i]ntercepts, records, or transcribes, in a surreptitious manner any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication. . . .” 720 ILCS 5/14-2(a).

47. The statute broadly defines “private electronic communication” to mean “any

transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation.” 720 ILCS 5/14-1(e).

48. By designing and programming the Bose Connect app to contemporaneously monitor, intercept, collect, record, transmit, and disclose the contents of private electronic communications that Plaintiff and the Illinois Subclass sent Bose Wireless Products and their smartphone operating systems—including the music and audio tracks they selected to play—Defendant intentionally and knowingly monitored, intercepted, collected, recorded, transmitted, and disclosed “private electronic communications,” in violation of 720 ILCS 5/14-2.

49. Plaintiff and the Illinois Subclass members intended that their Media Information would be private. Indeed, their Media Information reveals highly sensitive details about their private use of their personal headphones and speakers that Plaintiff and the Illinois Subclass expected to remain private and confidential. Beyond that, Defendant never notified Plaintiff and the Illinois Subclass that it was monitoring, intercepting, or disclosing their Media Information. Thus, there was no reason for them to believe that anybody could even potentially access, intercept, or disclose their private electronic communications in the first place.

50. Neither Plaintiff nor the members of the Illinois Subclass ever consented to Defendant’s interception, collection, recording, use, or disclosure of their private electronic communications.

51. As a result of Defendant’s unlawful conduct, Plaintiff and the members of the Illinois Subclass have been injured and seek: (1) an injunction prohibiting further eavesdropping by Defendant, (2) actual damages, including the amount paid for the Bose Wireless Products,

and (3) punitive damages in an amount to be determined by the court or by a jury pursuant to 720 ILCS 5/14-6(c).

THIRD CAUSE OF ACTION
Intrusion Upon Seclusion
(On behalf of Plaintiff and the Illinois Subclass)

52. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

53. As explained herein, Defendant has intruded upon the seclusion of Plaintiff and each member of the Illinois Subclass by secretly monitoring, collecting, transmitting, and disclosing their Media Information, which revealed specific details regarding their music and audio selections, preferences, and habits.

54. By designing and programming Bose Connect to secretly monitor, intercept, transmit, and disclose its customers' Media Information, Defendant intentionally and knowingly intruded upon the seclusion of Plaintiff's and Illinois Subclass members' private affairs.

55. Further, Defendant's monitoring, collection, transmission, and disclosure of Plaintiff's and Illinois Subclass members' Media Information—without their knowledge or consent—is highly offensive to a reasonable person as it is capable of revealing highly private details about their lives, including *inter alia* their personalities, behavior, and political affiliations and views, which they believed were confidential, and had no reason whatsoever to suspect that anybody would be spying on their music and audio selections.

56. Defendant's intrusion upon Plaintiff's and the Illinois Subclass members' privacy caused them to mental anguish and suffering in the form of anxiety and concern regarding the safety and whereabouts of their Media Information.

57. Plaintiff, on his own behalf and on behalf of the Illinois Subclass, seeks (1) an injunction that prohibits Defendant from monitoring, transmitting, or disclosing their Media

Information without informed consent, (2) actual damages, including the amount paid for the Bose Wireless Products, and (3) punitive damages, as well as for costs and reasonable attorneys' fees incurred.

FOURTH CAUSE OF ACTION
Violation of the Illinois Consumer Fraud and Deceptive Business Practice Act
815 ILCS 505/1 *et seq.*
(On behalf of Plaintiff and the Illinois Subclass)

58. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

59. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* ("ICFA") protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

60. The ICFA prohibits any unlawful, unfair, or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise, false advertising, misrepresentation, or the concealment, suppression, or omission of any material fact.

61. The ICFA applies to Defendant's conduct as described herein because it protects consumers in transactions that are intended to result, or which have resulted, in the sale of goods or services.

62. Defendant is a "person" as defined by 505/1(c) because it is a corporation.

63. Plaintiff and the Illinois Subclass members are "consumers" as defined by 505/1(e) because they purchased merchandise—the Bose Wireless Products—for their own use.

64. Defendant's Bose Wireless Products are "merchandise" as defined by 505/1(b) and their sale is considered "trade" or "commerce" under the ICFA.

65. Defendant violated the ICFA by concealing material facts about their Bose Wireless Products and the Bose Connect app. Specifically, Defendant omitted and concealed that Bose Connect secretly monitors, collects, transmits, and discloses its users' highly private and

sensitive Media Information to third parties, including data miners.

66. Defendant's data interception, collection, and disclosure practices are material to the transactions here. Defendant featured its Bose Connect app in its marketing and advertising, offered certain features and functions to customers that were only available through Bose Connect, and charged a higher price for its Bose Wireless Products relative to comparable, non-Bluetooth products. Had Plaintiff and the Illinois Subclass known the true characteristics and behavior of the device (that it collects, transmits, and discloses private usage data to third parties, including data miners), they would not have purchased the Bose Wireless Products or would have paid substantially less for them.

67. Defendant intentionally concealed the Bose Wireless Products' collection, transmission, and disclosure practices because it knew that consumers would not otherwise purchase their products. Indeed, Defendant's concealment of such facts was intended to mislead consumers.

68. Defendant's concealment, suppression, and omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the ICFA.

69. Thus, by failing to disclose and inform Plaintiff and the Illinois Subclass about its data collection practices, Defendant violated section 505/2 of the ICFA.

70. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each Illinois Subclass member has suffered actual harm in the form of money paid for a product that they would not have purchased had they known it would monitor, collect, transmit, and disclose Media Information to the third parties, including data miners.

71. As such, Plaintiff and the Illinois Subclass, seeks an order (1) requiring Defendant

to cease the unfair practices described herein, (2) awarding actual damages, including the amount paid for the Bose Wireless Products, and (3) awarding reasonable attorneys' fees and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On behalf of Plaintiff and the Class)

72. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

73. Plaintiff and the Class members conferred a benefit on to Defendant Bose when they purchased their Bose Wireless Products.

74. Defendant Bose appreciates and/or has knowledge of such benefit.

75. Given that Defendant monitored, collected, transmitted, and disclosed Plaintiff's and the Class's Media Information without their knowledge or consent—and because Plaintiff and the Class would never have purchased the product had they known that such information would be accessible and disclosed to third parties, including a data miner—Defendant has unjustly received and retained a benefit as a result of its conduct.

76. Principles of equity and good conscience require Bose to return the purchase price of the Bose Wireless Products to Plaintiff and the Class.

77. Plaintiff and the Class members seek disgorgement and restitution of any money received by Defendant as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Kyle Zak, on behalf of himself and the Class, and the Illinois Subclass requests that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Kyle Zak as a representative of the Classes, and appointing his counsel as class counsel;

B. Declaring that Defendant's actions violate the Wiretap Act, the Illinois Eavesdropping Statute, and the Illinois Consumer Fraud and Deceptive Business Practices Act, and that they constitute an Intrusion Upon Seclusion and Unjust Enrichment;

C. Awarding injunctive relief that (i) prohibits Defendant from collecting, monitoring, transmitting, or disclosing Plaintiff's and the Classes' Media Information without consent, and (ii) requires Defendant and any third parties with such information in their possession, including Segment.io, to destroy it immediately;

D. Awarding damages, including actual, statutory, and punitive damages, to Plaintiff and the Classes in an amount to be determined at trial;

E. Awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses;

F. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable;

G. Awarding such and other injunctive and declaratory relief as is necessary to protect the interests of Plaintiff and the Classes; and

H. Awarding such other and further relief as the Court deems reasonable and just.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: April 18, 2017

Respectfully submitted,

KYLE ZAK, individually and on behalf of
all other similarly situated,

By: /s/ Benjamin S. Thomassen
One of Plaintiff's Attorneys

Jay Edelson
jedelson@edelson.com
Benjamin S. Thomassen
bthomassen@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET AND TECHNOLOGY

In the Matter of

Assurance No. 17-056

**Investigation by ERIC T. SCHNEIDERMAN,
Attorney General of the State of New York, of**

**SAFETECH PRODUCTS, LLC, and RYAN HYDE, as an
individual,**

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to Executive Law § 63(12) and General Business Law (“GBL”) §§ 349 and 350 into the security of Safetech Products LLC, and its owner Ryan Hyde (“Respondents”), Bluetooth-enabled locks. This Assurance of Discontinuance (“Assurance”) contains the findings of the NYAG’s investigation and the relief agreed to by NYAG and Respondents.

FINDINGS OF NYAG

1. Safetech Products, LLC (“Safetech”) is a limited liability corporation with a principal place of business at 1601 North State Street, Lehi, Utah. It is owned by Ryan Hyde.
2. Safetech sells Bluetooth-enabled locks to customers through its website <https://www.thequicklock.com/> with the promise “Privacy When You Want It, Security When You Need It.” With Bluetooth-enabled locks, the user may control the locks with an application (“app”) installed on a smartphone.
3. Bluetooth is a wireless technology standard for exchanging data over short distances of up to 300 feet. It uses short-wavelength UHF radio waves in the ISM band from 2.4

to 2.485 GHz. To operate the Bluetooth-enabled lock, the smartphone and the lock must have their Bluetooth antennas turned on at the same frequency band and broadcast their identifiers to each other. A default password is used to secure the connection and exchange data.

4. In August 2016, independent security researchers reported that Respondents' Bluetooth-enabled locks transmitted passwords between the locks and the user's smartphone in plain text and without encryption. The researchers reported that a wrong-doer could intercept the passwords and proceed to unlock the locks. The researchers also reported that the locks contained weak default passwords that were not secure and could be guessed or discovered through brute force attacks (i.e., automated software used to generate a large number of consecutive guesses).

5. In October 2016, the NYAG contacted Respondents about the findings of the researchers and the security of the locks. Just prior to being contacted by the NYAG, Respondents voluntarily placed the following warning on the <https://www.thequicklock.com/> website:

SECURITY WARNING...Bluetooth keys for the hardware are passed
"unencrypted" on all current products.

We also strongly recommend the default password be changed at initial
setup. Please read "Security Risks Explained."

Upon clicking the "Security Risks Explained" hyperlink, the user is taken to a webpage that explains the risks identified above.

6. Respondents' locks limited the Bluetooth range to approximately 50 feet. Thus, a wrongdoer would need to be in close proximity to the lock to intercept the Bluetooth passwords. Additionally, the locks shutdown for 2 minutes with two failed password attempts. Thus, a brute force attack would be limited by the locks 2-minute lock-out feature.

7. By violating express and implied representations of reasonable data security, Respondents violated New York Executive Law § 63(12) and New York General Business Law §§ 349 and 350.

PROSPECTIVE RELIEF

WHEREAS, Respondents admit NYAG Findings (1)-(6) above;

WHEREAS, NYAG is willing to accept the terms of this Assurance pursuant to Executive Law § 63(15) and to discontinue its investigation into Respondents' representations concerning the security of its Bluetooth-enabled locks; and

WHEREAS, the parties each believe that the obligations imposed by this Assurance are prudent and appropriate;

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the parties, that:

8. This Assurance shall apply to Respondent Safetech Products LLC, and any officers, directors, servants, agents, employees, assignees, and any individual, subsidiary, division, or other entity through which the company may now or hereafter act, as well as any successors-in-interest, and Ryan Hyde, as an individual.

9. Respondents shall comply with Executive Law § 63(12), and GBL §§ 349 and 350, and shall not misrepresent, expressly or by implication, the security of its locks, or the security, confidentiality, or integrity of any data these devices transmit via Bluetooth or other radio frequencies.

10. Respondents shall encrypt all passwords, electronic keys or other credentials ("Security Information") in their locks and other Bluetooth-enabled devices that Respondents market or sell to individual consumers and the general public. Respondents' Bluetooth-enabled

devices shall prompt users to change the default password upon the customer's initial setup of wireless communication.

11. Within 30 days of the execution of this Assurance, Respondents shall establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing devices that use Security Information, and (2) protect the privacy, security, confidentiality, and integrity of Security Information. Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards appropriate to company's size and complexity, the nature and scope of the company's activities, and the sensitivity of the device's function or the information it collects, transmits or processes, including:

- a. The designation of an employee or employees to coordinate and be accountable for the security program;
- b. The identification of material internal and external risks to (1) the security of the devices that could result in unauthorized access to or unauthorized modification of the device and (2) the privacy, security, confidentiality, and integrity of Security Information;
- c. The risk assessments required by subpart b must include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing; (4) review, assessment, and response to third party security vulnerability

reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

- d. The design and implementation of reasonable safeguards to control the risks identified through risk assessment;
- e. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures including reasonable and appropriate security testing techniques such as vulnerability and penetration testing, security architecture reviews and code reviews;
- f. The development and use of reasonable steps to select and retain service providers (if any are hired) capable of maintaining security practices consistent with this Assurance, and requiring service providers by contract to implement and maintain appropriate safeguards consistent with this Assurance; and
- g. The evaluation and adjustment of Respondents' security program in light of the results of the testing and monitoring required by subpart e, any material changes to Respondents' operations or business arrangements, or any other circumstances that Respondents' knows or has reason to know may have a material impact on the effectiveness of the security program.

12. Respondents shall, within 10 business days of receiving a written request from NYAG, make available for NYAG review a copy of Respondents' written policies and procedures adopted pursuant to this Assurance or otherwise.

Miscellaneous

13. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondents and its counsel and NYAG's own factual

investigation as set forth in Findings (1)-(6) above. To the extent that any of Respondents' representations are later found to be inaccurate or misleading, this Assurance is voidable by the NYAG in its sole discretion.

14. If the Assurance is voided or breached, Respondents agree that any statute of limitations or other time-related defenses applicable to the subject of the Assurance and any claims arising from or relating thereto are tolled from and after the date of this Assurance. In the event the Assurance is voided or breached, Respondents expressly agree and acknowledge that this Assurance shall in no way bar or otherwise preclude NYAG from commencing, conducting or prosecuting any investigation, action or proceeding, however denominated, related to the Assurance, against the Respondents, or from using in any way any statements, documents or other materials produced or provided by Respondents prior to or after the date of this Assurance.

15. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondents in agreeing to this Assurance.

16. Respondents represent and warrant, through the signatures below, that the terms and conditions of this Assurance are duly approved, and execution of this Assurance is duly authorized. Respondents shall not take any action or make any statement denying, directly or indirectly, the propriety of this Assurance or expressing the view that this Assurance is without factual basis. Nothing in this paragraph affects Respondents' (i) testimonial obligations or (ii) right to take legal or factual positions in defense of litigation or other legal proceedings to which NYAG is not a party. This Assurance may not be used and is not intended for use by any third party in any other proceeding.

17. This Assurance may not be amended except by an instrument in writing signed on

behalf of all the parties to this Assurance.

18. This Assurance shall be binding on and inure to the benefit of the parties to this Assurance and their respective successors and assigns, provided that no party, other than NYAG, may assign, delegate, or otherwise transfer any of his rights or obligations under this Assurance without the prior written consent of NYAG.

19. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the NYAG such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

20. To the extent not already provided under this Assurance, Respondents shall, upon request by NYAG, provide documentation and information necessary for NYAG to verify compliance with this Assurance.

21. All notices, reports, requests, and other communications to any party pursuant to this Assurance shall be in writing and shall be directed as follows:

If to Respondents:

SafeTech Products, LLC
TheQuickLock LLC
1601 North State Street]
Lehi, Utah 84043

If to the NYAG, to:

Attorney General of the State of New York
120 Broadway
New York, New York 10271
Attention: Chief, Bureau of Internet and Technology

22. Acceptance of this Assurance by NYAG shall not be deemed approval by NYAG of any of the practices or procedures referenced herein, and Respondents shall make no

representation to the contrary.

23. Pursuant to Executive Law § 63(15), evidence of a violation of this Assurance shall constitute *prima facie* proof of violation of the applicable law in any action or proceeding thereafter commenced by NYAG.

24. If a court of competent jurisdiction determines that Respondents have breached this Assurance, Respondents shall pay to NYAG the cost, if any, of such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

25. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. The NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding.

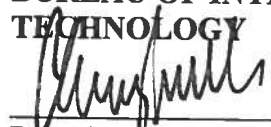
26. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

27. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

28. This Assurance may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

**ERIC T. SCHNEIDERMAN
NEW YORK ATTORNEY GENERAL
BUREAU OF INTERNET AND
TECHNOLOGY**


By: Clark Russell
Deputy Bureau Chief

5/9/17
Date

**SAFETECH PRODUCTS LLC AND RYAN
HYDE**


By:

May 3, 2017
Date

New York Attorney General's Office
120 Broadway
New York, NY 10271-0332
Phone: (212) 416-8433
Fax: (212) 416-8369

Expert Analysis

How The GDPR Changed Data Privacy In 2018

By **Jessica Lee**

December 14, 2018, 2:47 PM EST

The [European Union General Data Protection Regulation](#) became enforceable on May 25, 2018, bringing in a flurry of privacy notice updates, the shutdown of certain EU-facing websites and advertising activities, and a good amount of heartburn for companies within its territorial scope.

The threat of fines of up to 4 percent of a company's global revenue put a new spotlight on privacy and data protection, and caused a level of panic that was reminiscent of Y2K. Unlike Y2K, however, the road to GDPR compliance will extend well beyond its enforcement date.



Jessica Lee

What's Happened Since May?

In the past six months, compliance with the GDPR has moved from concept to reality, and both private citizens and data protection authorities, or DPAs, have taken action to enforce its requirements. Data subjects (individuals located in Europe) have started to enforce their rights, and DPAs have reported an increase in individual complaints.

Outside Europe, other countries have started to pass laws that mirror the GDPR's requirements, suggesting that at least some elements of the law may be our new global standard for privacy.

Enforcement Activity

As expected, tech companies have been among the first targets of GDPR enforcement activity. NOYB, a European consumer rights organization founded by Max Schrems, filed four lawsuits[1] against major tech companies the day GDPR went into effect, challenging the companies' consent mechanisms, and arguing that asking users to accept a company's privacy policies in order to access services violates the requirement that consent be "freely given."

In September, Dr. Johnny Ryan, chief policy and industry relations officer of Brave, a web browser that blocks ads and website trackers, filed a complaint[2] with several DPAs, asking them to investigate certain ad tech companies for "data breaches" caused by behavioral advertising. According to the press release, "every time a person visits a website and is shown a 'behavioural' ad on a website, intimate personal data that describes each visitor ... is broadcast to tens or hundreds of companies ... in order to solicit potential advertisers' bids for the attention of the specific individual visiting the website. A data breach occurs because this broadcast, known as a 'bid request' in the online industry, fails to protect these

intimate data against unauthorized access.”

In late November, consumer groups across seven European countries filed complaints[3] against another major tech company, alleging that it does not have a lawful basis for processing location data, because its users are not given a real choice about how that data is used. DPAs in France and the United Kingdom have also issued warnings to several ad tech companies, challenging the consent mechanisms used for the collection of location data.

While fines have been issued, they have been limited. A €4,800 fine for illegal video surveillance activities and a €400,000 fine imposed on a hospital after employees illegally accessed patient data are among the few reported fines issued.[4] In Germany, a €20,000 fine was imposed on a social media platform after an investigation following a reported security breach revealed that the company stored user passwords in plain text. The violation of the obligation to guarantee the security of personal data under Article 32 (1)(a) of the GDPR, rather than the breach itself, was cited as the justification for the fine.[5]

Below are some lessons learned from enforcement activities of the past six months.

Warnings Before Fines — For Now

In many cases, DPAs have issued warning letters and notices, rather than fines. In July, for example, the U.K. Information Commissioner’s Office (U.K. ICO) issued an enforcement notice[6] to AggregateIQ Data Services Ltd., or AIQ, a Canadian data analytics firm. AIQ was hired to target ads at voters during the Brexit referendum campaign.

Although AIQ used data that was collected prior to May 25, it retained and processed data after that date without having a lawful basis to do so, and without providing adequate transparency. The U.K. ICO alleged that by using this data to target individuals with political advertising on social media, AIQ “processed personal data in a way that those individuals were not aware of, for purposes which they would not have expected, and without a lawful basis for that processing.” According to the [BBC](#), AIQ plans to appeal the notice.

Although these warnings have been issued to specific companies, all companies subject to the GDPR should take note. Companies that fail to adjust their practices to meet the standards articulated in these warnings could ultimately be subject to fines.

Beware of Data Subject Complaints

Responding to data subject requests is one of the key elements of GDPR compliance, and one of the greatest sources of risk — a data subject’s complaint may put a company on a DPA’s radar for enforcement. The CNIL (France’s DPA) reported that since May 2018, it has received over 3,000 complaints from individuals, and the Irish DPA also provided figures indicating that, as of July, it had logged 743 complaints.[7]

Prompted by a consumer complaint, the Irish Data Protection Commissioner recently initiated an investigation into t.co, [Twitter](#)’s link-shortening system. Twitter allegedly declined to provide t.co data in response to the consumer’s access request, arguing that to do so would require disproportionate effort.[8]

Provide Consumers a Choice Before Using Location Data for Advertising Purposes

Both regulators and consumer groups have focused on the use of location data in the warnings or complaints issued since May. In July, the CNIL announced[9] formal notice proceedings against Fidzup and Teemo — two mobile ad tech companies — for failing to obtain GDPR-compliant consent from individuals when processing their geolocation data for advertising purposes. (Teemo was also put on notice for retaining geolocation data for 13 months, which the CNIL said was too long to justify the purpose of targeted advertising.)

In each case, the individuals were asked to consent only to the collection of data by the mobile application, not the software development kit, or SDK. Additionally, the CNIL challenged the timing of the consent, finding that the SDK started to collect data upon installation of the app, before consent was obtained. In late October, a similar proceeding[10] was opened involving SingleSpot, another mobile ad tech company. All three proceedings have since been closed.[11]

Each company updated its practices to require its publisher partners to display a banner during the app installation process to give users the choice to opt in to any data collection. These banners inform users of the following: 1) the purpose of the data collection; 2) the identity of controllers receiving that data (accessible via hyperlink); 3) the data collected; and 4) the possibility of withdrawing consent at any time. Teemo also updated its data retention policies so that raw data is deleted after 30 days and aggregate data is deleted after 12 months.

Programmatic Advertising Survives, With New Restrictions

The IAB Europe's Transparency and Consent Framework, or TCF, a protocol for collecting consent and conveying it throughout the adtech ecosystem, is positioned to be the industry's most viable solution for consent management. That said, there continue to be some challenges, particularly in the context of programmatic advertising where the requirement to be "specific" about the various purposes for which data is being collected and the identity of the recipients makes it difficult to draft language that is clear and understandable enough to demonstrate that the consent is also "informed."

At the end of October, the CNIL issued a notice[12] to Vectaury, another mobile ad tech company, for its failure to obtain GDPR-compliant consent for its data processing activities. Vectaury collected data both through its SDK and through real-time bidding offers initially transmitted via auctions for advertising inventory. Vectaury retained the data it received through the bidding offers for use beyond responding to the bid. Although Vectaury implemented a consent management platform as part of the TCF, the CNIL found that the consent language failed to notify the users how their data would be used and who it would be shared with.

Small Companies Won't Escape Enforcement

It is worth noting that the initial actions by the U.K. ICO and CNIL have been directed towards small ad tech companies, confirming that it is the activity of a company, rather than its size, that will determine the likelihood of enforcement.

Legitimate Interests Remains Viable — For Now

In each of the cases involving the collection of geolocation data addressed by the CNIL, the company relied on consent as its lawful basis for processing data.

What has yet to be tested is whether, rather than trying to meet the stringent requirements for consent, ad tech companies may find a better path forward with another lawful basis, such as legitimate interests (at least for processing activities that don't involve sensitive or special categories of data).

Data Breach Reporting Has Increased and Individuals Have Exercised Their Rights

One of the key changes to European privacy law introduced by the GDPR is the 72 hour window for reporting personal data breaches. The CNIL reported[13] that since May 2018, it has received approximately seven data breach notifications a day involving 15 million individuals.

The Irish DPA also provided figures indicating that, as of July, it had logged 1,184 data breach notifications. According to [Microsoft](#),[14] over five million people from 200 countries have used Microsoft's new privacy tools to manage their data, and over two million of those requests came from the U.S.

New Guidance on Territorial Scope

The European Data Protection Board, or EDPB, which replaced the Article 29 Working Party as the body in charge of ensuring that the GDPR is applied consistently across the European Union, issued draft guidance[15] on territorial scope. The guidance attempts to clarify that the processing of personal data of individuals in the EU by non-EU companies does not trigger the application of the GDPR, as long as the processing is not related (1) to a specific offer directed at individuals in the EU or (2) to a monitoring of their behavior in the EU.

The draft reinforces previous guidance that the mere accessibility of a website in the EU does not, by itself, provide sufficient evidence to demonstrate the controller's or processor's intention to offer goods or services to an individual located in the EU. With respect to monitoring, the EDPB does not consider that merely any online collection or analysis of personal data of individuals in the EU would automatically count as "monitoring."

Instead, it will consider the controller's purpose for processing the data and, in particular, any subsequent behavioral analysis or profiling techniques involving that data. Comments to the guidelines are due by Jan. 18, 2019.

What's Next?

In the next three to six months, we expect to see more enforcement action (including fines) as the DPAs work their way through pending complaints. In the long term, we expect that more countries will follow Brazil, India and California in passing "GDPR-like" regulations.

More than ever, understanding your data collection, use, storage and deletion practices is crucial so that you are prepared for these and future regulatory developments. Below are a few points to consider as your company prepares for 2019.

Data Mapping

Companies that didn't conduct a data-mapping exercise may consider doing so in 2019. Understanding what data you have, where it is stored, how it is used and to whom it is disclosed will put your organization ahead of the curve in complying with any new privacy regulations.

Ongoing Privacy Assessments

Data protection impact assessments drafted 6 months ago may already be out of date. Implementing an ongoing privacy assessment program will help privacy and business teams work together to manage the privacy risks presented by new projects.

Monitor Enforcement

Use the enforcement actions as a check against your company's practices. Companies may avoid enforcement by learning the lessons imposed on others.

Examine Security Practices

While companies have some flexibility to determine what level of technical and organizational security practices are appropriate for the nature of the data they process, security practices should at least align with industry best practices.

Jessica B. Lee is a partner at [Loeb & Loeb LLP](#).

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] <https://noyb.eu/4complaints/>.

[2] <https://brave.com/adtech-data-breach-complaint>.

[3] <https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html>.

[4] <https://iapp.org/news/a/germanys-first-fine-under-the-gdpr-offers-enforcement-insights/>.

[5] Id.

[6] <https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf>.

[7] <https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application>.

[8] <http://fortune.com/2018/10/12/twitter-gdpr-investigation-tco-tracking/>.

[9] <https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire>.

[10] <https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-pour-absence-de-consentement-au-traitement-de-donnees-de>.

[11] <https://www.cnil.fr/fr/applications-mobiles-cloture-des-mises-en-demeure-lencontre-des-societes-fidzup-et-singlespot>.

[12] <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037594451&fastReqId=974682228&fastPos=2>.

[13] <https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application>.

[14] <https://blogs.microsoft.com/on-the-issues/2018/09/17/millions-use-microsofts-gdpr-privacy-tools-to-control-their-data-including-2-million-americans/>.

[15] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf.

Cybersecurity

WWW.NYLJ.COM

VOLUME 259—NO. 42

MONDAY, MARCH 5, 2018

The GDPR: A Silver Lining For Data Governance

BY JESSICA B. LEE

The countdown to the enforcement date of the EU General Data Protection Regulation (GDPR) has begun and it's becoming increasingly clear that many U.S. organizations are poised to be caught in its crosshairs. Organizations that offer goods or services in the EU (whether or not a payment is involved) or that monitor the behavior of individuals in the EU, will be subject to the GDPR's requirements whether or not they have a presence in the EU. For U.S. organizations that are being exposed to the EU's regulatory regime for the first time, panic may be setting in (if it hasn't already). Requirements around honoring expanded data subject rights, maintaining records of processing, documenting the legal basis for such processing, and complying with the new security breach notification requirements, among others, may be particularly challenging



for organizations that don't have well-developed data governance policies or centralized systems and databases.

The GDPR replaces the previous Data Protection Directive 95/46/EC (the Directive) as the governing privacy regulation in the EU. While key principles of data privacy addressed in the Directive remain largely the same, there are some significant policy changes, and, as a result, a fair amount of uncertainty about how the regulation will be enforced. With reports suggesting that many

organizations won't be "fully compliant" by May 25, 2018 (the GDPR's enforcement date), the next year or two may prove instructive as the first round of enforcement begins.

Although some will find this uncertainty frustrating, there may be a silver lining. Where the Directive included an obligation to notify supervisory authorities about an organization's processing activities, the GDPR allows organizations to document their own processing activities, determine if they are compliant with the specific

requirements, identify and mitigate any risks created by their data use, and ultimately hold themselves accountable for compliance. This emphasis on accountability and record keeping may actually help create the safety net needed to navigate the GDPR's grey areas. Organizations with a robust data governance program, that have a documented and considered approach to GDPR compliance, are much less likely to be at the front lines of GDPR enforcement, and certainly should not be subject to the highest fines (up to \$20 million or 4 percent of global annual turnover).

GDPR: Accountability For Risk-Based Approach

Article 5(2) of the GDPR introduces the accountability principle, which requires organizations that control the processing of personal data ("controllers") to demonstrate (read: document) compliance with the GDPR's principles relating to the processing of personal data (i.e., lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality). This notion of accountability is not new; it was included as a basic data protection principle in the OECD Guidelines in 1980 (and the most recent update in 2013) and has been incorporated in various forms in other international privacy regulations. However, previous iterations of the accountability principle were centered on assigning

responsibility or fault for failures in privacy compliance. Under the GDPR, accountability is recast as an obligation to establish a systematic and ongoing approach to privacy. In effect, it codifies the obligation to create a data governance program that incorporates the principle of privacy by design, using tools like privacy impact assessments to routinize data protection within an organization. More than just a mandate to create policy documents, the GDPR creates a regulatory environment under which privacy and data governance are forced to become a standard element of an organization's operations.

The GDPR replaces the previous Data Protection Directive 95/46/EC as the **governing privacy regulation in the EU.**

This principle of accountability must be viewed in the context of the GDPR's risk-based approach to privacy. Under Article 24 of the GDPR, controllers are required to assess the nature, scope, context and purpose of processing, and based on the risks presented: (1) implement appropriate technical and organizational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and (2) review and update those measures where necessary. Organizations are directed to take into account "the state of the art and the costs of implementation" and "the nature, scope, context, and

purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." The GDPR provides suggestions (although no mandates) for which measures might be considered "appropriate to the risk." The pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and the creation of a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing will provide a good start for organizations to start mapping out their compliance efforts.

DPIAs. Historically, national data protection authorities in Europe (DPAs) have recommended privacy impact assessments (PIAs), tools used to identify and mitigate privacy risks during the design-phase of a project, as an element of privacy by design. Under Article 35 of the GDPR, data protection impact assessments (DPIAs)—a more robust version of the PIA—are now mandatory when an organization is engaging in activities that pose a high risk to an individual's rights and freedoms. The DPIA presents an opportunity to demonstrate that safeguards have (hopefully) been integrated into an organization's data processing activities and that

the risks presented by a processing activity have been sufficiently mitigated

While the risks analysis itself is largely left in the hands of each organization, determinations that are wildly off-base may not be defensible. However, if an organization can justify its position, relying on industry practice or other guidance, even if regulators ultimately determine that additional measures were required, it may be able to avoid significant fines. Notably, the failure to complete a DPIA itself could result in fines of up to 10 million Euros or up to 2 percent of the total worldwide turnover of the preceding year.

Records of Processing. Under the Directive, organizations were obligated to notify and register processing activities with local DPAs. The GDPR eliminates this requirement and instead puts the burden on both controllers and processors to maintain an internal record of processing activities, which must be made available to DPAs upon request. These records must contain all of the following information: (1) the name and contact details of the controller and where applicable, the data protection office; (2) the purposes of the processing; (3) a description of the categories of data subjects and of the categories of personal data; (4) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; (5) the transfers of personal data to a third country or an international organization,

including the documentation of suitable safeguards; (6) the envisaged time limits for erasure of the different categories of data; and (7) a general description of the applied technical and organizational security measures. Where processing activities take place across a variety of disconnected business units, organizing these records may be challenging. Organizations will need to audit each of their business units and their corresponding systems and processes to determine their processing activities and consider moving to a more centralized system.

Next Steps: Preparing For May 25th and Beyond

Between now and May 25th, organizations should be focused on creating the processes and documents that will help tell the story of their GDPR compliance:

- Investigate and document the flow of data through your organization. Understand the sources of data the organization has control over, the systems or databases that data is stored in, the controls in place to protect that data, and how and when it's transmitted to third parties.
- Create records of processing and a process going forward for keeping those records up to date.
- Audit vendors and update agreements to include GDPR compliant provisions.
- Track the key requirements of the GDPR and document the data protection policies in place to address those obligations. Create a

procedure for data breach response, data retention, and responding to data subject requests.

- Create a DPIA process—including a system to determine when a DPIA is needed and the team in charge of completion.
- Create a schedule and process to periodically audit the effectiveness of your data governance program.
- Conduct annual privacy training for employees.

While the process of preparing for the GDPR may be lengthy and expensive, it may ultimately give information security and internal data governance teams the resources needed to more effectively and strategically manage an organization's data. And, as the GDPR creates affirmative obligations for controllers to vet third party vendors for compliance with the GDPR's obligations, being able to demonstrate compliance with the GDPR through a strong data governance program won't just be a required regulatory obligation; it may be a selling point that distinguishes you as an organization that is safe to do business with.

General Data Protection Regulation



© 2018 LOEB & LOEB LLP

The Questions We'll Answer Today

- What Is the GDPR and Why Is Everyone Concerned About the Risks?
 - How to Determine Whether the GDPR Applies to Your Business?
- How Will These New Rules Impact Your Ability to Engage in Data-Driven Advertising/Marketing?
 - What You Should Be Doing Between Now and May 2018?



What Is the General Data Protection Regulation (GDPR)?

- Europe's new framework for data protection
- Designed to harmonize data privacy laws across—it applies to ALL EU member states
- Expands current data protection requirements
 - Applies to all organizations that process the data of individuals in the EU
 - Expands the definition of personal information
 - Strengthens the data protection rights of individuals
- Includes security breach notification requirements for the first time
- Has no grandfather provision

*****Enforcement began on May 25, 2018*****



What Are the Risks Of Non-compliance?



Large Fines/ “Collective Redress”

Penalties for breaking the law can be up to 4% of a global enterprise’s annual revenue

Administrative Oversight and Engagement

Data protection authorities can order changes to your practices, and can demand significant reporting obligations

PR Damage

Privacy is viewed as a fundamental right in Europe; violations are taken seriously

Business Relationships

Damage to relationships with partners and clients who may view it as risky to do business with you

How to Determine If You're Within the Territorial Scope



Are you an EU company:

applies to companies with an "establishment" in the EU

Are you a non-EU company that:

offers products and services in Europe

processes personal data from Europe

monitors behavior of people in Europe

****the mere accessibility a website by individuals in the EU is insufficient.**

**** the use of a language or a currency generally used in one or more Member States in connection with ordering goods and services, or the mentioning of customers or users who are in the EU will indicate an intent to offer products/services in the EU.**

Do You Process Personal Data?

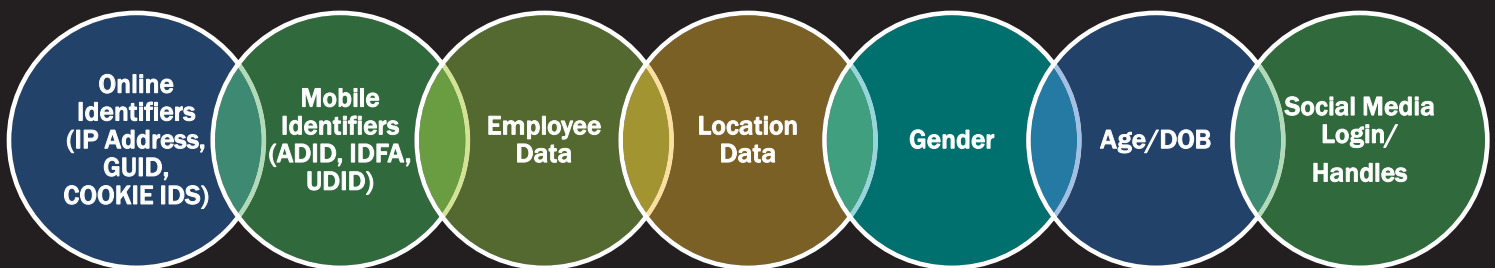
Processing

Includes: collection, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosure, transmission, and erasure

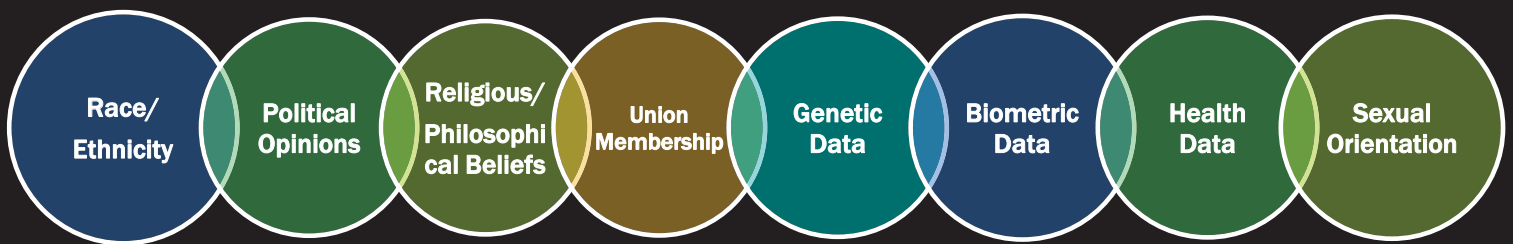
Personal Data

Includes: any information relating to an identified or identifiable natural person ("data subject"); includes name and address, but also location, online identifiers, social identity, description, image, and IP address

Personal Data Is More Than Name, Email or Phone Numbers...



Special/Sensitive Categories of Data Requires Special Treatment (Explicit Consent)



Can You Rely on “Anonymization”? Only If the Data Is Truly “Anonymized”

Pseudonymization

The separation of personal data from direct identifiers so that linkage to an identity is not possible without additional information.

The “*additional information*” must be “*kept separately and subject to technical and organizational security measures*”

Pseudonymized data is still personal data under the GDPR!

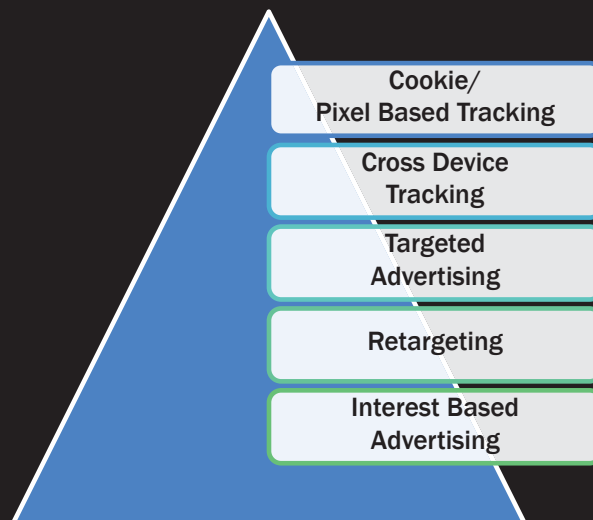
Data stripped of any identifiable information, making it impossible to re-identify.

Anonymized data is outside the scope of the GDPR!

Anonymization

Consider this: With only a few data points, it may be possible to identify a data subject, even without their name or home address.

Are You Engaging in Any Of These Activities?
If So, You May Be “Monitoring”



Data Protection Officers

- Some organizations must appoint a data protection officer (DPO)
- When to appoint a DPO:
 - Systematically monitor large groups of individuals
 - Carry out large-scale processing of special categories of data, including data related to criminal convictions and offences
- DPO responsibilities:
 - Actively monitor compliance with the GDPR
 - Provide advice on data impact assessments
 - Remain independent and report to “highest management level”



Data Breach Notification

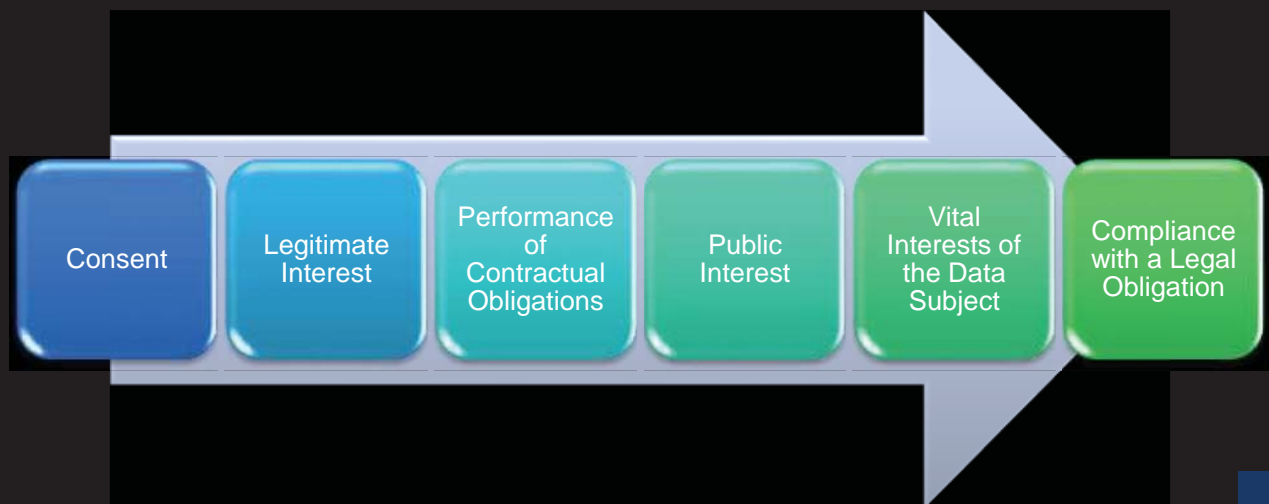
- **Breach Notification**
 - Notification to supervisory authority “without undue delay”
 - And, where feasible, not later than **72 hours** after becoming aware of the breach.
 - Notification to consumers in high risk situations



How Will These Rules Impact Your Data-driven Business?

Understand whether you have a lawful basis to process personal information

Under the GDPR, a Company Must Have a “Lawful Basis” to Process Personal Information



GDPR Mandates Affirmative Consent

Unambiguous

- A statement or clear affirmative action
- Silence, pre-ticked boxes and inactivity, will not constitute consent

Freely Given

Consent is not freely given if:

- The data subject has no genuine and free choice or is unable to refuse or withdraw consent without consequence
- The performance of a contract is made conditional on the data subject's consent
- Bundled with other consents

Informed

- Data subjects should understand the extent to which they are consenting and be aware, at least, of the identity of the controller and the purposes of the relevant processing

Specific

Consent must relate to specific processing operations:

- A general broad consent to unspecified processing operations will be invalid
- If data processing has multiple purposes, a consent should cover all those purposes

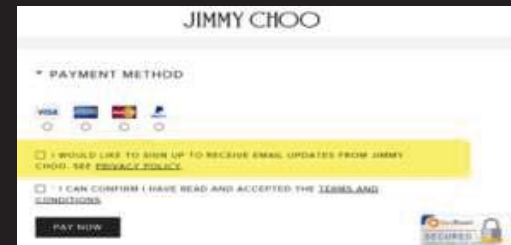
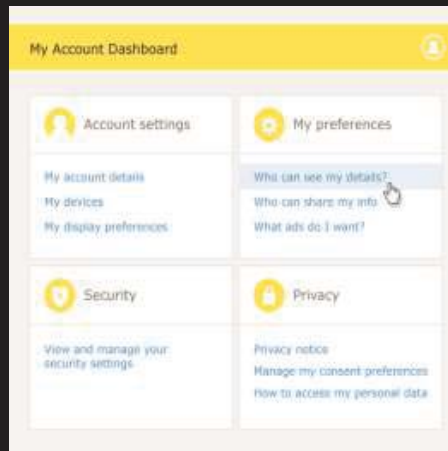
Explicit

Required for:

- Sensitive data
- Profiling activities
- Cross-border data transfers

What Does Unambiguous Consent Look Like?

- Signing a consent statement on a paper form
- Ticking box
- Selecting from equally prominent yes/no options
- Choosing technical settings or preference dashboard settings
- Responding to an email requesting consent
- Volunteering optional information for a specific purpose



Explicit Consent Requires a Direction Action

OK

Check an unchecked box
A radio button with a statement that clearly indicates assent

NOT OK


Silence/Inactivity
Pre-ticked box
Technical settings
Conditions

Checklist for Consent

- ☐ Is consent the most appropriate lawful basis for processing?
- ☐ Is the request for consent prominent and separate from the terms and conditions?
- ☐ Is consent given on an “opt-in” basis? (i.e. no pre-ticked boxes or consent by default)
- ☐ Is the consent written in clear, plain language that is easy to understand?
- ☐ Does the consent specify the scope of what is being collected and how it will be used?
- ☐ Is the individual given options to consent to independent processing operations? (e.g. emails, targeted ads, sharing with third parties)
- ☐ Do we provide the name of the company and any third party controllers who will be relying on the consent?
- ☐ Do we tell individuals they can withdraw their consent?
- ☐ Do we ensure that the individual can refuse to consent without detriment?
- ☐ Consent is not a precondition of a service.



Consent has limitations

- Consent can be revoked
 - Data subjects must be informed in advance that they can change their minds
 - Once consent is withdrawn, data subjects may ask to have their personal data erased and no longer used for processing.
- Consent is limited to the purpose for which it was collected
 - Consent for subsequent processing may not be required if the operations are “compatible”
 - Compatibility depends on:
 - ✓ the link between the processing purposes
 - ✓ the reasonable expectations of the data subject
 - ✓ the nature and consequences of further processing
 - ✓ the existence of appropriate safeguards for the data
- Must be able to demonstrate consent was obtained in compliance with the GDPR
-  Any consent already in place needs to be reviewed to meet GDPR standards

If Consent Isn't Available, Consider Whether You Can Establish a Legitimate Interest

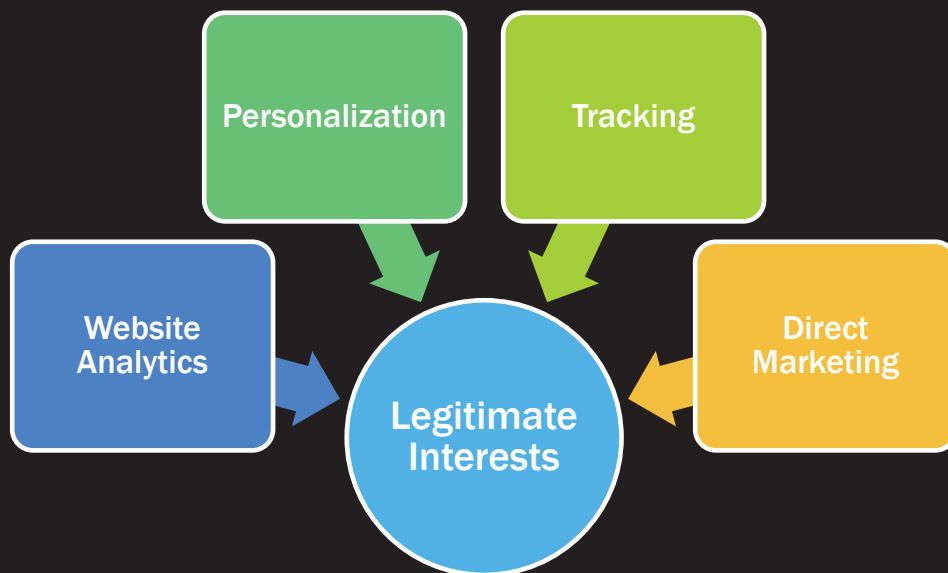
Legitimate Interest – 3 Part Test

- Identify the legitimate interest
 - Is it required to achieve a lawful business objective?
 - Consider all possible uses (including third party processing)
- Is it “necessary” ?
 - Be able to articulate why there is no other way to achieve the objective (or if alternative means would require disproportionate effort)
 - This may require a privacy impact assessment
- Balance your need against the consumer's interests
 - The rights and freedoms of the individual should not override the Legitimate Interest.

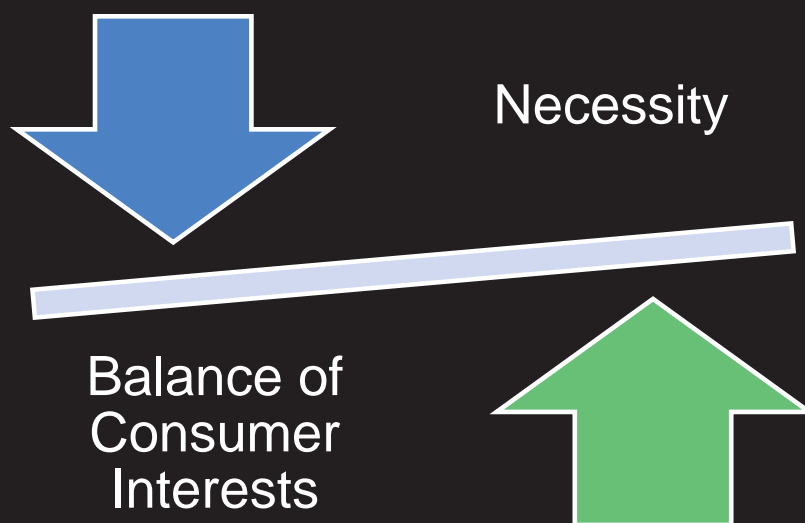
*** Legitimate Interests can be those of the Controller or a Third Party. A number of parties may have a Legitimate Interest in processing the Personal Data.*



These May Be Legitimate Interests



Do the Privacy Rights of The Data Subject Override the Need for the Processing?



Consider:

- ✓ The reasonable expectations of the individual
- ✓ The type of data (i.e. is additional protection required?)
- ✓ The benefit to the consumer
- ✓ The impact of processing
- ✓ Any safeguards which are or could be put in place

What Rights Do “Data Subjects” Have?

Right to Be Informed

- The data subject should be informed about what information is being collected, how it will be used, and the consequences of that use. The data subject should also be informed about the right to object or to request access, rectification or the erasure of the data (where applicable)

Right to Object

- The data subject has the right to object or withdraw consent to processing (including targeting/profiling) and avoid profiling-based decisions.

Right to Access

- The data subject has the right to obtain confirmation about what personal data a controller has and how it is being used, including whether it is being used for automated decision-making, and who it has been shared with. A data subject has a right to a copy of his/her data.

Right to Erasure/ Rectification

- If the basis for profiling is consent and consent is withdrawn, controllers must erase the relevant personal data, unless there is another legal basis for the profiling. If the data is inaccurate, data subjects have the right to request that it is rectified

What Other Principles Apply?

Purpose Limitation

- Data must be collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Compatibility of purposes depends on:
 - the relationship between the purposes
 - the context of the collection & reasonable expectations of the data subject
 - the nature of the data and the impact of the further processing
 - safeguards applied by the controller to ensure fair processing

Data Minimization

- Data minimization refers to the practice of limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose
- Don't collect data because "it might be useful in the future"
- Consider whether data can be anonymized for continued use

Memory Limitation

- Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Onboarding, Processing and Sharing Personal Information

Applying the Principles of the GDPR

What to Ask When Onboarding Data

- What type of data will you receive? (personal? sensitive? pseudonymized?)
- What consent was obtained when the data was initially collected?
- Can the data be used in the way you need to use it?
- What are the use cases, have those been clearly specified?
- Can the data be appended, merged, combined or aggregated with other data sets?
- Do you have promises/guarantees (reps and warranties) about the data ?



Processing Data: Special Rules For “Profiling”

What is profiling under the GDPR?

- Automated processing of personal data to evaluate certain personal aspects relating to a natural person
- Specific examples include: analyzing or predicting a person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements

PROFILING



TRACKING

- Profiling is the intention to ***make decisions*** regarding a data subject or ***analyze/predict*** the subject's behaviors and preferences.

Which of These Could Be Considered Profiling?

**CONTEXTUAL
ADVERTISING**



**BEHAVIORAL
RETARGETING**



**CREATING
AUDIENCE
SEGMENTS**



**INTEREST
BASED
ADVERTISING**



Special Rules for Automated Decision Making



Automated decision-making is the ability to make decisions by technological means without human involvement

- Prohibited (with exceptions) if it has a “Significant” or “Legal Effect”

Legal effects

- Has an impact on legal rights
- Affects a person's legal status
- Affects rights under a contract

Significant affects

- Must be more than trivial
- Must have the potential to significantly influence the circumstances, behavior or choices of individual
- Leads to discrimination

Examples: Automatic refusal of an on-line credit application or e-recruiting practices without any human intervention.

Data Subjects Have a Right Not to Be Subject to Automated Decision-making (“ADM”), Unless...

- These Exceptions Apply:
- ADM is necessary to enter a contract
- Explicit consent is given
- Authorized by Union or member state law, which includes suitable safeguards

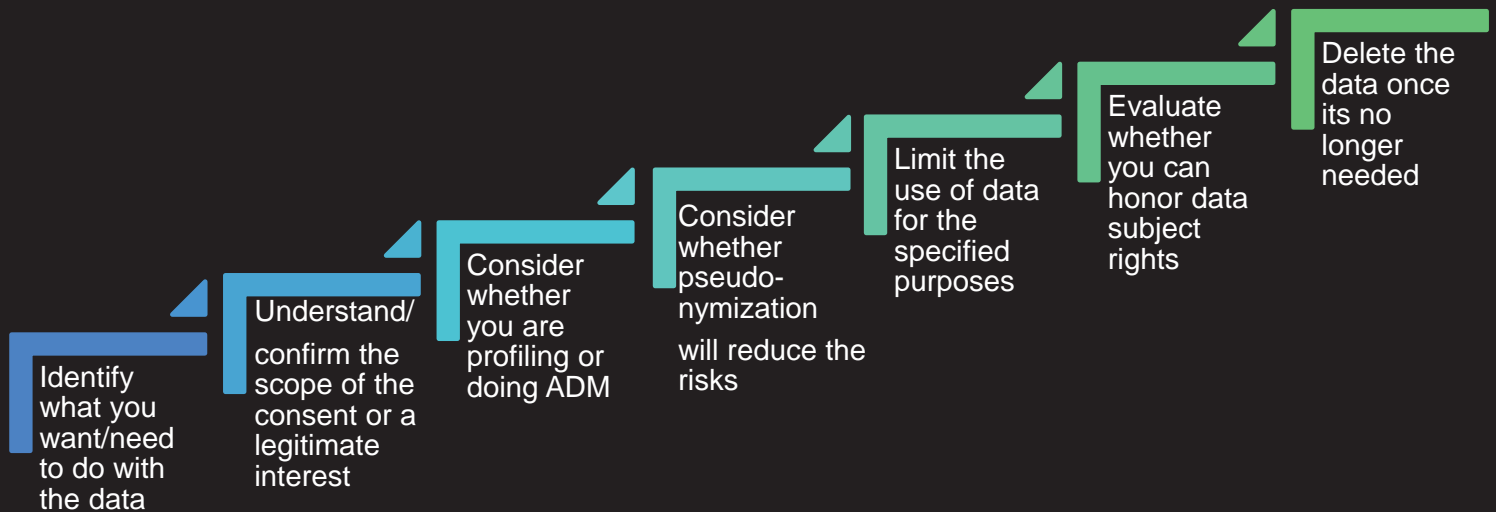


Safeguards MAY include anonymization or [pseudonymization](#)

Consider:

- The intrusiveness of the profiling
- The expectations of the data subject
- The right to challenge the decision

Consider These Steps Prior to Processing

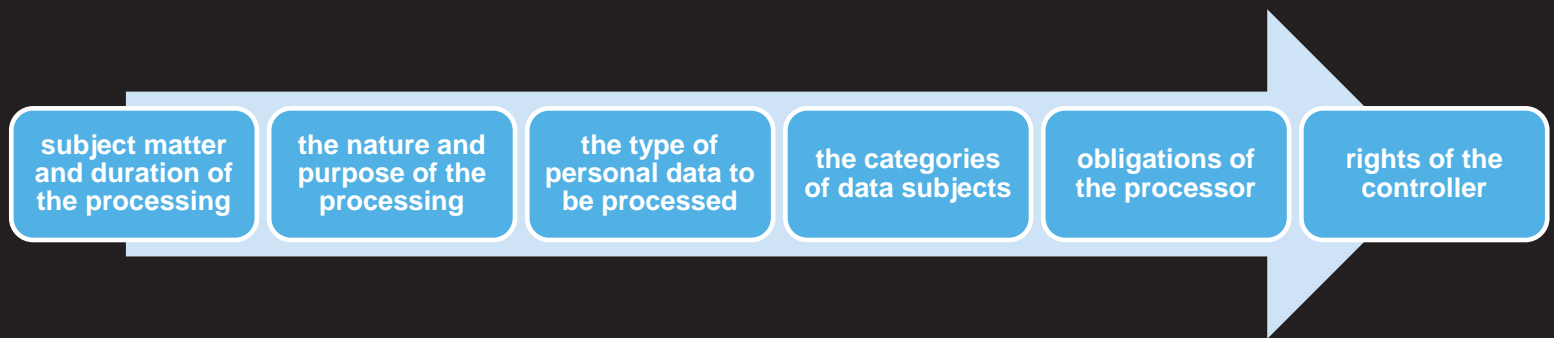


What to Consider Before Sharing Data

- What is the scope of your consent/legitimate interests?
- What will the third party do with that data - is any additional processing by the third party “compatible” with the original consent?
- Has the third party’s security protocols been vetted?
- Can/will the third party help you honor data subject rights and comply with your security breach notification obligations?



Sharing Data: Points to Address in a Data Processing Agreement



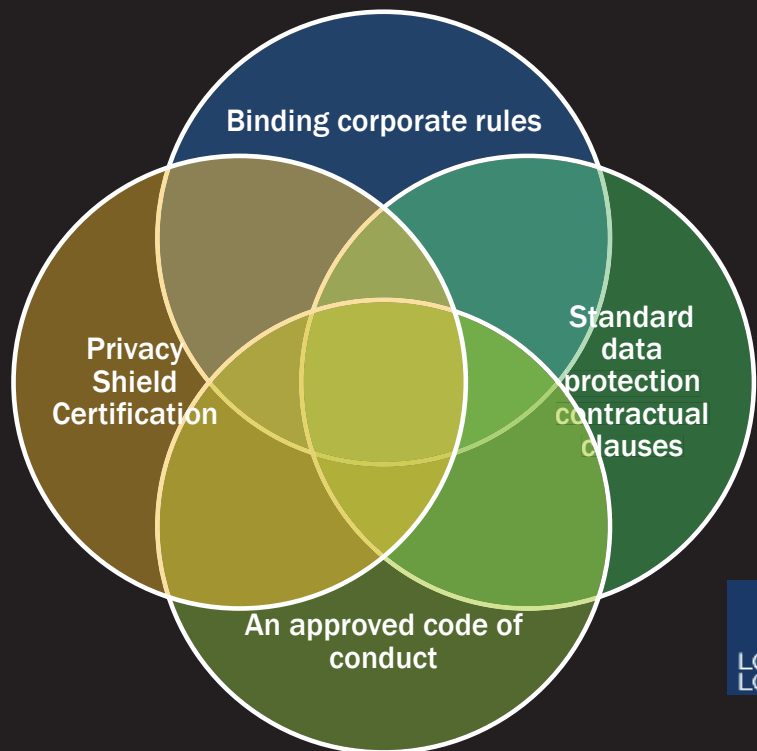
Vendor Due Diligence: Key Questions to Ask

- Where is the vendor based? Where will the data be held and accessed?
- Will the vendor act as a processor or controller?
- Does the vendor use the data to pursue its own interests?
- Will the vendor be using any subcontractors? If so, where are they based?
- What are the technical & organizational security measures the vendor uses to protect data?
- What are their policies / procedures / certifications to protect data? Are these good enough?
- Does the vendor comply with a code of conduct on how it uses data?
- Does the vendor have a privacy seal?
- Can the vendor assist in honoring data subject rights?



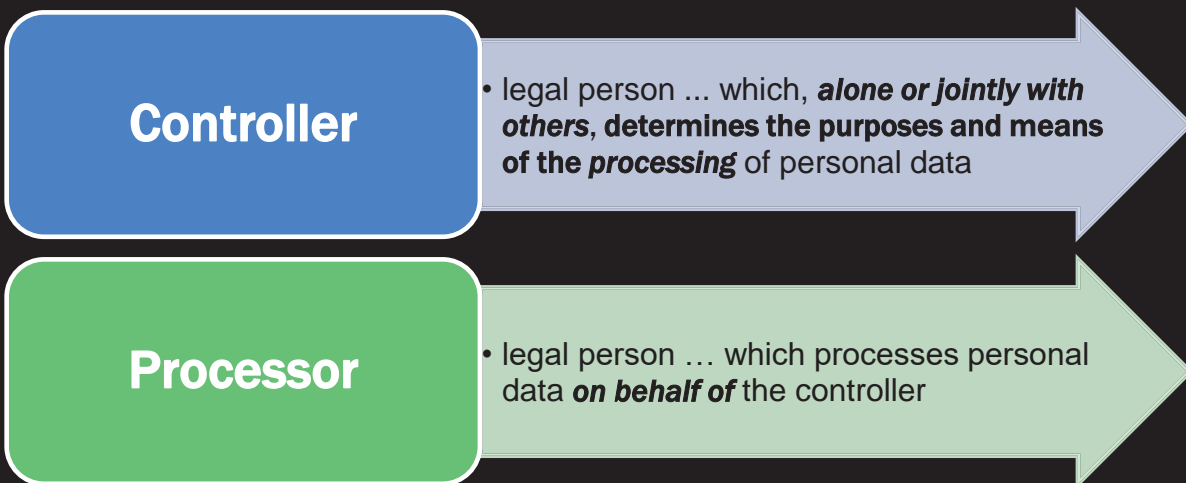
Special Mechanisms Are Needed to Transfer Data Outside of the EU

There are a handful of approved mechanisms:

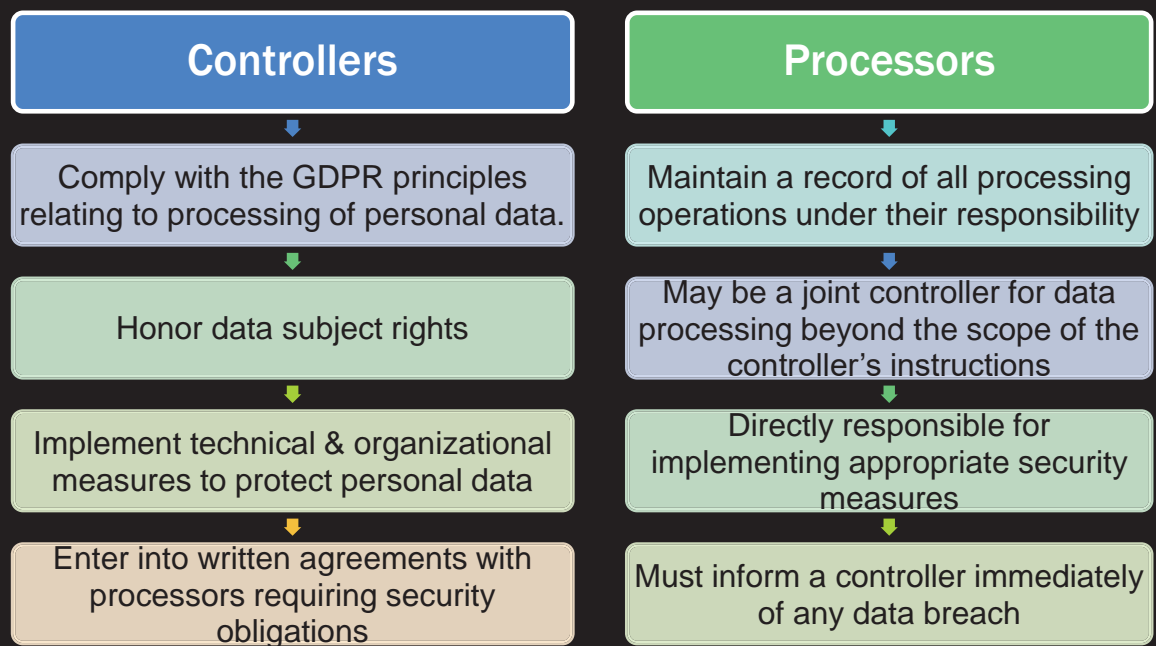


What Will You Need to Do?

Understand Your Role and Obligations




Controllers Vs. Processors



How to Determine Your Role

Consider:

- How did you obtain the data? Is it first, second or third party data?
- Do you determine the techniques used for processing (cookie syncing, data matching)?
- If you are a third party, do you incorporate the data into your own products or services?



Depending on the control you have over the data, you may be a controller, a processor or a joint controller – this determination is based on your activities, it cannot be determined by contract

Consider the Responsibilities/Obligations

As processors:

- You can only process data as permitted by controller agreements
- You will need prior consent to engage vendors (“sub-processors”)

As controllers, you have more control, but:

- You may have direct responsibility for honoring data subject rights
- You have more detailed record keeping obligations
- You are directly responsible for security breach notification obligations

** Joint-controllers will need to allocate responsibilities via contracts



“Accountability” Documenting Your Compliance

- **Maintain Records of Processing**
- **Conduct Privacy Impact Assessments**
 - May be conducted on a routine basis to help keep records up to date when collecting new information or sharing with a third party
- **Conduct Data Privacy Impact Assessment**
 - A mandatory operation for high risk processing
 - Examples of when a DPIA is needed
 - Profiling
 - Engaging in automated decision making with significant or legal effect
 - Large scale data processing
 - Processing that will prevent data subjects for exercising a right



“Accountability” Documenting Your Compliance

You must “implement appropriate technical and organizational measures” that are “appropriate to the risk”

Consider:

- Pseudonymization and encryption of personal data
- Access controls
- Back-up/contingency plan that will ensure the ongoing confidentiality, integrity, and availability of your systems
- A process for regularly testing, assessing and evaluating the effectiveness of your security measures



Record keeping obligations: controllers

Records must contain the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
- the purposes of the processing
- a description of the categories of data subjects and the categories of personal data being processed
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries
- where applicable, an indication of any transfers of personal data to a third country, including the name of the third country, and the documentation of suitable safeguards (if applicable)
- where possible, the time limits for erasure of the various categories of data being processed
- where possible, a general description of the applicable technical and organizational security measures

Record keeping obligations: processors

Records must contain the following information:

- the name and contact details of the processor or processors and of each controller on whose behalf the processor is acting and, where applicable, the controller's or processor's representative as well as the data protection officer
- the categories of processing carried out on behalf of each controller
- where applicable, an indication of any transfers of personal data to a third country, including the name of the third country, and the documentation of suitable safeguards (if applicable)
- where possible, a general description of the technical and organizational security measures taken to protect the personal data

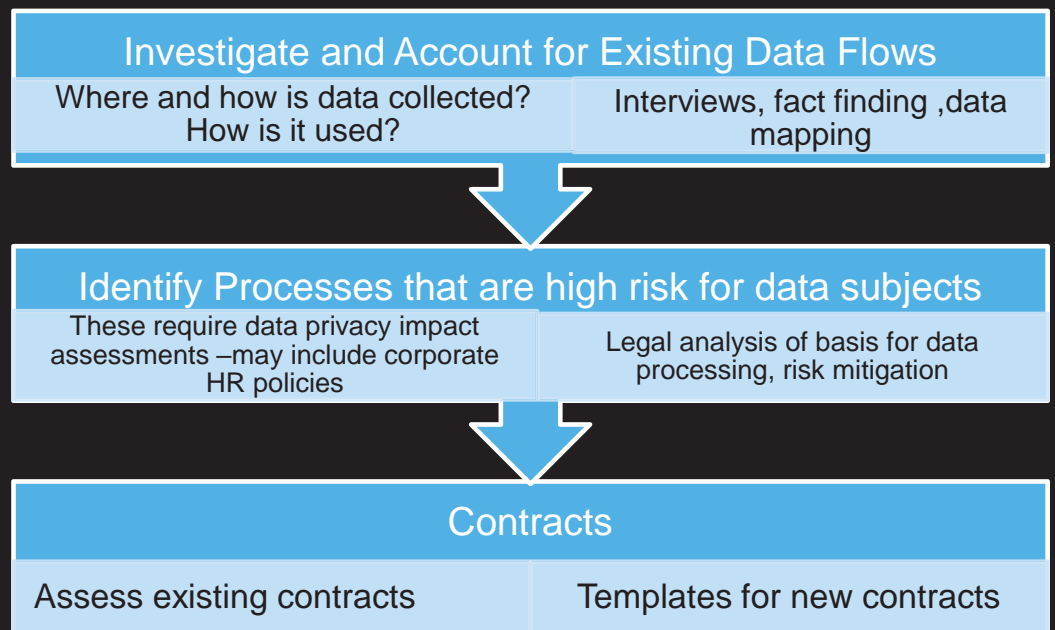
Next Steps in GDPR Readiness

Preparations for GDPR

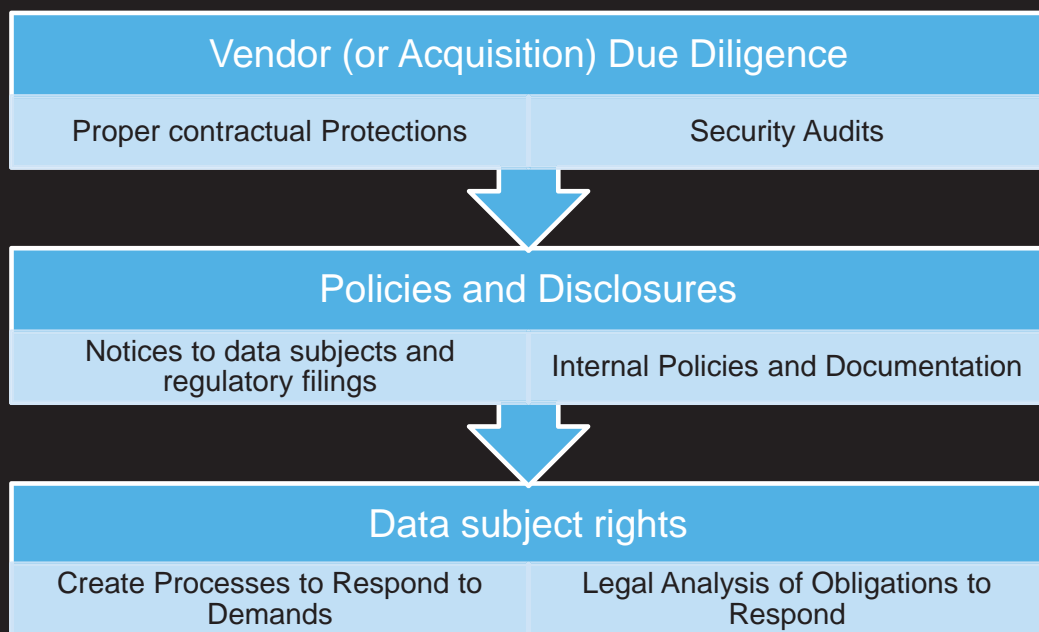
- **Create Framework** for ongoing compliance and data governance
- **Advise on selection of DPO** and support organization
- **Review existing data management** and identify gaps
- **Opportunity for ongoing support** of company's data governance and corporate governance



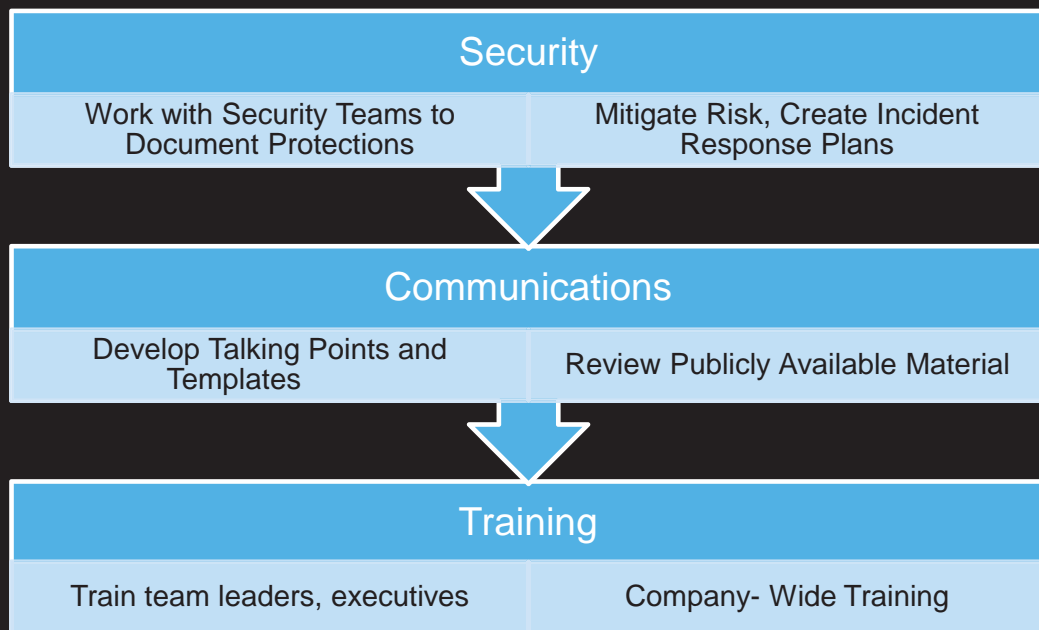
How do we
support
preparations
for GDPR?



Preparations for GDPR



Preparations for GDPR



What to Do Between Now and May 2018

- Investigate & understand the flow of data through your company
 - What do you collect/receive? What do you do with it?
Where do you send it/when do you delete it?
- Complete Records of Processing
- Complete a gap assessment
- Review & update contracts (if needed)
- Review & update consents/privacy notices (if needed)
- Create a Security Breach Notification process.
- Complete PIA/DPIA for ADM/Profiling/Processing based on Legitimate Interests



What to Look for in the Next Few Months

- Codes of Conduct
- Member State Guidance
- Industry Specific Guidance



Questions?

Jessica B. Lee

jblee@loeb.com

<https://www.loeb.com/attorney-jessicablee>



Internet of Things Update

NYSBA



CONNECTED DEVICES



IoT devices will go from 2 billion in 2006 to 200 billion in 2020



That's about

26 devices
per person

The number of
smart home
devices will
grow from

42

million



244

million within five years

Today's IoT Landscape

Things Move Fast...

L.L. Bean says it might offer discounts for clothing that tracks your habits



Dennis Green



Feb. 7, 2018, 4:48 PM

5,460

L.L. Bean To Continually Track Clothing After Purchase

by [Chuck Martin](#), Staff Writer, February 9, 2018

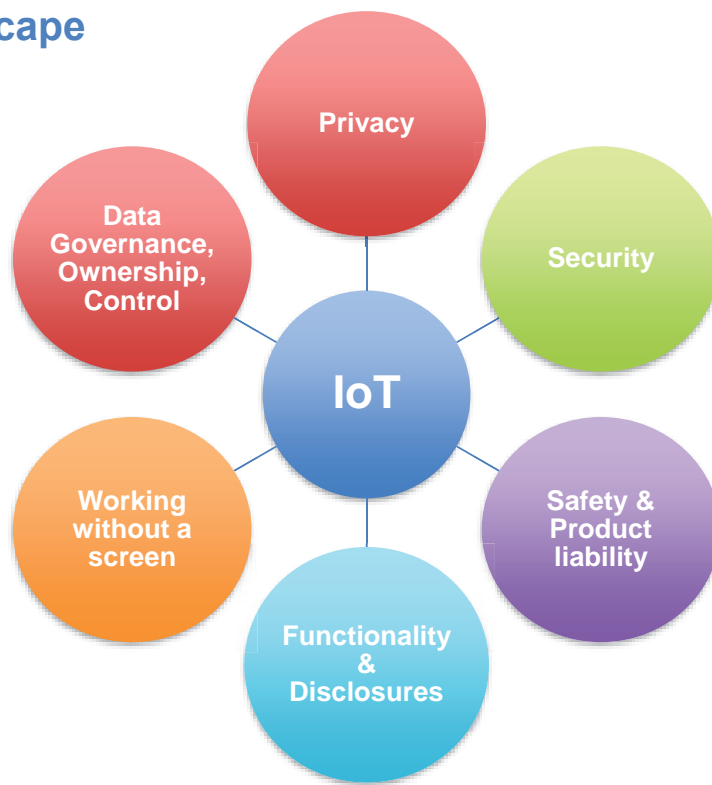
L.L. Bean Backs Off Of Continually Tracking Clothing After Purchase

by [Chuck Martin](#), Staff Writer, February 10, 2018

NYSBA

Today's IoT Landscape

Key Issues



NYSBA

Privacy

NYSBA





FEDERAL TRADE COMMISSION

PROTECTING AMERICA'S CONSUMERS

- **Updated COPPA Guidance** (June 2017)
 - Connected toys and devices, voice-activated tech
 - New methods of parental consent (including facial recognition)
- **Enforcement Policy Statement** (October 2017)
- **Workshop on Informational Injury** (December 2017)



v

vtech

January 2018: Connected toy app alleged to have collected children's info without parental consent

- Didn't link to privacy policy everywhere info was collected
- Didn't provide direct notice of collection
- Failed to protect information (intrusion prevention or detection)
- Failed to encrypt as stated in privacy policy
 - Alleged violations of COPPA, FTC Act
 - \$650,000 settlement

Consumer Product Safety Commission

The CPSC held a hearing focused on IoT product safety but limited the scope of its inquiry to **physical injury** (explicitly excluding data and privacy concerns from its analysis).

The FTC filed comments, and identified 3 security practices it thinks the CPSC should focus on to counter consumer hazards:

- **Risk assessment** – test authentication techniques and communication
- **Vendor oversight, interdependent products** – conduct due diligence with vendors, incorporate security standards in contracts, verify compliance
- **Software updates, “expiration dates” and default settings** – take a holistic view of the marketplace and stay up to date on new trends; consider patch vulnerabilities and security-only updates

NTIA to Update U.S. Privacy Laws

- Senate Committee on Commerce, Science & Technology holds hearing in November 2017 to discuss privacy and security threats to U.S. consumers.
- Industry groups urge Congress and NTIA to better protect consumers and propose consumer protects to ensure routine security devices for IoT devices and carefully assess IoT when used for “critical functions” such as transportation, home security or medical devices.

STATES ARE ALSO POLICING PRIVACY



NYSBA

Security

NYSBA



FTC Warns Device Makers on Security February 2018



- “Start with security” (repeated from June 2015)
- Streamline the update process for consumers
- More and better information about security update support

Consumer Reports – The Digital Standard

Test Name	Criteria	Indicators	Procedure Overview
Security (Is it safe?)			
Build Quality			
✓ Best Build Practices	The software was built and developed according to the industry's best practices for security.	The product was built with effectively implemented safety features.	Run static analysis software to determine what association-generating features are present. Are there Stack Guards, and if
⚠ Product Stability	The software is reliable.	The software is not susceptible to crashes. If the program is forced to unexpectedly terminate, it shuts down smoothly and responsibly without crashing.	Run software to test if and how it crashes. Under appropriate test settings, what was the crash coverage, number of crashes, and types of crashes? Are crashes attributable to an underlying strategy where a disruption of service?
Data security			
✓ Vulnerability disclosure program	The company is willing and able to address reports of vulnerabilities.	The company has a mechanism (e.g. bug bounty program) through which security researchers can submit vulnerabilities they discover. The company discloses the findings in which all major reports of vulnerabilities. The company commits not to pursue legal action against security researchers.	Investigation and analysis of publicly available documentation to determine what the company already discloses.

Some criteria is still under review:

- ✓ : Well understood with a developed testing approach in place.
- ⚠ : Under development with some outstanding questions.
- ! : Under discussion, usually due to the sensitivity and complexity of the issue.

Consumer Reports – Updates

- Consumer Reports conducted their first review using the Digital Standard to rate connected TVs
- Findings revealed overly-broad data collection, security flaws and privacy concerns
- More review of consumer products to come
- Recently introduced new ratings criteria to the Digital Standard (data privacy and security) to measure peer-to-peer payments
- Reviewed P2P payment services including Apple Pay, Facebook Payments (in Messenger), Square's Cash App, Venmo and Zelle

Consumer Reports – Smart TVs

February 2018

- Consumer Reports reviewed 5 different smart TVs (Samsung, TCL, LG, Sony and Vizio)
- Found all used automatic content recognition (ACR)
- Discovered security vulnerabilities on some models that allowed outside attacker to control TV functions
- Some features and data collection could be disabled but severely limited the functioning of TV
- Other categories to come soon!

Consumer Reports – Peer-to-Peer Payments

June 2018



MOBILE PEER-TO-PEER PAYMENT SERVICES						
SERVICE	OVERALL SCORE	PAYMENT AUTHENTICATION	DATA SECURITY	DATA PRIVACY	CUSTOMER SUPPORT	BROAD ACCESS
Apple Pay	76					
Venmo	69					
Cash App (Square)	64					
Facebook P2P Payments in Messenger	63					
Zelle (standalone app)	50					

Security Concerns

- Constant data collection
- Unexpected uses of consumer data
- Unencrypted data (especially at rest)
- Device and network authentication
- Representations about security can create liability



How long do IoT devices last?

What do consumers expect?

Grace v. Apple

Apple created an alternative version of FaceTime for iOS 7, and in April 2014 disabled FaceTime on iOS 6 and earlier versions. Users with earlier model phones/iOS sued Apple for their inability to use FaceTime.

- In July 2017, judge rules that iPhone 4 and 4S users can pursue nationwide class action claims that Apple intentionally “broke” FaceTime (to save money from routing calls through servers owned by a third party).
- As of August 2018, the parties are undergoing discovery, obtaining expert testimony and fighting over class certification. Expert discovery (including depositions) are scheduled to be completed by September 27, 2018.

Discontinuations and Product Lifecycle

- **Robot Kuri** – In July 2018, Mayfield Robotics (an entity of the Bosch Startup Platform) announced that it is pausing operations of its Robot Kuri, a “home” robot that launched at CES in 2017. Mayfield will stop manufacturing, will not ship robots out to customers and will refund all pre-order deposits.
- **Amazon “Mayday” Button** – In June 2018, Amazon announced that it will immediately discontinue the “Mayday” button which allows customers to summon face-to-face customer service on their Amazon Fire rather than calling the Amazon Customer Service Line.

Discontinuations and Product Lifecycle

- **Logitech Harmony Link** – In November 2017, Logitech announced that it will be discontinuing service for the Harmony Link remote system. The device and its cloud-based system allow users to control home theater and sound equipment from a mobile app. Customers received an e-mail explaining that Logitech will “discontinue service and support” for the Harmony Link as of March 2018, adding that Harmony Link devices “will no longer function after this date.” Effectively, Logitech’s decision has “bricked” the smart remote device.
- **Intel** – In June 2017, Intel announces it will discontinue the Galileo, Edison, and Joule computer products by posting notices on their website that the company will no longer support the product lines.

ADA Compliance

- January 2018 – new federal regulations took effect (requiring all federal websites comply with the ADA).
- Title III of the American with Disabilities Act regulates private sector businesses. “Business to consumer” websites should comply with the ADA.
- ADA includes minimum requirements for websites like being fully navigable via keyboard and/or screen reader software, text contrast, text scaling, etc.

Questions?

Thank you!

NYSBA



**Before the
CONSUMER PRODUCT SAFETY COMMISSION
Washington, DC**

In the Matter of	Docket No. CPSC-2018-007
The Internet of Things and Consumer Product Hazards	

To: Consumer Product Safety Commission
Date: June 15, 2018

**Comments of the Staff of the Federal Trade Commission’s
Bureau of Consumer Protection**

I. Introduction

The staff of the Federal Trade Commission’s (“FTC”) Bureau of Consumer Protection (“BCP”) (hereafter “BCP staff”) appreciate this opportunity to comment¹ on the Consumer Product Safety Commission’s (“CPSC”) Notice of Public Hearing and Request for Written Comments (“RFC”) on *The Internet of Things and Consumer Product Hazards*.² Among other things, the RFC seeks comment on existing Internet of Things (“IoT”) safety standards, how to prevent hazards related to IoT devices, and the role of government in the effort to promote IoT safety.

The market for Internet-connected devices—ranging from light bulbs to smart TVs to wearable fitness trackers—is flourishing. The rapid proliferation of such devices in recent years has been truly remarkable, with an estimated 8.4 billion IoT devices in use in 2017—a 31% increase from 2016.³ And this trend promises to continue: it is estimated that 55 billion IoT devices will be installed around the world by 2025.⁴

This burgeoning marketplace offers enormous benefits to consumers—including many products that offer safety benefits.⁵ For example, IoT medical devices track health data that

¹ These comments represent the views of the staff of the Bureau of Consumer Protection. The Commission has voted to authorize BCP staff to submit these comments.

² 83 Fed. Reg. 13122 (Mar. 27, 2018).

³ *Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent from 2016*, GARTNER (Feb. 7, 2017), <https://www.gartner.com/newsroom/id/3598917>.

⁴ Peter Newman, *The Internet of Things 2018 Report: How the IoT is Evolving to Reach the Mainstream with Businesses and Consumers*, BUS. INSIDER INTELLIGENCE (Feb. 26, 2018), <http://www.businessinsider.com/the-internet-of-things-2017-report-2018-2-26-1>.

⁵ See generally FED. TRADE COMM’N, FTC STAFF REPORT: INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, 7-10 (Jan. 2015) [hereinafter FTC IoT REPORT], <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013->

informs patients' diagnosis and treatment.⁶ Connected cars offer both safety and convenience benefits, such as real-time notifications of dangerous conditions and smartphone starter and sound-system control.⁷ And home IoT devices called "water bugs" detect flooding in basements, while other devices monitor energy use, identify maintenance issues, and remotely control devices such as lights, ovens, and wine cellars.⁸ Consumers also may purchase devices such as Internet-connected locks, burglar alarms, cameras, and garage doors for their physical safety.

But such benefits may be foreclosed if IoT devices themselves are a hazard. Like any other consumer product, IoT products might present hazards such as fires and burns, shock, and chemical exposure. IoT devices might also create additional technology-related hazards associated with the loss of a critical safety function, loss of connectivity, or degradation of data integrity.⁹ For example, a car's braking systems might fail when infected with malware,¹⁰ carbon monoxide detectors or fire alarms might stop working with the loss of connectivity,¹¹ and corrupted or inaccurate data on a medical device might pose health risks to a user of the device.¹² Consumers' physical safety could also be at risk if an intruder had access to a connected lock, garage door, or burglar alarm.

Requiring IoT devices to have perfect security would deter the development of devices that provide consumers with the safety and other benefits discussed above.¹³ Conversely, insecure devices can erode consumer trust if consumers cannot rely on the safety and security of

[workshop-entitled-internet-things-privacy/150127iotrpt.pdf](#) (discussing benefits of the IoT) (Commissioner Wright dissenting and Commissioner Ohlhausen issuing a concurring statement).

⁶ *Id.* at 7-8.

⁷ *Id.* at 9.

⁸ *Id.* at i and 8-9.

⁹ CONSUMER PROD. SAFETY COMM'N, POTENTIAL HAZARDS ASSOCIATED WITH EMERGING AND FUTURE TECHNOLOGIES, 16 (Jan. 18, 2017) [hereinafter CPSC EMERGING TECHNOLOGIES REPORT], <https://www.cpsc.gov/content/potential-hazards-associated-with-emerging-and-future-technologies> (citing potentially new consumer product hazards related to IoT, including loss of safety function, loss of connectivity, and issues related to data integrity).

¹⁰ See, e.g., Jeff Plungis, *Your Car Could Be The Next Ransomware Target*, CONSUMER REPORTS (June 01, 2017), <https://www.consumerreports.org/hacking/your-car-could-be-the-next-ransomware-target/>. See also Catalin Cimpanu, *Volkswagen and Audi Cars Vulnerable to Remote Hacking*, BLEEPINGCOMPUTER (April 30, 2018), <https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/> and Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4 M Vehicles For Bug Fix*, WIRED (July 24, 2015), <https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/>.

¹¹ Cf. Richard Speed, *Three-Hour Outage Renders Nest-Equipped Smart Homes Very Dumb*, THE REGISTER (May 17, 2018), https://www.theregister.co.uk/2018/05/17/nest_outage/ (reporting that an outage in the Nest system left consumers "unable to arm/disarm or lock/unlock" their homes remotely, leaving frustrated consumers to set their alarms and lock their doors manually).

¹² Shaun Sutner, *FDA and UL weigh in on security of medical devices, IoT*, IOT AGENDA, <https://internetofthingsagenda.techtarget.com/feature/FDA-and-UL-weigh-in-on-security-of-medical-devices-IoT>.

¹³ The FTC does not expect perfect security. See e.g. Prepared Statement of the Fed. Trade Comm'n, *Protecting Consumer Information: Can Data Breaches be Prevented? Before the Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, U.S. House of Representatives*, 4 (Feb. 5, 2014), <https://energycommerce.house.gov/hearings/protecting-consumer-information-can-data-breaches-be-prevented/> ("[T]he Commission has made clear that it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.")

their device.¹⁴ Companies that manufacture and sell IoT devices must take *reasonable* steps to secure them from unauthorized access. Poorly-secured IoT devices create opportunities for attackers to assume device control, opening up risks that may include safety hazards.¹⁵ For example, hackers used the Mirai botnet—composed of IoT devices, such as IP cameras and routers, infected with malicious software—to engage in a distributed denial of service (“DDoS”) attack of unprotected residential building management systems in Finland. By blocking Internet access, hackers sent these connected management systems into an endless cycle of rebooting, leaving apartment residents with no central heating in the middle of winter.¹⁶ Also, earlier this year, researchers discovered vulnerabilities in Internet-connected gas station pumps that, when remotely accessed, would allow hackers not only to steal credit card information but also change the temperature and pressure in gas tanks, potentially causing explosions.¹⁷

Although the request for comment specifically notes that the CPSC “will not address personal data security or privacy implications of IoT devices,” security risks associated with IoT devices may implicate broader safety concerns, not just privacy. For example, a criminal who hacks into a connected-home network could not only collect information about consumers who live in the house, but also could activate or deactivate home security devices, potentially causing threats to personal safety.¹⁸ A company setting up a program to address security risks on its IoT device should take measures to secure that device from hackers, for both privacy *and* safety issues. Through this comment, BCP staff shares some of its expertise in promoting IoT device security, and makes certain recommendations to the CPSC. The recommendations focus on three issues: (1) best practices for predicting and mitigating against security hazards; (2) the process for encouraging consumers to register for safety alerts and recall information; and (3) the role of government in IoT security.

II. Background on the FTC

The FTC is an independent administrative agency responsible for protecting consumers and promoting competition. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect consumers’ privacy and security. The primary law enforced by the FTC, the FTC Act, prohibits unfair and deceptive acts or practices in or affecting commerce,

¹⁴ See e.g. FED. TRADE COMM’N, MOBILE SECURITY UPDATES: UNDERSTANDING THE ISSUES, 1 (Feb. 2018) [hereinafter “MOBILE SECURITY REPORT”], <https://www.ftc.gov/reports/mobile-security-updates-understanding-issues>; FTC IOT REPORT at 20-21; and Comments of the Staff of the Fed. Trade Comm’n, *In the Matter of Communicating IoT Device Security Update Capability to Improve Transparency for Consumers*, Nat. Telecomm. Info. Admin. (June 19, 2017), <https://www.ftc.gov/policy/advocacy/advocacy-filings/2017/06/ftc-comment-national-telecommunications-information>.

¹⁵ *Id.* See also Chris Morris, *465,000 Pacemakers Recalled on Hacking Fears*, FORTUNE (Aug. 31, 2017), <http://fortune.com/2017/08/31/pacemaker-recall-fda/>; and Lisa Vaas, *350,000 Cardiac Devices Need a Security Patch*, NAKED SECURITY (May 4, 2018), <https://nakedsecurity.sophos.com/2018/05/04/half-a-million-pacemakers-need-a-security-patch/>.

¹⁶ Richard Chirgwin, *Finns Chilling as DDoS Knocks Out Building Control System*, THE REGISTER (Nov. 9, 2016), https://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/.

¹⁷ Alfred Ng, *Hackers Should Be Pumped About Gas Station Security Flaws*, CNET (Mar. 12, 2018), <https://www.cnet.com/news/gas-stations-online-are-easy-access-for-managers-and-hackers/>.

¹⁸ See e.g. John Leyden, *Half Baked Security: Hackers Can Hijack Your Smart Aga Oven ‘With a Text Message’*, THE REGISTER (April 13, 2017), https://www.theregister.co.uk/2017/04/13/aga_oven_iot_insecurity/.

including unfair and deceptive privacy and security practices.¹⁹ In the context of IoT security, this means that companies should maintain a reasonable security program and keep the promises they make to consumers concerning the security of their devices. The FTC also enforces sector-specific statutes that protect certain health, credit, financial, and children's information, and has issued regulations implementing each of these statutes.²⁰

The FTC has used its authority under these laws to protect consumers from insecure IoT devices.²¹ For example, in the *TRENDnet* case, the FTC alleged that the company engaged in unfair and deceptive security practices related to its Internet-connected cameras.²² The complaint alleged that the company's failure to reasonably test and review the camera's software for security problems; failure to encrypt data in storage and transit; and failure to monitor third-party security vulnerability reports led to a breach of private video feeds.²³ Likewise, in the *ASUS* case, the FTC alleged that the company's failure to reasonably secure its routers led to the unauthorized access of consumers' home networks.²⁴ The FTC's enforcement actions send an important message to companies about the need to secure and protect Internet-connected devices.

The FTC also has pursued numerous policy initiatives designed to enhance device security in an Internet-connected world. For example, the FTC has hosted workshops on the Internet of Things generally,²⁵ mobile security,²⁶ drones,²⁷ connected TVs,²⁸ ransomware,²⁹ and

¹⁹ 15 U.S.C. § 45. (For an unfair act or practice to violate Section 5 of the FTC Act it must "cause[] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." Additionally, deception requires a material representation, omission, or practice that is likely to mislead consumers, who are acting reasonably under the circumstances. See Fed. Trade Comm'n, *Policy Statement on Deception* (Oct. 14, 1983), <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.)

²⁰ See, e.g., Health Breach Notification Rule, 16 C.F.R. Part 318 *et seq.* (health information breach notification); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* and 16 C.F.R. Part 600 (consumer reporting information security and privacy); Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. Part 314 *et seq.* (financial information security); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq.* and 16 C.F.R. Part 312 (children's online information security and privacy).

²¹ See e.g., VTech Electronics Ltd., FTC No. 1623032 (Jan 8, 2018) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/162-3032/vtech-electronics-limited>; TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter>; ASUSTeK Computer, Inc., FTC No. 1423156 (Feb. 26, 2016) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter>; and VIZIO, Inc., No. 2:17-cv-00758 (Feb. 6, 2017) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc>.

²² TRENDnet, Inc., *supra* n. 22.

²³ *Id.*

²⁴ ASUSTeK Computer, Inc., *supra* n. 22.

²⁵ See generally, FTC IoT REPORT; see also FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Nov. 19, 2013) (workshop), <https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

²⁶ MOBILE SECURITY REPORT at 18.

²⁷ FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: DRONES (Oct. 13, 2016) (workshop), <https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones>.

²⁸ FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: SMART TV (Dec. 7, 2016) (workshop), <https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv>.

²⁹ FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: RANSOMWARE (Sept. 7, 2016) (workshop), <https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware>.

connected cars.³⁰ In its staff report from 2015 on the Internet of Things, the FTC made several recommendations for security best practices, including recommendations that companies conduct risk assessments, test their security measures before launching their products, train employees on security, and monitor products throughout their life cycle.³¹ In a more recent report on mobile device updates, the FTC discussed the complex and often time-consuming process that companies face when updating mobile devices.³² While noting that industry participants have taken steps to streamline the process, the report recommends that manufacturers consider taking additional steps to deliver security updates to user devices faster. It also recommends that manufacturers consider telling users how long a device will receive security updates and when update support is ending.³³

To encourage consumers to implement security updates, last year the FTC held its *IoT Home Inspector Challenge*, a public competition aimed at spurring the development of security update-related IoT tools.³⁴ The winning contestant developed a tool to enable users with limited technical expertise to scan their home Wi-Fi and Bluetooth networks to identify and inventory connected devices. The tool would also flag devices with out-of-date software and other common vulnerabilities, and provide instructions to consumers on how to update each of their devices and fix other vulnerabilities.³⁵

Finally, the FTC engages in consumer and business education regarding IoT device security. On the business education front, the Commission launched its *Start with Security* initiative,³⁶ *Stick with Security* blog series,³⁷ and “*Careful Connections*” IoT guidance,³⁸ which apply to businesses considering security issues in the IoT space. For example, the Commission’s *Careful Connections* guide emphasizes a risk-based approach to device security, encouraging device manufacturers to evaluate the risks to their devices and prioritize the allocation of security

³⁰ FED. TRADE COMM’N, CONNECTED CARS: PRIVACY, SECURITY ISSUES RELATED TO CONNECTED, AUTOMATED VEHICLES (Jun. 28, 2017) (workshop), <https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected>.

³¹ See generally, FTC IoT REPORT.

³² See generally, MOBILE SECURITY REPORT.

³³ *Id.* at 71-72.

³⁴ See FTC Notice of IoT Home Inspector Challenge, 82 Fed. Reg. 840-2, 840-41 (Jan. 4, 2017), https://www.ftc.gov/system/files/documents/feeral_register_noticies/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

³⁵ *FTC Announces Winner of its Internet of Things Home Device Security Contest*, Fed. Trade Comm’n (July 26, 2017), <https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security>.

³⁶ FED. TRADE COMM’N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015) [hereinafter START WITH SECURITY], <https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf>.

³⁷ Thomas B. Pahl, *Stick With Security*, FTC BUSINESS BLOG (Sept. 22, 2017), <https://www.ftc.gov/news-events/blogs/business-blog/2017/09/stick-security-put-procedures-place-keep-your-security>.

³⁸ FED. TRADE COMM’N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (Jan. 2015) [hereinafter CAREFUL CONNECTIONS], <https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf>.

resources where they are most needed.³⁹ On the consumer education front, a consumer education blog post describes the 2016 Mirai malware attack, in which the Mirai botnet, as described above, attacked a service used by a number of popular websites like Netflix, PayPal, and Twitter, knocking them offline. The education piece urged consumers to change default settings and passwords and download the latest security updates for their IoT devices.⁴⁰

III. Discussion

The CPSC requests comment on numerous issues. This comment focuses in particular on three: (1) What are some best practices for predicting and mitigating against safety hazards? (2) How can the CPSC encourage consumers to register for safety alerts and recall information? (3) What is the appropriate role of government in IoT security?

A. What are best practices for predicting and mitigating against safety hazards?

The FTC has provided IoT manufacturers with a host of guidance on how to predict and mitigate against privacy, security, and safety hazards. The discussion in this section is premised on the notion that there is no “one size fits all” approach to securing IoT devices. The level of reasonable security will depend on many factors, including the magnitude of potential risks, the likelihood of such risks, and the availability of low-cost tools to address the risks. This comment focuses on guidance in three areas in particular: risk assessment; reasonable vendor oversight for devices and other interdependent products; and software updates, product “expiration” dates, and default settings.

1. Risk Assessment

As the CPSC is well aware, a risk assessment is a starting point for a company to evaluate its security program. A risk assessment can help identify reasonably foreseeable threats and hazards, and solutions for mitigating against such threats and hazards. While the IoT industry is relatively new, companies have been conducting assessments to identify and mitigate against threats and hazards for several years. Companies can build on 20 years of lessons learned by security experts, who have already identified low-cost solutions to some common concerns raised by the Internet of Things.⁴¹

One example of a reasonably foreseeable risk is that hackers can compromise user credentials to take over an IoT device.⁴² The FTC has recommended that companies test

³⁹ CAREFUL CONNECTIONS at 1-2.

⁴⁰ Ari Lazarus, *What You Need to Know to Secure Your IoT Devices*, FTC CONSUMER BLOG (Dec. 7, 2016), <https://www.consumer.ftc.gov/blog/2016/12/what-you-need-know-secure-your-iot-devices>.

⁴¹ See CAREFUL CONNECTIONS at 2 (E.g. apply standard encryption techniques, apply “salt” to hashed data, and consider rate limiting).

⁴² See FTC cases concerning the security of credentials, such as Twitter, Inc., FTC No. 0923093 (Mar. 11, 2011) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation>; Reed Elsevier, Inc., FTC No. 052094 (Aug. 1, 2008), <https://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter>; Guidance Software, Inc., FTC No. 0623057 (April 3, 2007), <https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation>; and Twitter, Inc., FTC No.

authentication techniques and consider whether techniques, such as multi-factor authentication (such as a password and a code sent to a phone) or biometric authentication, are appropriate.⁴³ The FTC has also recommended that companies consider risks at the point where a service communicates with an IoT device, such as the interface between the device and the cloud.⁴⁴ Security experts have long warned against attack vectors such as cross-site scripting attacks, where malicious scripts are injected into otherwise trusted websites, and cross-site request forgery attacks, where unauthorized commands are sent from a user the website trusts.⁴⁵

Finally, the FTC has recommended that companies test a product's security measures before launch. There are readily available, free or cost-effective tools for most basic security testing tasks—network scanning for open ports, reverse engineering of programming code, checking password strength, and vulnerability scans.⁴⁶

2. Service Provider Oversight

While security protections are generally the responsibility of the manufacturer, IoT devices often are a product of components and software from a variety of service providers.⁴⁷ Prior to selling their products to consumers, IoT manufacturers should take reasonable measures to evaluate the overall security of those products, including any risks that their service providers might introduce.⁴⁸ Companies should provide oversight by exercising due diligence in their selection of service providers, incorporating security standards into their contracts, and taking reasonable steps to verify compliance with those security standards on an ongoing basis.⁴⁹

In circumstances where companies have failed reasonably to oversee the security practices of their service providers, the FTC has taken action.⁵⁰ For example, in its case against *BLU Products*, the FTC alleged that a mobile device manufacturer had violated Section 5 of the FTC Act by failing to maintain reasonable security when, among other things, it failed to exercise oversight of its service provider.⁵¹ In part, the FTC alleged that the company did not even put in place basic contractual provisions requiring its service providers to maintain

0923093 (Mar. 11, 2011) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation>.

⁴³ CAREFUL CONNECTIONS at 3.

⁴⁴ *Id.* at 4.

⁴⁵ *Id.* Fuzzing – a testing method that sends a device or system unexpected input data to detect possible defects – is one example of an approach recommended by security experts to addressing these issues as well as discovering other implementation bugs. *See also*, *Fuzzing*, Open Web Application Security Project, <https://www.owasp.org/index.php/Fuzzing>.

⁴⁶ *Id.* at 5.

⁴⁷ *See e.g.*, CPSC EMERGING TECHNOLOGIES REPORT at 6.

⁴⁸ CAREFUL CONNECTIONS at 1 (“There’s no one-size-fits all checklist to guarantee the security of connected devices. What’s reasonable will depend on a number of variables, including the kind and amount of information that’s collected, the type of functionality involved, and the potential security risks.”).

⁴⁹ START WITH SECURITY at 11.

⁵⁰ *BLU Products*, FTC No. 1723025 (April 30, 2018) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/172-3025/blu-products-samuel-ohev-zion-matter>; *Lenovo, Inc.*, FTC No. 1523134 (Sept. 13, 2017), <https://www.ftc.gov/enforcement/cases-proceedings/152-3134/lenovo-inc>; and *Upromise, Inc.*, FTC No. 1023116 (April 3, 2012), <https://www.ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc>.

⁵¹ *BLU Products*, *supra* n. 50.

reasonable security. As a result of the company's alleged failures, consumer data was put at an unreasonable risk of unauthorized access. In this case consumers' text message contents, call and text logs, and real-time location were shared with a Chinese service provider that did not have a business need for the information, in violation of the company's privacy policy.⁵²

As another example, in the FTC's recent case against *Lenovo*, the Commission alleged that Lenovo preinstalled third-party ad-injecting software on its laptops that created serious security vulnerabilities.⁵³ The complaint noted that, even after its service provider informed Lenovo of security problems during the development of the software, Lenovo did not seek further information and approved the software's use on Lenovo laptops.⁵⁴ This was one factor, among others, cited in the complaint alleging that Lenovo violated Section 5 by failing to implement reasonable security in overseeing its vendors.⁵⁵

3. Ongoing Oversight, Updating, and Patching

The FTC has recommended that companies have an ongoing process to keep up with security practices as threats, safety hazards, technologies, and business models evolve. This involves at least two components.

First, companies should take steps to stay abreast of threats identified in the marketplace by, for example, signing up for email updates from trusted sources; checking free databases of vulnerabilities identified by security researchers; and maintaining a channel through which security researchers can reach out about risks.⁵⁶ Indeed, in many cases, the FTC has alleged, among other things, that the failure to maintain an adequate process for receiving and addressing security vulnerability reports from security researchers and academics is an unreasonable practice, in violation of Section 5 of the FTC Act.⁵⁷

Second, companies should take reasonable steps to address threats to privacy, security and safety after launching products, including by issuing updates and patches. In our recently conducted study of mobile security updates, we found that the security update process varies significantly among mobile device manufacturers, and although they have made improvements, bottlenecks remain.⁵⁸ We encouraged all actors in the ecosystem to ensure that devices receive security updates for a period of time that is consistent with consumers' reasonable expectations. Such support should be a shared priority, reflected in policies, practices, and contracts among all parties involved in the creation of a device.⁵⁹ We also recommended that industry streamline the

⁵² *Id.*

⁵³ *Lenovo, Inc.*, *supra* n. 50.

⁵⁴ *Id.*

⁵⁵ While the BLU and Lenovo cases involve privacy and security, the same types of oversight of service providers would help prevent them from introducing safety hazards into IoT devices.

⁵⁶ CAREFUL CONNECTIONS at 7.

⁵⁷ See e.g. *HTC America*, FTC No. 1223049 (July 2, 2013) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter>; and *TRENDnet, Inc.* FTC No. 1223090 (Feb. 7, 2014) (complaint), <https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter>.

⁵⁸ MOBILE SECURITY REPORT at 65.

⁵⁹ *Id.* at 69.

security update process. In particular, we noted that companies should patch vulnerabilities in security-only updates when the benefits of more immediate action outweigh the convenience of a bundling a security update with a functionality update.⁶⁰ Finally, we recommended that device manufacturers consider giving consumers more and better information about security update support.⁶¹ Specifically, we recommended that manufacturers interested in providing security update information consider adopting and disclosing minimum guaranteed security support periods (and update frequency) for their devices.⁶² We further recommended that they consider giving device owners prompt notice when security support is about to end (and when it has ended), so that consumers can make informed decisions about device replacement or post-support use.⁶³

B. How can the CPSC encourage consumers to sign up for safety alert and recall information?

Although manufacturers can update some devices automatically, many devices require consumers to take affirmative steps to install the update. In particular, consumers must know how – and where – to check for security updates and how to install them. As the number of devices within the home multiply, the task of updating devices could become increasingly daunting. As noted above, in 2017, the FTC sponsored a prize competition under the America Competes Act to assist consumers and drive innovation in this area.⁶⁴ Encouraging the development of tools that allow consumers to monitor and maintain the security of their personal IoT devices will likely bring more general awareness to the issue, in addition to direct benefits to consumers that adopt those tools.

BCP staff recommends that the CPSC consider how companies might provide consumers with the opportunity to sign up for communications regarding safety notifications and recalls for IoT devices. Such a process could borrow from CPSC’s existing process of allowing consumers to sign up for safety notifications regarding infant and toddler products.⁶⁵ That process in part requires manufacturers and retailers of durable infant and toddler products to provide consumers with a safety registration card for mail-in registration. The registration card must also include an URL for online registration.⁶⁶ Given that consumers purchasing IoT devices necessarily have an Internet connection, however, it is likely that online registration would be a more effective option in the IoT space.⁶⁷

⁶⁰ *Id.* at 71.

⁶¹ *Id.*

⁶² *Id.*

⁶³ *Id.* at 71-72.

⁶⁴ See 82 Fed. Reg. 840 (2017).

⁶⁵ 74 Fed. Reg. 68677. See also, *Consumer Registration Cards for Durable Infant or Toddler Products*, CONSUMER PROD. SAFETY COMM’N, <https://www.cpsc.gov/Business--Manufacturing/Business-Education/Durable-Infant-or-Toddler-Products/Durable-Infant-or-Toddler-Product-Consumer-Registration-Cards/>.

⁶⁶ *Id.*

⁶⁷ For example, some panelists at the CPSC IOT HEARING raised the opportunities for application interfaces, pop-up notifications, and on-device alerts. CONSUMER PROD. SAFETY COMM’N, PUBLIC HEARING ON THE “INTERNET OF THINGS AND CONSUMER PRODUCT HAZARDS,” (May 16, 2018) [hereinafter CPSC IOT HEARING], https://www.youtube.com/watch?v=7RdbpJ_eD98. Additionally, many online retailers have a direct

Some consumers may be dissuaded from registering on the expectation that they will receive unwanted marketing communications. Indeed, a recent survey showed that, while many consumers like receiving marketing communications, 12 percent of consumers do not register products because they do not want to share their personal information.⁶⁸ BCP staff recommends that, to address potential concerns of these consumers, the CPSC should consider how companies might offer consumers a choice, during the product registration process, about whether they want to receive marketing communications.⁶⁹

C. What is the appropriate role of government in promoting IoT safety?

At the CPSC's IoT hearing, many panelists discussed the value of regulation and IoT-specific standards.⁷⁰ Although BCP staff does not take a position on whether or not the CPSC should implement regulations relating to IoT device hazards, to the extent the CPSC considers such regulation, we suggest that any such approach be technology-neutral and sufficiently flexible so that it does not become obsolete as technology changes.

In addition, to the extent that the CPSC considers certification requirements for IoT devices,⁷¹ the CPSC should consider requiring manufacturers to publicly set forth the standards to which they adhere. Such disclosures would improve transparency and provide consumers with information to better evaluate the safety and security of their IoT products. The FTC could use its authority under the FTC Act to take action against companies that misrepresent their security practices in their certifications. This additional tool would provide an enforcement backstop to help ensure that companies comply with their certifications. Examples of enforceable statements to consumers could include statements on websites, on a retail packaging, on the device itself, or in the user interface of the device.

relationship with customers and, in some instances, might be in a better position to effectuate notice of safety recalls to purchasers.

⁶⁸ See, e.g., *New Study: Millennials and Affluent Consumers Want to Connect with Brands Immediately Post-Purchase via Mobile*, REGISTRIA (April 26, 2017) [hereinafter Registrria survey], <http://www.marketwired.com/press-release/new-study-millennials-affluent-consumers-want-connect-with-brands-immediately-post-purchase-2212124.htm> (Registrria also finds that 25 percent of survey respondents cite safety and recall notifications as the most important reason to register their product). See also, "Should you register that new product? Product-registration cards—and the info you put on them—aren't always needed for warranty coverage," CONSUMER REPORTS (Dec. 2013), available at <https://www.consumerreports.org/cro/2013/12/do-you-need-to-register-new-products-you-buy/index.htm> ("When you buy a toaster or TV, or receive one as a gift, is it the manufacturer's business to ask about your income, education, hobbies, and car? Frankly, no. Nevertheless, many products include registration cards harvesting personal information that companies then sell to marketers. The companies get money; you get peppered with spam and sales pitches.").

⁶⁹ 15 U.S.C. § 2056 (Consumer Product Safety Standards). See also, *Contact/FAQ*, Consumer Prod. Safety Comm'n, <https://www.cpsc.gov/About-CPSC/Contact-Information> (discussing the CPSC's authority to develop voluntary standards, issue mandatory standards, and research potential hazards), and *Voluntary Standards*, Consumer Prod. Safety Comm'n, <https://www.cpsc.gov/Regulations-Laws--Standards/Voluntary-Standards/> (discussing the development of voluntary standards in collaboration with stakeholders, such as industry groups, government agencies, and consumer groups).

⁷⁰ CPSC IoT HEARING, https://www.youtube.com/watch?v=7RdbpJ_eD98.

⁷¹ 83 Fed. Reg. 13122 (Mar. 27, 2018) ("Should certification to appropriate standards be required before IoT devices are allowed in the marketplace?").

IV. Conclusion

BCP staff hopes that this information has been of assistance in furthering CPSC's inquiry into protecting consumers from the hazards associated with Internet-connected devices. The FTC continues to devote substantial resources in this area and looks forward to working with CPSC and other stakeholders to foster competition and innovation in the IoT marketplace while protecting the safety of consumers.

A network diagram featuring several nodes connected by lines. The nodes are colored yellow, blue, green, and orange. One yellow node is enclosed in a dashed circle. The text "internet of things" is written in a large, lowercase, sans-serif font, with the "of" being smaller and positioned between "internet" and "things".

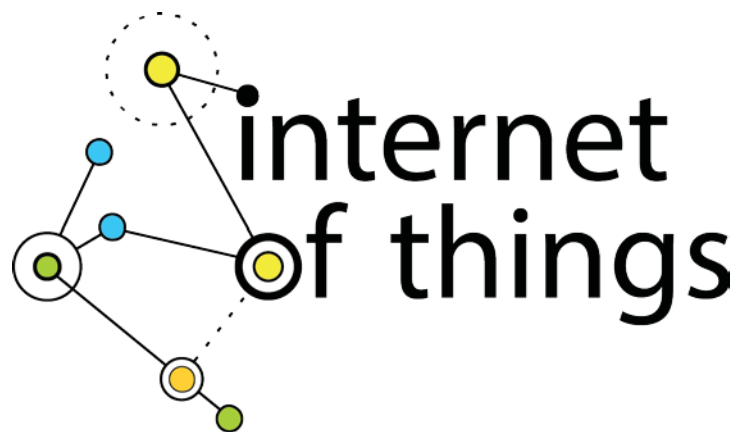
internet of things

Privacy & Security in a Connected World

A large, faint network diagram in the background, consisting of various sized circles (nodes) connected by thin lines. Some nodes are solid, while others are dashed or outlined. The diagram is spread across the bottom half of the page.

FTC Staff Report

JANUARY 2015



FTC Staff Report
January 2015

Table of Contents

Executive Summary	i
Background	1
What is the “Internet of Things”?.....	5
Benefits & Risks	7
Benefits	7
Risks	10
Application of Traditional Privacy Principles	19
Summary of Workshop Discussions.....	19
Post-Workshop Developments.....	25
Commission Staff’s Views and Recommendations for Best Practices	27
Legislation	47
Summary of Workshop Discussions.....	47
Recommendations.....	48
Conclusion	55

Executive Summary

The Internet of Things (“IoT”) refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.

Six years ago, for the first time, the number of “things” connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.

Given these developments, the FTC hosted a workshop on November 19, 2013 – titled *The Internet of Things: Privacy and Security in a Connected World*. This report summarizes the workshop and provides staff’s recommendations in this area.¹ Consistent with the FTC’s mission to protect consumers in the commercial sphere and the focus of the workshop, our discussion is limited to IoT devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, nor does it address broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Workshop participants discussed benefits and risks associated with the IoT. As to benefits, they provided numerous examples, many of which are already in use. In the health arena, connected medical devices can allow consumers with serious medical conditions to work

¹ Commissioner Wright dissents from the issuance of this Staff Report. His concerns are explained in his separate dissenting statement.

with their physicians to manage their diseases. In the home, smart meters can enable energy providers to analyze consumer energy use, identify issues with home appliances, and enable consumers to be more energy-conscious. On the road, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership. Participants generally agreed that the IoT will offer numerous other, and potentially revolutionary, benefits to consumers.

As to risks, participants noted that the IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. Participants also noted that privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions. Others noted that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.

In addition, workshop participants debated how the long-standing Fair Information Practice Principles (“FIPPs”), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability, should apply to the IoT space. The main discussions at the workshop focused on four FIPPs in particular: security, data minimization, notice, and choice. Participants also discussed how use-based approaches could help protect consumer privacy.

1. Security

There appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities. Commission staff encourages companies to consider adopting the best practices highlighted by workshop participants, including those described below.

First, companies should build security into their devices at the outset, rather than as an afterthought. As part of the security by design process, companies should consider: (1) conducting a privacy or security risk assessment; (2) minimizing the data they collect and retain; and (3) testing their security measures before launching their products. Second, with respect to personnel practices, companies should train all employees about good security, and ensure that security issues are addressed at the appropriate level of responsibility within the organization. Third, companies should retain service providers that are capable of maintaining reasonable security and provide reasonable oversight for these service providers. Fourth, when companies identify significant risks within their systems, they should implement a defense-in-depth approach, in which they consider implementing security measures at several levels. Fifth, companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network. Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

2. Data Minimization

Data minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it. Although some participants expressed concern that requiring data minimization could curtail innovative uses of data, staff agrees with the participants who stated that companies should consider reasonably limiting their collection and retention of consumer data.

Data minimization can help guard against two privacy-related risks. First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event. Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.

To minimize these risks, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff's recommendation on data minimization is a flexible one that gives companies many options. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data, as explained below.

3. Notice and Choice

The Commission staff believes that consumer choice continues to play an important role in the IoT. Some participants suggested that offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface. However, staff believes that providing notice and choice remains important.

This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits. This principle applies equally to the Internet of Things.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach. Some options include developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard. Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents. In addition, companies may want to consider using a combination of approaches.

Some participants expressed concern that even if companies provide consumers with choices only in those instances where the collection or use is inconsistent with context, such as

approach could restrict unexpected new uses of data with potential societal benefits. These participants urged that use limitations be considered as a supplement to, or in lieu of, notice and choice. With a use-based approach, legislators, regulators, self-regulatory bodies, or individual companies would set “permissible” and “impermissible” uses of certain consumer data.

Recognizing concerns that a notice and choice approach could restrict beneficial new uses of data, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. In addition, if a company collects a consumer’s data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. Furthermore, the Commission protects privacy through a use-based approach, in some instances. For example, it enforces the Fair Credit Reporting Act, which restricts the permissible uses of consumer credit report information under certain circumstances. The Commission also applies its unfairness authority to challenge certain harmful uses of consumer data.

Staff has concerns, however, about adopting a pure use-based model for the Internet of Things. First, because use-based limitations are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful. Second, use limitations alone do not address the privacy and security

risks created by expansive data collection and retention. Finally, a pure use-based model would not take into account consumer concerns about the collection of sensitive information.²

The establishment of legislative or widely-accepted multistakeholder frameworks could potentially address some of these concerns. For example, a framework could set forth permitted or prohibited uses. In the absence of consensus on such frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

4. Legislation

Participants also discussed whether legislation over the IoT is appropriate, with some participants supporting legislation, and others opposing it. Commission staff agrees with those commenters who stated that there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, in light of the ongoing threats to data security and the risk that emerging IoT technologies might amplify these threats, staff reiterates the Commission’s previous recommendation for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach. General data security legislation should protect against unauthorized access to both personal information and device functionality itself. For

² In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards, which the Commission previously recommended in its 2012 privacy report. Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness. Commission staff thus again recommends that Congress enact broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.³

In the meantime, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
The Commission enforces the FTC Act, the FCRA, the health breach notification provisions of the HI-TECH Act, the Children’s Online Privacy Protection Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws.
- **Consumer and business education:**
The Commission staff will develop new consumer and business education materials in this area.

³ Commissioner Ohlhausen does not agree with the recommendation for baseline privacy legislation. *See infra* note 191.

- **Participation in multi-stakeholder groups:**
Currently, Commission staff is participating in multi-stakeholder groups that are considering guidelines related to the Internet of Things, including on facial recognition and smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers.
- **Advocacy:**
Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area.

Background

Technology is quickly changing the way we interact with the world around us. Today, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things (“IoT”), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn’t a mobile phone, tablet, or traditional computer.

Six years ago, for the first time, the number of “things” connected to the Internet surpassed the number of people.¹ Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.² Some estimate that by 2020, 90% of consumer cars will have an Internet connection, up from less than 10 percent in 2013.³ Three and one-half billion sensors already are in the

¹ DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

² *Id.*

³ TELEFONICA, CONNECTED CAR INDUSTRY REPORT 2013 9 (2013), *available at* http://websrv.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.

marketplace,⁴ and some experts expect that number to increase to trillions within the next decade.⁵ All of these connected machines mean much more data will be generated: globally, by 2018, mobile data traffic will exceed fifteen exabytes – about 15 quintillion bytes – each month.⁶ By comparison, according to one estimate, an exabyte of storage could contain 50,000 years’ worth of DVD-quality video.⁷

These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident. And the Internet of Things may bring benefits that we cannot predict.

However, these connected devices also will collect, transmit, store, and potentially share vast amounts of consumer data, some of it highly personal. Given the rise in the number and types of connected devices already or soon to be on the market, the Federal Trade Commission (“FTC” or “Commission”) announced in April 2013 that it would host a workshop on the privacy and security issues associated with such devices and requested public input about the issues to

⁴ See Stanford Univ., *TSensors Summit™ for Trillion Sensor Roadmap 1* (Oct. 23-25, 2013), available at <http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf>.

⁵ *Id.*

⁶ CISCO, CISCO VISUAL NETWORKING INDEX: GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2013–2018 3 (2014), available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

⁷ University of Bristol, Exabyte Informatics, available at <http://www.bris.ac.uk/research/themes/exabyte-informatics.html>.

consider.⁸ In response to the request for comment, staff received twenty-nine public comments⁹ from a variety of consumer advocacy groups, academics, and industry representatives. The workshop – titled *The Internet of Things: Privacy and Security in a Connected World* – took place on November 19, 2013, and featured panels of academics, researchers, consumer advocates, and representatives from government and industry.¹⁰

The workshop consisted of four panels,¹¹ each of which focused on a different aspect of the IoT.¹² The first panel, “The Smart Home,”¹³ looked at an array of connected devices, such as home automation systems and smart appliances. The second panel, “Connected Health and Fitness,”¹⁴ examined the growth of increasingly connected medical devices and health and fitness products, ranging from casual wearable fitness devices to connected insulin pumps. The third panel, “Connected Cars,”¹⁵ discussed the different technologies involved with connected

⁸ Press Release, FTC, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-internet-things>.

⁹ Pre-workshop comments (“#484 cmt.”) are available at <http://www.ftc.gov/policy/public-comments/initiative-484>.

¹⁰ For a description of the workshop, see <http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

¹¹ In addition to the four panels, workshop speakers included Keith Marzullo of the National Science Foundation (“Marzullo”), who gave an overview of the IoT space (Transcript of Workshop at 15-34); Carolyn Nguyen (“Nguyen”) of Microsoft Corp., who discussed contextual privacy and its implications for the IoT (Transcript of Workshop at 35-51); and Vinton “Vint” Cerf (“Cerf”) of Google Inc., who gave the workshop’s Keynote Address (Transcript of Workshop at 118-153).

¹² A complete transcript of the proceeding is available at http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf. Videos of the workshop also are available at <http://www.ftc.gov/news-events/audio-video/ftc-events>.

¹³ Transcript of Workshop at 52-115.

¹⁴ *Id.* at 164-234.

¹⁵ *Id.* at 235-291.

cars, including Event Data Recorders (“EDRs”)¹⁶ and other vehicle “telematics,” a term that refers to data collection, transmission, and processing technologies for use in vehicles. Finally, the fourth panel, “Privacy and Security in a Connected World,”¹⁷ discussed the broader privacy and security issues raised by the IoT.

Following the workshop, the Commission invited comments on the issues raised by the panels.¹⁸ In response, staff received seventeen public comments from private citizens, trade organizations, and privacy advocates.¹⁹

This report summarizes the workshop and provides staff’s recommendations in this area. Section II of this report discusses how we define the “Internet of Things.” Section III describes some of the benefits and risks of the new technologies that are part of the IoT phenomenon. Section IV examines the application of existing privacy principles to these new technologies, and Section V addresses whether legislation would be appropriate in this area. Sections IV and V begin by discussing the views of written commenters and workshop speakers (collectively, “participants”), and then set forth staff recommendations. These recommendations focus on the types of products and services consumers are likely to encounter today and in the foreseeable future. We look forward to continuing to explore privacy issues as new IoT technologies come to market.

¹⁶ An EDR is “a device or function in a vehicle that records the vehicle’s dynamic time-series data during the time period just prior to a crash event (*e.g.*, vehicle speed vs. time) or during a crash event . . . intended for retrieval after the crash event.” 49 C.F.R. § 563.5.

¹⁷ Transcript of Workshop at 292-364.

¹⁸ Press Release, FTC, FTC Seeks Comment on Issues Raised at Internet of Things Workshop (Dec. 11, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-comment-issues-raised-internet-things-workshop>.

¹⁹ Post-workshop comments (“#510 cmt.”) are available at <http://www.ftc.gov/policy/public-comments/initiative-510>.

What is the “Internet of Things”?

Although the term “Internet of Things” first appeared in the literature in 2005,²⁰ there is still no widely accepted definition.²¹ One participant described the IoT as the connection of “physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing.”²² Another participant described it as including “embedded intelligence” in individual items that can detect changes in their physical state.²³ Yet another participant, noting the lack of an agreed-upon definition of the IoT, observed, “[w]hat all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data.”²⁴

The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines. For example, the term IoT can include the type of Radio Frequency Identification (“RFID”) tags that businesses place on products in stores to monitor inventory; sensor networks to monitor electricity use in hotels; and Internet-connected jet engines and drills on oil rigs. Moreover, the “things” in the IoT generally do not include desktop or laptop computers and their close analogs, such as smartphones and tablets, although these devices are often employed to control or communicate with other “things.”

²⁰ See Remarks of Marzullo, Transcript of Workshop at 19.

²¹ See *Comment of ARM/AMD*, #510 cmt. #00018 at 1.

²² *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 1.

²³ Remarks of Marzullo, Transcript of Workshop at 19.

²⁴ *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 3.

For purposes of this report, we use the term IoT to refer to “things” such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. Consistent with the FTC’s mission to protect consumers in the commercial sphere, our discussion of IoT is limited to such devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, such as sensors in hotel or airport networks; nor does it discuss broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Benefits & Risks

Like all technologies, the Internet of Things has benefits and risks. To develop policy approaches to this industry, one must understand both. Below is a summary of the benefits and risks of IoT, both current and potential, highlighted by workshop participants.

Benefits

Most participants agreed that the IoT will offer numerous, and potentially revolutionary, benefits to consumers.²⁵ One area in which these benefits appear highly promising is health care.²⁶ For example, insulin pumps and blood-pressure cuffs that connect to a mobile app can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office. This is especially beneficial for aging patients, for whom connected health devices can provide "treatment options that would allow them to manage their health care at home without the need for long-term hospital stays or transition to a long-term care facility."²⁷ Patients can also give caregivers, relatives, and doctors access to their health data through these apps, resulting in numerous benefits. As one panelist noted, connected health devices can "improve quality of life and safety by providing a richer source of data to the patient's doctor for diagnosis and treatment[,] . . . improve disease prevention, making the healthcare system more efficient and driving costs down[,] . . . [and] provide an incredible wealth of data, revolutionizing

²⁵ See *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 4; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 2.

²⁶ See *Comment of AT&T Inc.*, #484 cmt. #00004 at 5.

²⁷ *Comment of Med. Device Privacy Consortium*, #484 cmt. #00022 at 1.

medical research and allowing the medical community to better treat, and ultimately eradicate, diseases.”²⁸

Recent studies demonstrate meaningful benefits from connected medical devices. One workshop participant said that “one of the most significant benefits that we have from this connected world [is] the ability to . . . draw the patients in and engage them in their own care.”²⁹ Another participant described a clinical trial showing that, when diabetic patients used connected glucose monitors, and their physicians received that data, those physicians were five times more likely to adjust medications, resulting in better disease management and substantial financial savings for patients. He stated that the clinical trial demonstrated that diabetic patients using the connected glucose monitor reduced their average blood sugar levels by two points and that, by comparison, the Food and Drug Administration (“FDA”) considers medications that reduce blood sugar by as little as one half point to be successful.³⁰

Consumers can benefit from the IoT in many other ways. In the home, for example, smart meters can enable energy providers to analyze consumer energy use and identify issues with home appliances, “even alerting homeowners if their insulation seems inadequate compared to that of their neighbors,”³¹ thus empowering consumers to “make better decisions about how they use electricity.”³² Home automation systems can provide consumers with a “single platform that

²⁸ *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 16.

²⁹ *See* Remarks of Stan Crosley, Indiana Univ. (“Crosley”), Transcript of Workshop at 199.

³⁰ *See* Remarks of Anand Iyer, WellDoc Communications, Inc. (“Iyer”), Transcript of Workshop at 188–189.

³¹ *Comment of AT&T Inc.*, #484 cmt. #00004 at 4-5.

³² Remarks of Eric Lightner, Department of Energy (“Lightner”), Transcript of Workshop at 54.

can connect all of the devices within the home, [with] a single app for controlling them.”³³

Connected ovens allow consumers to “set [their] temperatures remotely . . . , go from bake to broil . . . , [and] monitor [their] products from various locations inside . . . and outside [their] home[s].”³⁴ Sensors known as “water bugs” can notify consumers if their basements have flooded,³⁵ and wine connoisseurs can monitor the temperature in their wine cellars to preserve their finest vintages.³⁶

On the road, connected cars will increasingly offer many safety and convenience benefits to consumers. For example, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership.³⁷ Connected cars also can “offer real-time vehicle diagnostics to drivers and service facilities; Internet radio; navigation, weather, and traffic information; automatic alerts to first responders when airbags are deployed; and smartphone control of the starter and other aspects of the car.”³⁸ In the future, cars will even drive themselves. Participants discussed the ability of self-driving cars to create safety benefits. For example, rather than having error-prone humans decide which car should go first at a four-way stop sign, self-driving cars will be able to figure out who should

³³ Remarks of Jeff Hagins, SmartThings (“Hagins”), Transcript of Workshop at 64.

³⁴ Remarks of Michael Beyerle, GE Appliances (“Beyerle”), Transcript of Workshop at 60.

³⁵ See Remarks of Scott Peppet, Univ. of Colorado School of Law (“Peppet”), Transcript of Workshop at 167.

³⁶ See Remarks of Cerf, Transcript of Workshop at 132.

³⁷ See Remarks of Christopher Wolf, Future of Privacy Forum (“Wolf”), Transcript of Workshop at 247-48.

³⁸ *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 13.

go first according to a standard protocol.³⁹ They would also allow people with visual impairments to use their own cars as a mode of transportation.⁴⁰

Risks

Despite these important benefits, there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks.⁴¹

SECURITY RISKS

According to panelists, IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below.

First, on IoT devices, as with desktop or laptop computers, a lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the

³⁹ See Remarks of Cerf, Transcript of Workshop at 127.

⁴⁰ See *id.* at 138.

⁴¹ See, e.g., Remarks of Craig Heffner, Tactical Network Solutions (“Heffner”), Transcript of Workshop at 73-77, 109-10; Remarks of Lee Tien, Electronic Frontier Foundation (“Tien”), Transcript of Workshop at 82-83; Remarks of Hagins, Transcript of Workshop at 92-93, 110; Remarks of Jay Radcliffe, InGuardians, Inc. (“Radcliffe”), Transcript of Workshop at 182-84; Remarks of Iyer, Transcript of Workshop at 223; Remarks of Tadayoshi Kohno, Univ. of Washington (“Kohno”), Transcript of Workshop at 244-47, 263-64; Remarks of David Jacobs, Electronic Privacy Information Center (“Jacobs”), Transcript of Workshop at 296; Remarks of Marc Rogers, Lookout, Inc. (“Rogers”), Transcript of Workshop at 344-45. See also, e.g., HP, INTERNET OF THINGS RESEARCH STUDY 5 (2014), available at <http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en> (“HP Security Research reviewed 10 of the most popular devices in some of the most common IoT niches revealing an alarmingly high average number of vulnerabilities per device. Vulnerabilities ranged from Heartbleed to denial of service to weak passwords to cross-site scripting.”); *id.* at 4 (noting that 80 percent of devices tested raised privacy concerns).

device. For example, new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer.⁴² Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud.⁴³ Thus, as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.⁴⁴

Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems.⁴⁵ For example,

⁴² See, e.g., Erica Fink & Laurie Segall, *Your TV might be watching you*, CNN MONEY (Aug. 1, 2013), available at <http://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html> ("Today's high-end televisions are almost all equipped with 'smart' PC-like features, including Internet connectivity, apps, microphones and cameras.").

⁴³ See Mario Ballano Barcena *et al.*, *Security Response, How safe is your quantified self?*, SYMANTEC (Version 1.1 – Aug. 11, 2014), available at www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf (noting risks relating to IoT including identity theft). According to the most recent statistics from the Bureau of Justice Statistics of the Department of Justice, an estimated 16.6 million Americans – about seven percent of Americans sixteen or older – experienced at least one incident of identity theft in 2012. Losses due to personal identity theft totaled \$24.7 billion, billions of dollars more than the losses for all other property crimes combined. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012 (Dec. 2013)), available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf>. Another study demonstrated that one in four people who received notice of a breach involving their personal information were victims of identity theft, a significantly higher figure than for individuals who did not receive a breach notice. See Javelin, 2013 Identity Fraud Report, available at <https://www.javelinstrategy.com/brochure/276>.

⁴⁴ See, e.g., Remarks of Marzullo, Transcript of Workshop at 18-19 (discussing ubiquitous or pervasive computing); *id.* at 28-30 (discussing potential security vulnerabilities in devices ranging from pacemakers to automobiles); Remarks of Nguyen, Transcript of Workshop at 35 ("the first thing that really comes to mind are the sensors that are expected to be ubiquitously present and the potential for everything inanimate, whether it be in the home, in the car, or attached to the individual, to measure and transmit data").

⁴⁵ See Remarks of Heffner, Transcript at 113 ("[I]f I, as someone out on the Internet, can break into a device that is inside your network, I am now inside your network and I can access other things that you do care about . . . There should never be a device on your network that you shouldn't care about the security of.").

a compromised IoT device could be used to launch a denial of service attack.⁴⁶ Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks.⁴⁷ Another possibility is that a connected device could be used to send malicious emails.⁴⁸

Third, unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases. One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine.⁴⁹ Another participant discussed a set of experiments where an attacker could gain “access to the car’s internal computer network without ever physically touching the car.”⁵⁰ He described how he was able to hack into a car’s built-in telematics unit and control the vehicle’s engine and braking, although he noted that “the risk to car owners today is incredibly small,” in part because “all the automotive manufacturers that I know of are proactively trying to address these things.”⁵¹ Although the risks currently may be small, they could be amplified as fully

⁴⁶ See, e.g., Dick O’Brien, *The Internet of Things: New Threats Emerge in a Connected World*, SYMANTEC (Jan. 21, 2014), available at www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world (describing worm attacking IoT devices that connects them to a botnet for use in denial of service attacks).

⁴⁷ *Id.*

⁴⁸ See Paul Thomas, *Despite the News, Your Refrigerator is Not Yet Sending Spam*, SYMANTEC (Jan. 23, 2014), available at <http://www.symantec.com/connect/blogs/despise-news-your-refrigerator-not-yet-sending-spam> (debunking reports that an Internet worm had used compromised IoT devices to send out spam, but adding, “While malware for IoT devices is still in its infancy, IoT devices are susceptible to a wide range of security concerns. So don’t be surprised if, in the near future, your refrigerator actually does start sending spam.”).

⁴⁹ See Remarks of Radcliffe, Transcript of Workshop at 182. See also Remarks of Tien, Transcript of Workshop at 82-83 (“And obviously one of the big differences between, say, a problem with your phone and a problem with your . . . diabetes pump or your defibrillator is that if it is insecure and it is subject to any kind of malware or attack, it is much more likely there would be very serious physical damage.”).

⁵⁰ Remarks of Kohno, Transcript of Workshop at 245.

⁵¹ See *id.* at 245-47, 266.

automated cars, and other automated physical objects, become more prevalent. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns.⁵² Likewise, unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home.

These potential risks are exacerbated by the fact that securing connected IoT devices may be more challenging than securing a home computer, for two main reasons. First, as some panelists noted, companies entering the IoT market may not have experience in dealing with security issues.⁵³ Second, although some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable.⁵⁴ In those cases, if a vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch.⁵⁵ And if an update is available, many consumers may never hear about it.⁵⁶ Relatedly, many

⁵² See discussion of TRENDnet, *infra* notes 132-34 and accompanying text (FTC settlement alleging that hackers were able to access video streams from TRENDnet cameras). In another notorious incident, a hacker gained access to a video and audio baby monitor. See Chris Matyszczyk, *Hacker Shouts at Baby Through Baby Monitor*, CNET (Apr. 29, 2014), available at www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/. See also Kashmir Hill, 'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users, FORBES (Aug. 27, 2013), available at www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/ (recounting a similar incident).

⁵³ Remarks of Tien, Transcript of Workshop at 71; Remarks of Heffner, Transcript of Workshop at 73-75; Remarks of Hagins, Transcript of Workshop at 92-93.

⁵⁴ See *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2.

⁵⁵ See, e.g., Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 9 (Sept. 16, 2014) ("Article 29 Working Group Opinion"), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ("For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries.").

⁵⁶ *Id.* See also Hill, *supra* note 52 (noting that some 40,000 of 46,000 purchasers of connected cameras had not installed a firmware update addressing a security vulnerability).

companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.⁵⁷

PRIVACY RISKS

In addition to risks to security, participants identified privacy risks flowing from the Internet of Things. Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information – risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time,⁵⁸ which may allow an entity that has not directly collected sensitive information to infer it.

The sheer volume of data that even a small number of devices can generate is stunning: one participant indicated that fewer than 10,000 households using the company’s IoT home-automation product can “generate 150 million discrete data points a day”⁵⁹ or approximately one data point every six seconds for each household.⁶⁰

⁵⁷ See, e.g., Bruce Schneier, *The Internet of Things Is Wildly Insecure — And Often Unpatchable*, WIRED (Jan. 6, 2014), available at <http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem> (“The problem with this process is that no one entity has any incentive, expertise, or even ability to patch the software once it’s shipped. The chip manufacturer is busy shipping the next version of the chip, and the [original device manufacturer] is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn’t a priority.”).

⁵⁸ See, e.g., Remarks of Tien, Transcript of Workshop at 67; *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 4-5.

⁵⁹ Remarks of Hagins, Transcript of Workshop at 89.

⁶⁰ Cf. *infra* note 73 and accompanying text (discussing inferences possible from smart meter readings taken every two seconds).

Such a massive volume of granular data allows those with access to the data to perform analyses that would not be possible with less rich data sets.⁶¹ According to a participant, “researchers are beginning to show that existing smartphone sensors can be used to infer a user’s mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson’s disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement.”⁶² This participant noted that such inferences could be used to provide beneficial services to consumers, but also could be misused. Relatedly, another participant referred to the IoT as enabling the collection of “sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals.”⁶³ Some panelists cited to general privacy risks associated with these granular information-collection practices, including the concern that the trend towards abundant collection of data creates a “non-targeted dragnet collection from devices in the environment.”⁶⁴

Others noted that companies might use this data to make credit, insurance, and employment decisions.⁶⁵ For example, customers of some insurance companies currently may opt into programs that enable the insurer to collect data on aspects of their driving habits – such

⁶¹ See Article 29 Working Group Opinion, *supra* note 55, at 8 (“Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.”).

⁶² Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 115-16 (2014) (citations omitted) (“*Regulating the Internet of Things*”), available at <http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf>. Although we do not include smartphones in our definition of IoT (*see supra* p. 6), many IoT devices contain sensors similar to the sensors in smartphones, and therefore, similar types of inferences may be possible using data from IoT devices.

⁶³ *Comment of Elec. Privacy Info. Ctr.*, #484 cmt. #00011 at 3.

⁶⁴ Remarks of Tien, Transcript of Workshop at 67.

⁶⁵ See Remarks of Peppet, Transcript of Workshop at 169.

as in one case, the number of “hard brakes,” the number of miles driven, and the amount of time spent driving between midnight and 4 a.m. – to help set the insurance rate.⁶⁶ Use of data for credit, insurance, and employment decisions could bring benefits – *e.g.*, enabling safer drivers to reduce their rates for car insurance or expanding consumers’ access to credit – but such uses could be problematic if they occurred without consumers’ knowledge or consent, or without ensuring accuracy of the data.

As a further example, one researcher has hypothesized that although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user’s suitability for credit or employment (*e.g.*, a conscientious exerciser is a good credit risk or will make a good employee).⁶⁷ According to one commenter, it would be of particular concern if this type of decision-making were to systematically bias companies against certain groups that do not or cannot engage in the favorable conduct as much as others or lead to discriminatory practices against protected classes.⁶⁸

Participants noted that the Fair Credit Reporting Act (“FCRA”)⁶⁹ imposes certain limits on the use of consumer data to make determinations about credit, insurance, or employment, or for similar purposes.⁷⁰ The FCRA imposes an array of obligations on entities that qualify as

⁶⁶ See Peppet, *Regulating the Internet of Things*, *supra* note 62, at 106-07. See also, *e.g.*, Progressive, Snapshot Common Questions, available at <http://www.progressive.com/auto/snapshot-common-questions/>; StateFarm, Drive Safe & Save with In-Drive, available at <https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/indrive>.

⁶⁷ See Remarks of Peppet, Transcript of Workshop at 167-169.

⁶⁸ See *id.* at 93, 123-24.

⁶⁹ 15 U.S.C. § 1681 *et seq.*

⁷⁰ See, *e.g.*, Remarks of Crosley, Transcript of Workshop at 213; Remarks of Peppet, Transcript of Workshop at 213; Peppet, *Regulating the Internet of Things*, *supra* note 62, at 126-127.

consumer reporting agencies, such as employing reasonable procedures to ensure maximum possible accuracy of data and giving consumers access to their information.⁷¹ However, the FCRA excludes most “first parties” that collect consumer information; thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers’ connected devices and use the data to make in-house credit, insurance, or other eligibility decisions – something that could become increasingly common as the IoT develops. For example, an insurance company may offer consumers the option to submit data from a wearable fitness tracker, in exchange for the prospect of lowering their health insurance premium. The FCRA’s provisions, such as those requiring the ability to access the information and correct errors, may not apply in such circumstances.

Yet another privacy risk is that a manufacturer or an intruder could “eavesdrop” remotely, intruding into an otherwise private space. Companies are already examining how IoT data can provide a window into the previously private home.⁷² Indeed, by intercepting and analyzing unencrypted data transmitted from a smart meter device, researchers in Germany were

⁷¹ See 15 U.S.C. §§1681e, 1681j.

⁷² See, e.g., Louise Downing, *WPP Unit, Onzo Study Harvesting Smart-Meter Data*, BLOOMBERG (May 12, 2014), available at <http://origin-www.bloomberg.com/apps/news?pid=conewsstory&tkr=WPP:LN&sid=aPY7EUU9oD6g> (reporting that the “world’s biggest advertising agency” and a software company are collaborating to explore uses of smart meter data and quoting a CEO who noted, “Consumers are leaving a digital footprint that opens the door to their online habits and to their shopping habits and their location, and the last thing that is understood is the home, because at the moment, when you shut the door, that is it.”). See also *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2-3 (“to the extent that a powerful commercial entity controls an IoT networking platform within a home or business, that positions them to collect, analyze, and act upon copious amounts of data from within traditionally private spaces.”).

able to determine what television show an individual was watching.⁷³ Security vulnerabilities in camera-equipped devices have also raised the specter of spying in the home.⁷⁴

Finally, some participants pointed out that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential and may result in less widespread adoption.⁷⁵ As one participant stated, “promoting privacy and data protection principles remains paramount to ensure societal acceptance of IoT services.”⁷⁶

⁷³ See Dario Carluccio & Stephan Brinkhaus, Presentation: “Smart Hacking for Privacy,” 28th Chaos Communication Congress, Berlin, December 2011, *available at* <https://www.youtube.com/watch?v=YYe4SwQn2GE&feature=youtu.be>. Moreover, “the two-second reporting interval provides so much data that [the researchers] were able to accurately chart power usage spikes and lulls indicative of times a homeowner would be home, asleep or away.” *Id.* (In most smart meter implementations, data is reported at much longer intervals, usually fifteen minutes.) In addition to the privacy concerns, as noted above, the researchers discovered that the encryption was not implemented properly and that they could alter the energy consumption data reported by the meter. *Id.*

⁷⁴ See, e.g., Fink & Segall, *supra* note 42 (describing a security vulnerability in Samsung smart TVs, since patched, that “enabled hackers to remotely turn on the TVs’ built-in cameras without leaving any trace of it on the screen”).

⁷⁵ See, e.g., *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 17-18; *Comment of CTIA – The Wireless Ass’n*, #510 cmt. #00014 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5.

⁷⁶ *Comment of GSI US*, #484 cmt. #00030 at 4.

Application of Traditional Privacy Principles

Summary of Workshop Discussions

Participants debated how the long-standing Fair Information Practice Principles (“FIPPs”) of notice, choice, access, accuracy, data minimization, security, and accountability should apply to the IoT space. While some participants continued to support the application of all of the FIPPs,⁷⁷ others argued that data minimization, notice, and choice are less suitable for protecting consumer privacy in the IoT.⁷⁸

The FIPPs were first articulated in 1973 in a report by what was then the U.S. Department of Health, Education and Welfare.⁷⁹ Subsequently, in 1980, the Organization for Economic Cooperation and Development (“OECD”) adopted a set of privacy guidelines, which embodied the FIPPs.⁸⁰ Over time, the FIPPs have formed the basis for a variety of both government and private sector initiatives on privacy. For example, both the European Union

⁷⁷ See, e.g., Remarks of Michelle Chibba, Office of the Information and Privacy Commissioner, Ontario, Canada (“Chibba”), Transcript of Workshop at 329; Remarks of Jacobs, Transcript of Workshop at 328-329; *Comment of AAA*, #510 cmt. #00012 at 2; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3.

⁷⁸ See, e.g., *Comment of GSI US*, #484 cmt. #00030 at 5; *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3.

⁷⁹ See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.27 (1998), available at <http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

⁸⁰ See OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm>. (In 2013, the OECD updated its guidelines to address risk management, interoperability, and other issues. The update is available at <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>). See also FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 3-4, 43 n.25 (2000).

Directive on the protection of personal data⁸¹ and the Health Insurance Portability and Accountability Act (“HIPAA”)⁸² are based, in large part, on the FIPPs. In addition, many self-regulatory guidelines include the principles of notice, choice, access, and security.⁸³ The Obama Administration’s Consumer Privacy Bill of Rights also includes these principles,⁸⁴ as does the privacy framework set forth in the Commission’s 2012 Privacy Report.⁸⁵

Workshop discussion focused on four FIPPs in particular – data security, data minimization, notice, and choice. As to data security, there was widespread agreement on the need for companies manufacturing IoT devices to incorporate reasonable security into these devices. As one participant stated, “Inadequate security presents the greatest risk of actual consumer harm in the Internet of Things.”⁸⁶ Accordingly, as another participant noted,

⁸¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

⁸² Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

⁸³ See, e.g., NETWORK ADVERTISING INITIATIVE, NAI CODE OF CONDUCT 2013, available at http://www.networkadvertising.org/2013_Principles.pdf; INTERNET ADVERTISING BUREAU, INTERACTIVE ADVERTISING PRIVACY PRINCIPLES (Feb. 24, 2008), available at <http://www.iab.net/guidelines/508676/1464>.

⁸⁴ THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

⁸⁵ FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS vii-viii (2012) (“Privacy Report”), available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>. Commissioners Ohlhausen and Wright were not members of the Commission at that time and thus did not offer any opinion on that matter.

⁸⁶ *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 9 (and listing types of security measures that are already being implemented to secure the IoT).

“[s]ecurity must be built into devices and networks to prevent harm and build consumer trust in the IoT.”⁸⁷

Participants were more divided about the continuing applicability of the principles of data minimization, notice, and choice to the IoT.⁸⁸ With respect to data minimization – which refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it – one participant expressed concerns that requiring fledgling companies to predict what data they should minimize would “chok[e] off potential benefits and innovation.”⁸⁹ A second participant cautioned that “[r]estricting data collection with rules like data minimization could severely limit the potential opportunities of the Internet of Things” based on beneficial uses that could be found for previously-collected data that were not contemplated at the time of collection.⁹⁰ Still another participant noted that “[d]ata-driven innovation, in many ways, challenges many interpretations of data minimization where data purpose specification and use limitation are overly rigid or prescriptive.”⁹¹

With respect to notice and choice, some participants expressed concern about its feasibility, given the ubiquity of IoT devices and the persistent and pervasive nature of the

⁸⁷ *Comment of Infineon Tech. N. Am. Corp.*, #510 cmt. #00009 at 2; *see also* Remarks of Rogers, Transcript of Workshop at 312 (“There are some pretty good examples out there of what happens to companies when security becomes an afterthought and the cost that companies can incur in trying to fight the damage, the cost to brand reputation, the loss of customer confidence. And there are also some great examples of companies, even in the Internet of Things, as new as it is, companies that have gotten it right and they’ve done well. And they’ve gone on to push out products where there have been no issues.”).

⁸⁸ *See, e.g., Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3-4.

⁸⁹ Remarks of Dan Caprio, McKenna, Long & Aldridge, LLP (“Caprio”), Transcript of Workshop at 339.

⁹⁰ *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 3.

⁹¹ *Comment of Software & Info. Indus. Ass’n*, #484 cmt. #00025 at 6-7; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013 at 5 (purpose specification and data minimization as applied to the IoT “risks unduly limiting the development of new services and the discoveries that may follow from valuable research”).

information collection that they make possible. As one participant observed, when “a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . are measuring all sorts of things,” it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.⁹² Another participant talked about the risk that, if patients have “to consent to everything” for a health monitoring app, “patients will throw the bloody thing away.”⁹³ Yet another participant noted that any requirement to obtain consent could be “a barrier to socially beneficial uses of information.”⁹⁴

A related concern is that many IoT devices – such as home appliances or medical devices – have no screen or other interface to communicate with the consumer, thereby making notice on the device itself difficult, if not impossible.⁹⁵ For those devices that do have screens, the screens may be smaller than even the screens on mobile devices, where providing notice is already a challenge.⁹⁶ Finally, even if a device has screens, IoT sensors may collect data at times when the consumer may not be able to read a notice (for example, while driving).⁹⁷

⁹² Remarks of Peppet, Transcript of Workshop at 215–16.

⁹³ Remarks of Iyer, Transcript of Workshop at 230.

⁹⁴ *Comment of Software & Info. Indus. Ass’n*, #484 cmt. #00025 at 8.

⁹⁵ See, e.g., *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 2 and 6; *Comment of Transatl. Computing Continuum Policy Alliance*, #510 cmt. #00017 at 2.

⁹⁶ See FTC STAFF REPORT, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 10–11 (2013) (“Mobile Disclosures Report”), available at <http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>.

⁹⁷ In addition, some participants also suggested that notice and choice is not workable for IoT products and services that are not consumer-facing – e.g., a sensor network to monitor electricity use in hotels. See, e.g., *Comment of GSI US*, #484 cmt. #00030 at 5 (noting that “[i]t is difficult to anticipate how the existing mechanisms of notice and choice, both being sound principles for privacy protection, would apply to sensors. . . . [H]ow would one provide adequate notice for every embedded sensor network? How would consent be obtained?”); *Comment of Future of*

Despite these challenges, participants discussed how companies can provide data minimization, notice, and choice within the IoT. One participant suggested that, as part of a data minimization exercise, companies should ask themselves a series of questions, such as whether they need a particular piece of data or whether the data can be deidentified.⁹⁸ Another participant gave a specific example of how data could be minimized in the context of connected cars. This participant noted that the recording device on such cars could “automatically delete old data after a certain amount of time, or prevent individual data from being automatically synched with a central database.”⁹⁹

As to notice and choice, one auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in “[p]lain language and multiple choices of levels.”¹⁰⁰ Another discussed a “consumer profile management portal[]” approach that would include privacy settings menus that consumers can configure and revisit,¹⁰¹ possibly on a separate device such as a smartphone or a webportal. In addition to the types of specific settings and choices, another participant suggested that devices and their associated platforms could enable consumers to aggregate choices into “packets.”¹⁰² Finally, one participant noted that

Privacy Forum, #510 cmt. #00013, Appendix A at 4. As noted above, this report addresses privacy and security practices for consumer-facing products.

⁹⁸ Remarks of Chibba, Transcript of Workshop at 300-01.

⁹⁹ Comment of EPIC, #484 cmt. #00011 at 17-18.

¹⁰⁰ Remarks of Kenneth Wayne Powell, Toyota Technical Center (“Powell”), Transcript of Workshop at 278.

¹⁰¹ *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

¹⁰² Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology (“Hall”), Transcript of Workshop at 216.

companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize privacy choices.¹⁰³

Some participants advocated for an increased focus on certain types of use restrictions to protect consumer data.¹⁰⁴ With this approach, legislators, regulators, self-regulatory bodies, or individual companies would set “permissible” and “impermissible” uses of certain consumer data. One commenter characterized this approach as “shifting responsibility away from data subjects toward data users, and increasing the emphasis on responsible data stewardship and accountability.”¹⁰⁵

Participants offered a variety of approaches to adding use-based data protections. One participant proposed that companies “tag” data with its appropriate uses so that automated processes could identify and flag inappropriate uses.¹⁰⁶ Other participants noted that policymakers could constrain certain uses of IoT data that do not comport with consumer expectations and present the most risk of harm, either through law¹⁰⁷ or through voluntary

¹⁰³ Remarks of Nguyen, Transcript of Workshop at 48.

¹⁰⁴ See Remarks of Peppet, Transcript of Workshop at 210-211 (advocating “drawing some lines around acceptable use” through legislation or regulation in addition to notice and choice); see also Remarks of Crosley at 213 (supporting “the appropriate use of the context”); Remarks of Hall at 214 (expressing support for “[u]se restrictions, as long as they have teeth. That’s why I think vanilla self-regulatory efforts are probably not the answer. You need to have something that is enforced by an independent body”).

¹⁰⁵ Comment of Software & Information Industry Association, #484 cmt #00025 at 8.

¹⁰⁶ *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 10–11 (citing Hal Abelson, *Information Accountability as the Foundation of 21st Century Privacy Protection* (2013), available at http://kit.mit.edu/sites/default/files/documents/Abelson_MIT_KIT_2013_Conference.pdf). We note that such an approach would require coordination and potential associated costs.

¹⁰⁷ See Peppet, *Regulating the Internet of Things*, *supra* note 62, at 149 (proposing regulatory constraints).

self-regulatory efforts¹⁰⁸ or seal programs.¹⁰⁹ For example, as one participant has pointed out, some state laws restrict access by auto insurance companies and other entities to consumers' driving data recorded by an EDR.¹¹⁰

Post-Workshop Developments

Since the November 2013 workshop, the IoT marketplace has continued to develop at a remarkable pace. For example, in June 2014, Apple announced "HealthKit," a platform that "functions as a dashboard for a number of critical metrics as well as a hub for select third-party fitness products,"¹¹¹ as a way to help protect health information that some connected devices may collect. Similarly, in October 2014, Microsoft announced Microsoft Health, a "cloud-based service that ... provid[es] actionable insights based on data gathered from the fitness devices and apps" and which will work in conjunction with Microsoft's HealthVault, which for a decade has offered "a trusted place to store health information and share it with medical professionals on a security-enhanced platform."¹¹² And last November, Intel announced a "new platform ...

¹⁰⁸ See, e.g., *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 7; *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010 at 2; *Comment of CTIA – The Wireless Ass'n*, # 510 cmt. #00014 at 4; *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

¹⁰⁹ See, e.g., *Comment of AT&T Inc.*, #484 cmt. #00004 at 9–10; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 13.

¹¹⁰ Peppet, *Regulating the Internet of Things*, *supra* note 62, at 153-54.

¹¹¹ Rachel King, *Apple takes app-based approach to health tech with HealthKit*, ZDNet (June 2, 2014), available at <http://www.zdnet.com/article/apple-takes-app-based-approach-to-health-tech-with-healthkit/>.

¹¹² Microsoft Health, <http://www.microsoft.com/Microsoft-Health/en-us> (last visited Jan. 9, 2015).

designed to make it easier for developers to connect devices securely, bring device data to the cloud, and make sense of that data with analytics.”¹¹³

Policymakers have also tried to keep pace with these developments in the IoT. For example, in May 2014, the White House released a Big Data report (“White House Big Data Report”), and the President’s Council of Advisors on Science and Technology released a companion report (“PCAST Report”). Both reports weigh in on the debate between the application of data minimization, notice, and choice versus use limitations. The White House Big Data Report opined that “the notice and consent framework threatens to be overcome” in certain instances, “such as the collection of ambient data by our household appliances.”¹¹⁴ The White House Big Data Report concluded that,

Putting greater emphasis on a responsible use framework has many potential advantages. It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.¹¹⁵

Attention to the impact of the IoT spans the globe. In September 2014, Europe’s Article 29 Working Group – composed of data protection authorities of EU member countries – issued

¹¹³ Aaron Tilley, Intel Releases New Platform To Kickstart Development In The Internet Of Things, FORBES (Dec. 9, 2014), available at <http://www.forbes.com/sites/aarontilley/2014/12/09/intel-releases-new-platform-to-kickstart-development-in-the-internet-of-things/>.

¹¹⁴ Executive Office of the President, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 2014) (“White House Big Data Report”) at 56, available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. See also President’s Council of Advisors on Science and Technology, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (May 2014), available at <http://www.whitehouse.gov/administration/eop/ostp/pcast>.

¹¹⁵ *White House Big Data Report* at 56.

an Opinion on Recent Developments on the Internet of Things.¹¹⁶ In the opinion, the Working Group emphasized the importance of user choice, noting that “users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific.”

In addition to policy work by government agencies, standards organizations related to the Internet of Things continue to proliferate. One such area for standard-setting is data security. For example, in August 2014, oneM2M, a global standards body, released a proposed security standard for IoT devices. The standard addresses issues such as authentication, identity management, and access control.¹¹⁷

Commission Staff’s Views and Recommendations for Best Practices

This section sets forth the Commission staff’s views on the issues of data security, data minimization, and notice and choice with respect to the IoT and provides recommendations for best practices for companies.

DATA SECURITY

As noted, there appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Participants also discussed a number of specific security best practices. The Commission staff encourages companies to consider adopting these

¹¹⁶ Article 29 Working Group Opinion, *supra* note 55.

¹¹⁷ See oneM2M, *Technical Specification, oneM2M Security Solutions* at 15-16, available at http://www.onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf.

practices. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities. Nonetheless, the specific security best practices companies should consider include the following:

First, companies should implement “security by design” by building security into their devices at the outset, rather than as an afterthought.¹¹⁸ One participant stated that security should be designed into every IoT product, at every stage of development, including “early on in the design cycle of a technology.”¹¹⁹ In addition, a company should do a privacy or security risk assessment, consciously considering the risks presented by the collection and retention of consumer information.¹²⁰ As part of this process, companies should incorporate the use of smart defaults, such as requiring consumers to change default passwords – if they use default passwords at all – during the set-up process.¹²¹ Companies also should consider how to minimize the data they collect and retain, as discussed further below. Finally, companies should test their security measures before launching their products. As one participant pointed out, such testing should occur because companies – and service providers they might use to help develop their

¹¹⁸ *Comment of ARM and AMD*, #510 cmt. #00018 at 2; *see also* Remarks of Hagins, Transcript of Workshop at 111; Remarks of Jacobs, Transcript of Workshop at 296; Remarks of Caprio, Transcript of Workshop at 298.

¹¹⁹ Remarks of Kohno, Transcript of Workshop at 281.

¹²⁰ Remarks of Chibba, Transcript of Workshop at 301; *see also* Remarks of Rogers, Transcript of Workshop at 343.

¹²¹ *See generally* Remarks of Rogers, Transcript of Workshop at 344 (“Default passwords are something that should never pass through into production space. It’s an easy thing to pick up with a very basic assessment, yet we are constantly seeing these come through because these companies aren’t often doing this kind of assessment – so they see it as a hindrance, an extra step. Or they claim the consumer should be responsible for setting the security, once it lands on the consumer’s desk which, at the end of the day, the consumers aren’t capable of setting that level of security, nor should they have to.”).

products – may simply forget to close “backdoors” in their products through which intruders could access personal information or gain control of the device.¹²²

This last point was illustrated by the Commission’s recent actions against the operators of the Credit Karma and Fandango mobile apps. In these cases, the companies overrode the settings provided by the Android and iOS operating systems, so that SSL encryption was not properly implemented. As a result, the Commission alleged, hackers could decrypt the sensitive consumer financial information being transmitted by the apps. The orders in both cases include provisions requiring the companies to implement reasonable security.¹²³

Second, companies must ensure that their personnel practices promote good security. As part of their personnel practices, companies should ensure that product security is addressed at the appropriate level of responsibility within the organization. One participant suggested that “if someone at an executive level has responsibility for security, it tends to drive hiring and processes and mechanisms throughout the entire organization that will improve security.”¹²⁴ Companies should also train their employees about good security practices, recognizing that technological expertise does not necessarily equate to security expertise. Indeed, one participant stated that being able to write software code “doesn’t mean...understand[ing] anything whatsoever about the security of an embedded device.”¹²⁵

¹²² See generally Remarks of Heffner, Transcript of Workshop at 73-74.

¹²³ Credit Karma, Inc., File No. 132-3091 (Mar. 28, 2014) (consent), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc>; Fandango, LLC, File No. 132-3089 (Mar. 28, 2014) (consent), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc>. See also HTC America, Inc., No. C-4406 (July 2, 2013) (consent) (alleging that HTC, among other things, failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter>.

¹²⁴ Remarks of Hagins, Transcript of Workshop at 110.

¹²⁵ *Id.* at 92.

Third, companies must work to ensure that they retain service providers that are capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so. Failure to do so could result in an FTC law enforcement action. For example, in the Commission’s recent settlement with GMR Transcription Services, the Commission alleged that a medical and legal transcription company outsourced transcription services to independent typists in India without adequately checking to make sure they could implement reasonable security measures. According to the Commission’s complaint, among other things, the service provider stored transcribed notes in clear text on an unsecured server. As a result, U.S. consumers found their doctors’ notes of their physical examinations freely available through Internet searches. This case illustrates the strong need for appropriate service provider oversight.

Fourth, for systems with significant risk, companies should implement a defense-in-depth approach, where security measures are considered at several levels. For example, participants raised concerns about relying on the security of consumers’ own networks, such as passwords for their Wi-Fi routers, alone to protect the information on connected devices.¹²⁶ They noted that companies must take “additional steps to encrypt [the information] or otherwise secure it.”¹²⁷ FTC staff shares these concerns and encourages companies to take additional steps to secure information passed over consumers’ home networks. Indeed, encryption for sensitive information, such as that relating to health, is particularly important in this regard.¹²⁸ Regardless of the specific technology, companies should reasonably secure data in transit and in storage.

¹²⁶ *Id.* at 102.

¹²⁷ Remarks of Heffner, Transcript of Workshop at 102-03.

¹²⁸ Remarks of Hall, Transcript of Workshop at 178-79.

Fifth, panelists noted that companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network.¹²⁹ In the IoT ecosystem, strong authentication could be used to permit or restrict IoT devices from interacting with other devices or systems. The privileges associated with the validated identity determine the permissible interactions between the IoT devices and could prevent unauthorized access and interactions.¹³⁰ In implementing these protections, companies should ensure that they do not unduly impede the usability of the device. As noted above, the proposed oneM2M security standard includes many of the recommendations discussed above.¹³¹ Such efforts are important to the success of IoT.

Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities. Many IoT devices have a limited life cycle, resulting in a risk that consumers will be left with out-of-date IoT devices that are vulnerable to critical, publicly known security or privacy bugs. Companies may reasonably decide to limit the time during which they provide security updates and software patches, but it is important that companies weigh these decisions carefully. Companies should also be forthright in their representations about providing ongoing security updates and software patches. Disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe 'expiration dates' for their commodity Internet-

¹²⁹ See, e.g., BRETT C. TJADEN, FUNDAMENTALS OF SECURE COMPUTER SYSTEMS 5 (2004). See also HP, INTERNET OF THINGS RESEARCH STUDY, *supra* note 41, at 4-5 (noting that approximately 60% of IoT devices examined had weak credentials).

¹³⁰ There may be other appropriate measures, as the security measures that a company should implement vary, depending on the risks presented by unauthorized access to the device, and the sensitivity of any information collected.

¹³¹ oneM2M Candidate Release August 2014, available at <http://www.onem2m.org/technical/candidate-release-august-2014> (last visited Dec. 19, 2014).

connected devices. In addition, companies that do provide ongoing support should also notify consumers of security risks and updates.

Several of these principles are illustrated by the Commission's first case involving an Internet-connected device. TRENDnet¹³² marketed its Internet-connected cameras for purposes ranging from home security to baby monitoring, claiming that they were "secure." In its complaint, the Commission alleged, among other things, that the company transmitted user login credentials in clear text over the Internet, stored login credentials in clear text on users' mobile devices, and failed to test consumers' privacy settings to ensure that video feeds marked as "private" would in fact be private.¹³³ As a result of these alleged failures, hackers were able to access live feeds from consumers' security cameras and conduct "unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."¹³⁴ This case demonstrates the importance of practicing security-by-design.

¹³² Press Release, FTC, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), *available at* <http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles>.

¹³³ Complaint of FTC, TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (consent), *available at* <http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf>.

¹³⁴ *Id.* at 5.

Of course, the IoT encompasses a wide variety of products and services, and, as noted, the specific security measures that a company needs to implement will depend on a number of factors.¹³⁵ Devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens, or insulin pumps), or connect to other devices or networks in a manner that would enable intruders to access those devices or networks should be more robustly secured than, for example, devices that simply monitor room temperatures, miles run, or calories ingested.

DATA MINIMIZATION

Commission staff agrees with workshop participants who stated that the data minimization principle remains relevant and important to the IoT.¹³⁶ While staff recognizes that companies need flexibility to innovate around new uses of data, staff believes that these interests can and should be balanced with the interests in limiting the privacy and data security risks to consumers.¹³⁷ Accordingly, companies should examine their data practices and business needs

¹³⁵ See, e.g., FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), available at <http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>:

The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

¹³⁶ See, e.g., Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7.

¹³⁷ See, e.g., *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3; Remarks of Chibba, Transcript of Workshop at 329–30.

and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.¹³⁸

Data minimization is a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD Privacy Guidelines, the 2002 Asia-Pacific Economic Cooperation (“APEC”) Privacy Principles, and the 2012 White House Consumer Privacy Bill of Rights.¹³⁹ Some observers have debated how data minimization would apply to new technologies.¹⁴⁰ In the IoT ecosystem, data minimization is challenging, but it remains important.¹⁴¹ Indeed, data minimization can help guard against two privacy-related risks. First, collecting and retaining large amounts of data increases the potential harms associated with a data breach, both with respect to data stored on the device itself as well as in the cloud. Larger data stores present a more attractive target for data thieves, both outside and inside a company –

¹³⁸ Privacy Report, *supra* note 85, at 26–27; *see also* Mobile Disclosures Report, *supra* note 96, at 1 n.2; FTC, Data Brokers: A Call for Transparency and Accountability 55 (2014) (“Data Broker Report”), *available at* <http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

¹³⁹ *See* Privacy Report, *supra* note 85, at 26–27; OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, at ¶ 7 (2013), *available at* <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> (same); Dept. of Homeland Security, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security § 5 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (stating a Data Minimization principle: “DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).”); Exec. Office of the President, National Strategy for Trusted Identities in Cyberspace 45 (Apr. 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (stating a Data Minimization principle: “Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).”).

¹⁴⁰ *See* White House Big Data Report, *supra* note 114, at 54 (Because “the logic of collecting as much data as possible is strong ... focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy.”); PCAST Report at x-xi (“[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).”).

¹⁴¹ *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7. *See also* Article 29 Working Group Opinion, *supra* note 55, at 16–17.

and increases the potential harm from such an event.¹⁴² Thieves cannot steal data that has been deleted after serving its purpose; nor can thieves steal data that was not collected in the first place. Indeed, in several of its data security cases, the Commission has alleged that companies could have mitigated the harm associated with a data breach by disposing of customer information they no longer had a business need to keep.¹⁴³

Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations. For example, in 2010, Commission staff sent a letter to the founders of XY magazine, a magazine for gay youth, regarding their negotiations to sell in bankruptcy customer information dating back to as early as 1996. The staff noted that, because the magazine had ceased to exist for a period of three years, the subscribers were likely to have become adults and moved on, and because continued use of their information would have been contrary to their reasonable expectations, XY should delete the personal information.¹⁴⁴ In this case, the risk associated with continued storage and use of the subscribers' personal information contrary to their reasonable expectations would not have existed if the company had engaged in reasonable data minimization practices.

Although these examples are not IoT-specific, they demonstrate the type of risk created by the expansive collection and retention of data. To minimize these risks, companies should

¹⁴² Remarks of Chibba, Transcript of Workshop at 340; Privacy Report, *supra* note 85, at 27–29.

¹⁴³ See *CardSystems Solutions, Inc.*, No. C-4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch>; *DSW, Inc.*, No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (consent order); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter>. Commissioner Ohlhausen was not a commissioner at the time of these cases and therefore did not participate in them.

¹⁴⁴ Letter from David C. Vladeck, Dir., FTC Bureau of Consumer Prot., to Peter Larson and Martin E. Shmagin (July 1, 2010), available at <http://www.ftc.gov/enforcement/cases-proceedings/closing-letters/letter-xy-magazine-xycom-regarding-use-sale-or>.

examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.¹⁴⁵ Such an exercise is integral to a privacy-by-design approach and helps ensure that the company has given thought to its data collection practices on the front end by asking questions such as what types of data it is collecting, to what end, and how long it should be stored.¹⁴⁶ The process of mindfully considering data collection and retention policies and engaging in a data minimization exercise could also serve an education function for companies, while at the same time, protecting consumer privacy.¹⁴⁷

As an example of how data minimization might work in practice, suppose a wearable device, such as a patch, can assess a consumer's skin condition. The device does not need to collect precise geolocation information in order to work; however, the device manufacturer believes that such information might be useful for a future product feature that would enable users to find treatment options in their area. As part of a data minimization exercise, the company should consider whether it should wait to collect geolocation until after it begins to offer the new product feature, at which time it could disclose the new collection and seek consent. The company should also consider whether it could offer the same feature while collecting less information, such as by collecting zip code rather than precise geolocation. If the company does decide it needs the precise geolocation information, it should provide a prominent disclosure about its collection and use of this information, and obtain consumers' affirmative

¹⁴⁵ *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

¹⁴⁶ *Id.* See also Remarks of Chibba, Transcript of Workshop at 330.

¹⁴⁷ *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

express consent. Finally, it should establish reasonable retention limits for the data it does collect.

To the extent that companies decide they need to collect and maintain data to satisfy a business purpose, they should also consider whether they can do so while maintaining data in de-identified form. This may be a viable option in some contexts and helps minimize the individualized data companies have about consumers, and thus any potential consumer harm, while promoting beneficial societal uses of the information. For example, one university hospital offers a website and an associated smart phone app that collect information from consumers, including geolocation information, to enable users to find and report flu activity in their area.¹⁴⁸ The hospital can maintain and post information in anonymous and aggregate form, which can benefit public health authorities and the public, while at the same time maintaining consumer privacy.

A key to effective de-identification is to ensure that the data cannot be reasonably re-identified. For example, U.S. Department of Health and Human Service regulations¹⁴⁹ require entities covered by HIPAA to either remove certain identifiers, such as date of birth and five-digit zip code, from protected health information¹⁵⁰ or have an expert determine that the risk of re-identification is “very small.”¹⁵¹ As one participant discussed,¹⁵² in 2009, a group of experts attempted to re-identify approximately 15,000 patient records that had been de-identified under

¹⁴⁸ See *Flu Near You*, available at <https://flunearyou.org/>.

¹⁴⁹ 45 C.F.R. §§ 164.514(a)-(c).

¹⁵⁰ 45 C.F.R. § 165.514(b)(2).

¹⁵¹ 45 C.F.R. § 165.514(b)(1).

¹⁵² *Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 8.

the HIPAA standard. They used commercial data sources to re-identify the data and were able to identify only 0.013% of the individuals.¹⁵³ While deidentification can be challenging in several contexts,¹⁵⁴ appropriately de-identified data sets that are kept securely and accompanied by strong accountability mechanisms, can reduce many privacy risks.

Of course, as technology improves, there is always a possibility that purportedly de-identified data could be re-identified.¹⁵⁵ This is why it is also important for companies to have accountability mechanisms in place. When a company states that it maintains de-identified or anonymous data, the Commission has stated that companies should (1) take reasonable steps to de-identify the data, including by keeping up with technological developments; (2) publicly commit not to re-identify the data; and (3) have enforceable contracts in place with any third parties with whom they share the data, requiring the third parties to commit not to re-identify the data.¹⁵⁶ This approach ensures that if the data is not reasonably de-identified and then is re-identified in the future, regulators can hold the company responsible.

With these recommendations on data minimization, Commission staff is mindful of the need to balance future, beneficial uses of data with privacy protection. For this reason, staff's recommendation is a flexible one that gives companies many options: they can decide not to

¹⁵³ *Id.*

¹⁵⁴ Technical experts continue to evaluate the effectiveness of deidentification for different types of data, and some urge caution in interpreting claims about the effectiveness of specific technical means of deidentification. *See, e.g.,* Arvind Narayanan and Edward Felten, No Silver Bullet: De-Identification Still Doesn't Work (July 9, 2014), available at <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>.

¹⁵⁵ *See, e.g.,* Ann Cavoukian and Khaled El Emam, De-identification Protocols: Essential for Protecting Privacy (June 25, 2014), available at http://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identification_essential.pdf; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 8; Privacy Report, *supra* note 85, at 21.

¹⁵⁶ *See* Privacy Report, *supra* note 85, at 21; *see also* *Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 7.

collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options work, it can seek consumers' consent for collecting additional, unexpected data. In addition, in considering reasonable collection and retention limits, it is appropriate to consider the sensitivity of the data at issue: the more sensitive the data, the more harmful it could be if the data fell into the wrong hands or were used for purposes the consumer would not expect. Through this approach, a company can minimize its data collection, consistent with its business goals.¹⁵⁷ As one participant noted, “[p]rotecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and privacy by design.”¹⁵⁸

NOTICE AND CHOICE

While the traditional methods of providing consumers with disclosures and choices may need to be modified as new business models continue to emerge, staff believes that providing notice and choice remains important, as potential privacy and security risks may be heightened due to the pervasiveness of data collection inherent in the IoT. Notice and choice is particularly important when sensitive data is collected.¹⁵⁹

¹⁵⁷ See, e.g., *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 10 (describing its Smart Grid privacy seal).

¹⁵⁸ *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 3. See also Remarks of Chibba, Transcript of Workshop at 330.

¹⁵⁹ See, e.g., *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 6 (“In some cases, however, such as when consumers are purchasing connected devices that will collect personally identifiable health information, the presentation of privacy policies will be important to helping consumers make informed choices.”); *Comment of Ctr. for Digital Democracy*, #484 cmt. #00006 at 3 (“[T]he combined impact of the mobile marketing and real-time data revolution and the Internet of Things places consumer privacy at greater risk than ever before.”).

Moreover, staff believes that providing consumers with the ability to make informed choices remains practicable in the IoT. This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits.¹⁶⁰ This principle applies equally to the Internet of Things.

For example, suppose a consumer buys a smart oven from ABC Vending, which is connected to an ABC Vending app that allows the consumer to remotely turn the oven on to the setting, "Bake at 400 degrees for one hour." If ABC Vending decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context of the consumer's relationship with the manufacturer, and the company should give the consumer a choice. The practice of distinguishing contextually appropriate data practices from those that are inconsistent with

¹⁶⁰ Privacy Report, *supra* note 85, at 38-39; *id.* at 38 ("The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary.").

context reduces the need for companies to provide opportunities for consumer choice before every single data collection.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface, and recognizes that there is no one-size-fits-all approach. Some options – several of which were discussed by workshop participants – include the following:

- **Choices at point of sale:**
One auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in “[p]lain language and multiple choices of levels.”¹⁶¹
- **Tutorials:**
Facebook offers a video tutorial to guide consumers through its privacy settings page. IoT device manufacturers can offer similar vehicles for explaining and providing choices to consumers.
- **Codes on the device:**
Manufacturers could affix a QR code or similar barcode that, when scanned, would take the consumer to a website with information about the applicable data practices and enable consumers to make choices through the website interface.¹⁶²
- **Choices during set-up:**
Many IoT devices have an initial set-up wizard, through which companies could provide clear, prominent, and contextual privacy choices.

¹⁶¹ Remarks of Kenneth Wayne Powell, Toyota Technical Center (“Powell”), Transcript of Workshop at 278.

¹⁶² See Article 29 Working Group Opinion, *supra* note 55, at 18 (proposing that a “device manufacturer could print on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures as well as the purposes of these data collections”).

- **Management portals or dashboards:**¹⁶³
In addition to the availability of initial set-up choices, IoT devices could also include privacy settings menus that consumers can configure and revisit. For example, in the mobile context, both Apple and Google (for Android) have developed dashboard approaches that seem promising – one that is framed by data elements, such as geolocation and contacts (Apple), and one that is framed by individual apps (Android).¹⁶⁴ Similarly, companies developing “command centers” for their connected home devices¹⁶⁵ could incorporate similar privacy dashboards. Properly implemented, such “dashboard” approaches can allow consumers clear ways to determine what information they agree to share.
- **Icons:**
Devices can use icons to quickly convey important settings and attributes, such as when a device is connected to the Internet, with a toggle for turning the connection on or off.
- **“Out of Band” communications requested by consumers:**
When display or user attention is limited, it is possible to communicate important privacy and security settings to the user via other channels. For example, some home appliances allow users to configure their devices so that they receive important information through emails or texts.
- **General Privacy Menus:**
In addition to the types of specific settings and choices described above, devices and their associated platforms could enable consumers to aggregate choices into “packets.”¹⁶⁶ This could involve having more general settings like “low privacy,” “medium,” or “high,” accompanied by a clear and conspicuous explanation of the settings.
- **A User Experience Approach:**
One participant noted that companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize choices.¹⁶⁷ For example, a manufacturer that offers two or more devices could use the consumer’s preferences on one device (e.g., “do not transmit any of my information to third parties”) to set a default preference on another. As another example, a single device, such as a home appliance “hub” that stores data locally – say on the consumer’s home network – could learn a consumer’s preferences based on prior behavior and predict future privacy preferences as new appliances are added to the hub.

¹⁶³ *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

¹⁶⁴ *See Mobile Disclosures Report*, *supra* note 96, at 16-17.

¹⁶⁵ Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 4, 2015), *available at* <http://www.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511>.

¹⁶⁶ Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology (“Hall”), Transcript of Workshop at 216.

¹⁶⁷ Remarks of Nguyen, Transcript of Workshop at 48.

Of course, whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents.¹⁶⁸ In addition, companies may want to consider using a combination of approaches.

Staff also recognizes concerns discussed at the workshop¹⁶⁹ and, as noted above, in the White House Big Data Report and PCAST Report that, applied aggressively, a notice and choice approach could restrict unexpected new uses of data with potential societal benefits. For this reason, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. Companies should not collect sensitive data without affirmative express consent.

In addition, if a company enables the collection of consumers' data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. As noted above, robust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way.¹⁷⁰ Companies can use such de-identified data without having to offer consumers choices.

¹⁶⁸ This discussion refers to how companies should communicate choices to consumers. Lengthy privacy policies are not the most effective consumer communication tool. However, providing disclosures and choices through these privacy policies serves an important accountability function, so that regulators, advocacy groups, and some consumers can understand and compare company practices and educate the public. *See* Privacy Report, *supra* note 85, at 61-64.

¹⁶⁹ *See, e.g., Comment of Future of Privacy Forum*, #510 cmt. #00013, App. A at 9; *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 6-9.

¹⁷⁰ *See, e.g., Comment of CTIA – The Wireless Ass'n*, #484 cmt. #00009 at 10-11; *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 5.

Staff also notes that existing laws containing elements of the use-based approach apply to the IoT. The FCRA sets forth a number of statutory protections applicable to “consumer report” information, including restrictions on the uses for which this information can be shared.¹⁷¹ Even when there is a permissible use for such information, the FCRA imposes an array of protections, including those relating to notice, access, disputes, and accuracy.¹⁷² In addition, the FTC has used its “unfairness” authority to challenge a number of harmful uses of consumer data. For example, in the agency’s recent case against Leap Lab, the Commission alleged that defendants sold consumer payday loan applications that included consumers’ Social Security and financial account numbers to non-lenders that had no legitimate need for this sensitive personal information.¹⁷³

Staff has concerns, however, about adopting solely a use-based model for the Internet of Things. First, because use-based limitations have not been fully articulated in legislation or other widely-accepted multistakeholder codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful.¹⁷⁴ If a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust. For example, there was considerable consumer outcry over Facebook’s launch of the Beacon service,

¹⁷¹ FCRA, 15 U.S.C. § 1681–1681v. Section 604 of the FCRA sets forth the permissible purposes for which a consumer reporting company may furnish consumer report information, such as to extend credit or insurance or for employment purposes. 15 U.S.C. 1681b.

¹⁷² FCRA, 15 U.S.C. § 1681–1681v.

¹⁷³ Press Release, FTC, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers’ Accounts (Dec. 23, 2014), *available at* <http://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars>.

¹⁷⁴ ANN CAVOUKIAN ET AL., INFO. & PRIVACY COMM’R, ONT., CAN., THE UNINTENDED CONSEQUENCES OF PRIVACY PATERNALISM (2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/03/pbd-privacy_paternalism.pdf.

as well as Google's launch of the Buzz social network, which ultimately led to an FTC enforcement action.¹⁷⁵

Second, use limitations alone do not address the privacy and security risks created by expansive data collection and retention. As explained above, keeping vast amounts of data can increase a company's attractiveness as a data breach target, as well as the risk of harm associated with any such data breach. For this reason, staff believes that companies should seek to reasonably limit the data they collect and dispose of it when it is no longer needed.

Finally, a use-based model would not take into account concerns about the practice of collecting sensitive information.¹⁷⁶ Consumers would likely want to know, for example, if a company is collecting health information or making inferences about their health conditions, even if the company ultimately does not use the information.¹⁷⁷

¹⁷⁵ See, e.g., Google Inc., No. C-4336 (Oct. 13, 2011) (consent order), available at <http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf>.

¹⁷⁶ In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

¹⁷⁷ Of course, if a company misstates how it uses data, this could be a deceptive practice under Section 5 of the FTC Act. The FTC has brought cases against companies that promise to use consumers' data one way, but used it in another way. See, e.g., Google Inc., *supra* note 175. The FTC can also use its unfairness authority to prohibit uses of data that cause or are likely to cause substantial injury to a consumer, where that injury was not reasonably avoidable by the consumer, and where the injury was not outweighed by a benefit to consumers or competition. See, e.g., Designerware, LLC, No. C-4390 (Apr. 11, 2013) (consent order) (alleging that installing and turning on webcams on people's home computers without their knowledge or consent was an unfair practice), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter>.

The establishment of legislative or widely-accepted multistakeholder use-based frameworks could potentially address some of these concerns and should be considered. For example, the framework could set forth permitted or prohibited uses. In the absence of such legislative or widely accepted multistakeholder frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

Legislation

Summary of Workshop Discussions

Workshop participants discussed whether legislation is needed to ensure appropriate protections for data collected through connected devices. Some participants expressed trepidation that the benefits of the IoT might be adversely affected should policymakers enact laws or regulations on industry.¹⁷⁸ One participant stated, “[t]he FTC should be very cautious about proposing regulation of this sector, given its importance to innovation in America.”¹⁷⁹ Another participant noted that “we should be careful to kind of strike a balance between guiding companies in the right direction and enforcing.”¹⁸⁰ Still another worried that the workshop might “represent[] the beginning of a regulatory regime for a new set of information technologies that are still in their infancy” and advised policymakers to “exercise restraint and avoid the impulse to regulate before serious harms are demonstrated.”¹⁸¹ Another participant questioned what legislation would look like, given the difficulty of defining the contours of privacy rights.¹⁸²

A number of participants noted that self-regulation is the appropriate approach to take to the IoT. One participant stated, “self-regulation and best business practices – that are technology

¹⁷⁸ See, e.g., *Comment of Direct Mktg. Ass’n*, #484 cmt. #00010.

¹⁷⁹ *Comment of Internet Commerce Coal.*, #484 cmt. #00020 at 2.

¹⁸⁰ Remarks of Rogers, Transcript of Workshop at 359.

¹⁸¹ *Comment of Tech. Policy Program of the Mercatus Ctr., George Mason Univ.*, #484 cmt. #00024 at 1 and 9.

¹⁸² Remarks of Cerf, Transcript of Workshop at 149-50 (“Well, I have to tell you that regulation is tricky. And I don’t know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don’t think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we understand the nature of the problems and maybe even the nature of the solutions.”).

neutral – along with consumer education serve as the preferred framework for protecting consumer privacy and security while enhancing innovation, investment, competition, and the free flow of information essential to the Internet of Things.”¹⁸³ Another participant agreed, stating “[s]elf-regulatory regimes have worked well to ensure consumer privacy and foster innovation, and industry has a strong track record of developing and implementing best practices to protect information security.”¹⁸⁴

Other participants noted that the time is ripe for legislation, either specific to the IoT or more generally.¹⁸⁵ One participant who called for legislation noted that the “explosion of fitness and health monitoring devices is no doubt highly beneficial to public health and worth encouraging,” but went on to state:

At the same time, data from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential public health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decisionmaking.¹⁸⁶

Recommendations

The Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is

¹⁸³ *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

¹⁸⁴ *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 18.

¹⁸⁵ Remarks of Hall, Transcript of Workshop at 180-81 (supporting baseline privacy legislation); *see also* Remarks of Jacobs, Transcript of Workshop at 360 (emphasizing importance of enforcement “in the meantime”).

¹⁸⁶ Peppet, *Regulating the Internet of Things*, *supra* note 62, at 151.

great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs¹⁸⁷ designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, while IoT specific-legislation is not needed, the workshop provided further evidence that Congress should enact general data security legislation. As noted above, there was wide agreement among workshop participants about the importance of securing Internet-enabled devices, with some participants stating that many devices now available in the market are not reasonably secure, posing risks to the information that they collect and transmit and also to information on consumers' networks or even to others on the Internet.¹⁸⁸ These problems highlight the need for substantive data security and breach notification legislation at the federal level.

The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach. Reasonable and appropriate security practices are critical to addressing the problem of data breaches and protecting consumers from identity theft and other harms. Notifying consumers of breaches after they occur helps consumers protect themselves from any harm that is likely to be caused by the misuse of their data. These principles apply equally to the IoT ecosystem.¹⁸⁹

¹⁸⁷ Remarks of Lightner, Transcript of Workshop at 56-57 (discussing voluntary code of conduct for energy data); *Comment of Future of Privacy Forum*, #484 cmt. #00013 (discussing self-regulatory efforts in a variety of contexts).

¹⁸⁸ See discussion *supra* pp. 10-14 and accompanying notes.

¹⁸⁹ One commenter argued that breach notification laws should be even broader in the IoT context. See Remarks of Peppet, Transcript of Workshop at 220 (urging that breach notification laws be extended for the IoT to cover additional types of information that would lead to consumer harm but would not meet the definition of personal

We emphasize that general technology-neutral data security legislation should protect against unauthorized access to both personal information and device functionality itself. The security risks associated with IoT devices, which are often not limited to the compromise of personal information but also implicate broader health and safety concerns, illustrate the importance of these protections. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.¹⁹⁰ Similarly, a criminal who hacks into a car's network could cause a car crash. Accordingly, general data security legislation should address risks to both personal information and device functionality.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards.¹⁹¹ Commission staff thus again recommends that Congress consider enacting broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as when to provide privacy notices to consumers and offer them choices about data collection and use practices. Although the Commission currently has authority to take action against some IoT-related practices, it cannot

information protected under existing laws). The Commission has not taken a position on such an approach at this time.

¹⁹⁰ Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheney-s-heart/>.

¹⁹¹ Commissioner Ohlhausen disagrees with this portion of the staff's recommendation. She believes that the FTC's current Section 5 authority to prohibit unfair and deceptive acts or practices already requires notice and choice for collecting sensitive personally identifiable information and protects against uses of consumer information that cause or are likely to cause substantial consumer harm not outweighed by benefits to consumers or competition. Furthermore, the FCRA, HIPAA, and other laws already provide additional sector-specific privacy protections. Thus, Commissioner Ohlhausen questions what harms baseline privacy legislation would reach that the FTC's existing authority cannot.

mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness.

The Commission has issued a report and testified before Congress calling for baseline federal privacy legislation.¹⁹² These recommendations have been based on concerns about the lack of transparency regarding some companies’ data practices and the lack of meaningful consumer control of personal data. These concerns permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue.

Staff believes such legislation will help build trust in new technologies that rely on consumer data, such as the IoT. Consumers are more likely to buy connected devices if they feel that their information is adequately protected.¹⁹³ A 2012 survey shows, for example, that a majority of consumers uninstalled an app because they were concerned that it was collecting too much personal information, or declined to install an app at all.¹⁹⁴ A 2014 survey shows that 87% of consumers are concerned about the type of data collected through smart devices, and 88% of

¹⁹² See, e.g., Privacy Report, *supra* note 85, at 12-13; *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. On Commerce, Science & Transportation* (May 9, 2012) (statement of FTC), available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf.

¹⁹³ Remarks of Chibba, Transcript of Workshop at 312-13; see also Remarks of Wolf, Transcript of Workshop at 260 (noting that “the Michigan Department of Transportation and the Center for Automotive Research identified security as the primary concern for connected car technologies”); *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5 (“If there are lax controls and insufficient oversight over the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. Even with proper controls and oversight, helping consumers understand the benefits from these innovations and the protections in place is important lest they feel that personal control has been sacrificed for corporate gain.”).

¹⁹⁴ JAN LAUREN BOYLES ET AL., PEW INTERNET PROJECT, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012), available at http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.

consumers want to control the data that is collected through smart devices.¹⁹⁵ Surveys also show that consumers are more likely to trust companies that provide them with transparency and choices.¹⁹⁶ General privacy legislation that provides for greater transparency and choices could help both consumers and businesses by promoting trust in the burgeoning IoT marketplace.

In addition, as demonstrated at the workshop, general privacy legislation could ensure that consumers' data is protected, regardless of who is asking for it. For example, workshop participants discussed the fact that HIPAA protects sensitive health information, such as medical diagnoses, names of medications, and health conditions, but only if it is collected by certain entities, such as a doctor's office or insurance company.¹⁹⁷ Increasingly, however, health apps are collecting this same information through consumer-facing products, to which HIPAA protections do not apply. Commission staff believes that consumers should have transparency and choices over their sensitive health information, regardless of who collects it. Consistent standards would also level the playing field for businesses.

¹⁹⁵ The TRUSTe Internet of Things Privacy Index, 2014 U.S. Edition, available at <http://www.truste.com/us-internet-of-things-index-2014/>.

¹⁹⁶ See, e.g., Adam DeMartino, Evidon, *RESEARCH: Consumers Feel Better About Brands that Give Them Transparency and Control Over Ads* (Nov. 10, 2010), available at <http://www.evidon.com/blog/research-consumers-feel-better-about-brands-that-give-them-transparency-and-control-over-ads>; Scott Meyer, *Data Transparency Builds Trust*, BRANDREPUBLIC (Oct. 31, 2012), available at <http://www.brandrepublic.com/news/1157134/>; TRUSTe, *New TRUSTe Survey Finds Consumer Education and Transparency Vital for Sustainable Growth and Success of Online Behavioral Advertising* (July 25, 2011), available at http://www.truste.com/about-TRUSTe/press-room/news_truste_behavioral_advertising_survey_2011.

¹⁹⁷ Remarks of Hall, Transcript of Workshop at 179; Remarks of T. Drew Hickerson, Happtique, Transcript of Workshop at 350; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 12.

While Commission staff encourages Congress to consider privacy and security legislation, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices and services. Specifically, we will engage in the following initiatives:

- **Law enforcement:**

The Commission enforces the FTC Act, the FCRA, the Children’s Online Privacy Protection Act, the health breach notification provisions of the HI-TECH Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws. The TRENDNet case, discussed above, was the Commission’s first IoT case. We will continue to look for cases involving companies making IoT devices that, among other things, do not maintain reasonable security, make misrepresentations about their privacy practices, or violate the requirements of the FCRA when they use information for credit, employment, insurance, or other eligibility decisions. Staff believes that a strong FTC law enforcement presence will help incentivize appropriate privacy and security-protective practices by companies manufacturing and selling connected devices.

- **Consumer and business education:**

Consumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings. Businesses, and in particular small businesses, would benefit from additional information about how to reasonably secure IoT devices. The Commission staff will develop new consumer and business education materials in this area.

- **Participation in multi-stakeholder groups:**

Currently, Commission staff is working with a variety of groups that are considering guidelines related to the Internet of Things. For example, staff participates in NTIA’s multi-stakeholder group that is considering guidelines for facial recognition and the Department of Energy’s multi-stakeholder effort to develop guidelines for smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers. Commission staff will continue to participate in multistakeholder groups to develop guidelines related to the IoT.

- **Advocacy:**

Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area. Among other things, staff will share the best practices discussed in this report with other government entities in order to ensure that they consider privacy and security issues.

Conclusion

The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car, and with wearables and ingestibles, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.



Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR
BUSINESSES AND POLICYMAKERS

FTC REPORT



Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR
BUSINESSES AND POLICYMAKERS

FTC REPORT
MARCH 2012

CONTENTS

Executive Summary	i
Final FTC Privacy Framework and Implementation Recommendations	vii
I. Introduction	1
II. Background	2
A. FTC Roundtables and Preliminary Staff Report	2
B. Department of Commerce Privacy Initiatives	3
C. Legislative Proposals and Efforts by Stakeholders	4
1. Do Not Track	4
2. Other Privacy Initiatives	5
III. Main Themes From Commenters	7
A. Articulation of Privacy Harms	7
B. Global Interoperability	9
C. Legislation to Augment Self-Regulatory Efforts	11
IV. Privacy Framework	15
A. Scope	15
1. Companies Should Comply with the Framework Unless They Handle Only Limited Amounts of Non-Sensitive Data that is Not Shared with Third Parties.	15
2. The Framework Sets Forth Best Practices and Can Work in Tandem with Existing Privacy and Security Statutes	16
3. The Framework Applies to Offline As Well As Online Data.	17
4. The Framework Applies to Data That is Reasonably Linkable to a Specific Consumer, Computer, or Device.	18
B. Privacy by Design	22
1. The Substantive Principles: Data Security, Reasonable Collection Limits, Sound Retention Practices, and Data Accuracy	23
2. Companies Should Adopt Procedural Protections to Implement the Substantive Principles..	30
C. Simplified Consumer Choice	35
1. Practices That Do Not Require Choice	36
2. For Practices Inconsistent with the Context of their Interaction with Consumers, Companies Should Give Consumers Choices.	48
D. Transparency	60
1. Privacy Notices	61
2. Access	64
3. Consumer Education	71
V. Conclusion	72
FTC Privacy Milestones	
Personal Data Ecosystem	
Dissenting Statement of Commissioner J. Thomas Rosch	

EXECUTIVE SUMMARY

In today's world of smart phones, smart grids, and smart cars, companies are collecting, storing, and sharing more information about consumers than ever before. Although companies use this information to innovate and deliver better products and services to consumers, they should not do so at the expense of consumer privacy.

With this Report, the Commission calls on companies to act now to implement best practices to protect consumers' private information. These best practices include making privacy the "default setting" for commercial data practices and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency. Implementing these best practices will enhance trust and stimulate commerce.

This Report follows a preliminary staff report that the Federal Trade Commission ("FTC" or "Commission") issued in December 2010. The preliminary report proposed a framework for protecting consumer privacy in the 21st Century. Like this Report, the framework urged companies to adopt the following practices, consistent with the Fair Information Practice Principles first articulated almost 40 years ago:

- ◆ **Privacy by Design:** Build in privacy at every stage of product development;
- ◆ **Simplified Choice for Businesses and Consumers:** Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism, while reducing the burden on businesses of providing unnecessary choices; and
- ◆ **Greater Transparency:** Make information collection and use practices transparent.

The Commission received more than 450 public comments in response to the preliminary report from various stakeholders, including businesses, privacy advocates, technologists and individual consumers. A wide range of stakeholders, including industry, supported the principles underlying the framework, and many companies said they were already following them. At the same time, many commenters criticized the slow pace of self-regulation, and argued that it is time for Congress to enact baseline privacy legislation. In this Report, the Commission addresses the comments and sets forth a revised, final privacy framework that adheres to, but also clarifies and fine-tunes, the basic principles laid out in the preliminary report.

Since the Commission issued the preliminary staff report, Congress has introduced both general privacy bills and more focused bills, including ones addressing Do Not Track and the privacy of teens. Industry has made some progress in certain areas, most notably, in responding to the preliminary report's call for Do Not Track. In other areas, however, industry progress has been far slower. Thus, overall, consumers do not yet enjoy the privacy protections proposed in the preliminary staff report.

The Administration and certain Members of Congress have called for enactment of baseline privacy legislation. The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

The remainder of this Executive Summary describes key developments since the issuance of the preliminary report, discusses the most significant revisions to the proposed framework, and lays out several next steps.

DEVELOPMENTS SINCE ISSUANCE OF THE PRELIMINARY REPORT

In the last 40 years, the Commission has taken numerous actions to shape the consumer privacy landscape. For example, the Commission has sued dozens of companies that broke their privacy and security promises, scores of telemarketers that called consumers on the Do Not Call registry, and more than a hundred scammers peddling unwanted spam and spyware. Since it issued the initial staff report, the Commission has redoubled its efforts to protect consumer privacy, including through law enforcement, policy advocacy, and consumer and business education. It has also vigorously promoted self-regulatory efforts.

On the law enforcement front, since December 2010, the Commission:

- ◆ Brought enforcement actions against Google and Facebook. The orders obtained in these cases require the companies to obtain consumers' affirmative express consent before materially changing certain of their data practices and to adopt strong, company-wide privacy programs that outside auditors will assess for 20 years. These orders will protect the more than one billion Google and Facebook users worldwide.
- ◆ Brought enforcement actions against online advertising networks that failed to honor opt outs. The orders in these cases are designed to ensure that when consumers choose to opt out of tracking by advertisers, their choice is effective.
- ◆ Brought enforcement actions against mobile applications that violated the Children's Online Privacy Protection Act as well as applications that set default privacy settings in a way that caused consumers to unwittingly share their personal data.
- ◆ Brought enforcement actions against entities that sold consumer lists to marketers in violation of the Fair Credit Reporting Act.
- ◆ Brought actions against companies for failure to maintain reasonable data security.

On the policy front, since December 2010, the FTC and staff:

- ◆ Hosted two privacy-related workshops, one on child identity theft and one on the privacy implications of facial recognition technology.
- ◆ Testified before Congress ten times on privacy and data security issues.
- ◆ Consulted with other federal agencies, including the Federal Communications Commission, the Department of Health and Human Services, and the Department of Commerce, on their privacy initiatives. The Commission has supported the Department of Commerce's initiative to convene stakeholders to develop privacy-related codes of conduct for different industry sectors.
- ◆ Released a survey of data collection disclosures by mobile applications directed to children.
- ◆ Proposed amendments to the Children's Online Privacy Protection Act Rule.

On the education front, since December 2010, the Commission:

- ◆ Continued outreach efforts through the FTC's consumer online safety portal, OnGuardOnline.gov, which provides information in a variety of formats – articles, games, quizzes, and videos – to help consumers secure their computers and protect their personal information. It attracts approximately 100,000 unique visitors per month.
- ◆ Published new consumer education materials on identity theft, Wi-Fi hot spots, cookies, and mobile devices.
- ◆ Sent warning letters to marketers of mobile apps that do background checks on individuals, educating them about the requirements of the Fair Credit Reporting Act.

To promote self-regulation, since December 2010, the Commission:

- ◆ Continued its call for improved privacy disclosures and choices, particularly in the area of online behavioral tracking. In response to this call, as well as to Congressional interest:
 - ◆ A number of Internet browser vendors developed browser-based tools for consumers to request that websites not track their online activities.
 - ◆ The World Wide Web Consortium, an Internet standard setting organization, is developing a universal web protocol for Do Not Track.
 - ◆ The Digital Advertising Alliance (“DAA”), a coalition of media and marketing organizations, has developed a mechanism, accessed through an icon that consumers can click, to obtain information about and opt out of online behavioral advertising. Additionally, the DAA has committed to preventing the use of consumers’ data for secondary purposes like credit and employment and honoring the choices about tracking that consumers make through the settings on their browsers.
- ◆ Participated in the development of enforceable cross-border privacy rules for businesses to harmonize and enhance privacy protection of consumer data that moves between member countries of the forum on Asia Pacific Economic Cooperation.

THE FINAL REPORT

Based upon its analysis of the comments filed on the proposed privacy framework, as well as commercial and technological developments, the Commission is issuing this final Report. The final framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC. While retaining the proposed framework's fundamental best practices of privacy by design, simplified choice, and greater transparency, the Commission makes revised recommendations in three key areas in response to the comments.

First, the Commission makes changes to the framework's scope. The preliminary report proposed that the privacy framework apply to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. To address concerns about undue burdens on small businesses, the final framework does not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties. Commenters also expressed concern that, with improvements in technology and the ubiquity of public information, more and more data could be "reasonably linked" to a consumer, computer or device, and that the proposed framework provided less incentive for a business to try to de-identify the data it maintains. To address this issue, the Report clarifies that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.

Second, the Commission revises its approach to how companies should provide consumers with privacy choices. To simplify choice for both consumers and businesses, the proposed framework set forth a list of five categories of "commonly accepted" information collection and use practices for which companies need not provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing). Several business commenters expressed concern that setting these "commonly accepted practices" in stone would stifle innovation. Other commenters expressed the concern that the "commonly accepted practices" delineated in the proposed framework were too broad and would allow a variety of practices to take place without consumer consent.

In response to these concerns, the Commission sets forth a modified approach that focuses on the context of the consumer's interaction with the business. Under this approach, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law. Although many of the five "commonly accepted practices" identified in the preliminary report would generally meet this standard, there may be exceptions. The Report provides examples of how this new "context of the interaction" standard would apply in various circumstances.

Third, the Commission recommends that Congress consider enacting targeted legislation to provide greater transparency for, and control over, the practices of information brokers. The proposed framework recommended that companies provide consumers with reasonable access to the data the companies maintain about them, proportionate to the sensitivity of the data and the nature of its use. Several commenters discussed in particular the importance of consumers' ability to access information that information brokers have about them. These commenters noted the lack of transparency about the practices of information brokers, who often buy, compile, and sell a wealth of highly personal information about consumers but never interact directly with them. Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.

The Commission agrees that consumers should have more control over the practices of information brokers and believes that appropriate legislation could help address this goal. Any such legislation could be

modeled on a bill that the House passed on a bipartisan basis during the 111th Congress, which included a procedure for consumers to access and dispute personal data held by information brokers.

IMPLEMENTATION OF THE PRIVACY FRAMEWORK

While Congress considers privacy legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission's final privacy framework. Although some companies have excellent privacy and data security practices, industry as a whole must do better. Over the course of the next year, Commission staff will promote the framework's implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- ◆ **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the Digital Advertising Alliance ("DAA") has developed its own icon-based tool and has committed to honor the browser tools; and the World Wide Web Consortium ("W3C") has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- ◆ **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.
- ◆ **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- ◆ **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media seek, to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

- ◆ **Promoting Enforceable Self-Regulatory Codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

FINAL FTC PRIVACY FRAMEWORK AND IMPLEMENTATION RECOMMENDATIONS

The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

SCOPE

Final Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.

PRIVACY BY DESIGN

Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

A. The Substantive Principles

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

B. Procedural Protections to Implement the Substantive Principles

Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

A. Practices That Do Not Require Choice

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.

To balance the desire for flexibility with the need to limit the types of practices for which choice is not required, the Commission has refined the final framework so that companies engaged in practices consistent with the context of their interaction with consumers need not provide choices for those practices.

B. Companies Should Provide Consumer Choice for Other Practices

Final Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

The Commission commends industry's efforts to improve consumer control over online behavioral tracking by developing a Do Not Track mechanism, and encourages continued improvements and full implementation of those mechanisms.

TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

A. Privacy notices

Final Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

B. Access

Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

The Commission has amplified its support for this principle by including specific recommendations governing the practices of information brokers.

C. Consumer Education

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

LEGISLATIVE RECOMMENDATIONS

The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security and data broker legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

FTC WILL ASSIST WITH IMPLEMENTATION IN FIVE KEY AREAS

As discussed throughout the Commission's final Report, there are a number of specific areas where policy makers have a role in assisting with the implementation of the self-regulatory principles that make up the final privacy framework. Areas where the FTC will be active over the course of the next year include the following:

1. Do Not Track

Industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.

2. Mobile

The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

3. Data Brokers

To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

4. Large Platform Providers

To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

5. Promoting Enforceable Self-Regulatory Codes

The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

In all other areas, the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the final privacy framework, to the extent they have not already done so. For its part, the FTC will focus its policy efforts on the five areas identified above, vigorously enforce existing laws, work with industry on self-regulation, and continue to target its education efforts on building awareness of existing data collection and use practices and the tools to control them.

I. INTRODUCTION

In December 2010, the Federal Trade Commission (“FTC” or “Commission”) issued a preliminary staff report to address the privacy issues associated with new technologies and business models.¹ The report outlined the FTC’s 40-year history of promoting consumer privacy through policy and enforcement work, discussed the themes and areas of consensus that emerged from the Commission’s “Exploring Privacy” roundtables, and set forth a proposed framework to guide policymakers and other stakeholders regarding best practices for consumer privacy. The proposed framework called on companies to build privacy protections into their business operations (*i.e.*, adopt “privacy by design”²), offer simplified choice mechanisms that give consumers more meaningful control, and increase the transparency of their data practices.

The preliminary report included a number of questions for public comment to assist and guide the Commission in developing a final privacy framework. The Commission received more than 450 comments from a wide variety of interested parties, including consumer and privacy advocates, individual companies and trade associations, academics, technologists, and domestic and foreign government agencies. Significantly, more than half of the comments came from individual consumers. The comments have helped the Commission refine the framework to better protect consumer privacy in today’s dynamic and rapidly changing marketplace.

In this Final Report, the Commission adopts staff’s preliminary framework with certain clarifications and revisions. The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

The Report highlights the developments since the FTC issued staff’s preliminary report, including the Department of Commerce’s parallel privacy initiative, proposed legislation, and actions by industry and other stakeholders. Next, it analyzes and responds to the main issues raised by the public comments. Based on those comments, as well as marketplace developments, the Report sets forth a revised privacy framework and legislative recommendations. Finally, the Report outlines a series of policy initiatives that FTC staff will undertake in the next year to assist industry with implementing the final framework as best practices.

1 FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report* (Dec. 2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

2 Privacy by Design is an approach that Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada, has advocated. See Information and Privacy Commissioner, Ontario, Canada, Privacy by Design, <http://privacybydesign.ca/>.

II. BACKGROUND

A. FTC ROUNDTABLES AND PRELIMINARY STAFF REPORT

Between December 2009 and March 2010, the FTC convened its “Exploring Privacy” roundtables.³ The roundtables brought together stakeholders representing diverse interests to evaluate whether the FTC’s existing approach to protecting consumer privacy was adequate in light of 21st Century technologies and business models. From these discussions, as well as submitted materials, a number of themes emerged. First, the collection and commercial use of consumer data in today’s society is ubiquitous and often invisible to consumers. Second, consumers generally lack full understanding of the nature and extent of this data collection and use and, therefore, are unable to make informed choices about it. Third, despite this lack of understanding, many consumers are concerned about the privacy of their personal information. Fourth, the collection and use of consumer data has led to significant benefits in the form of new products and services. Finally, the traditional distinction between personally identifiable information and “anonymous” data has blurred.

Participants also pointed to shortcomings in existing frameworks that have attempted to address privacy concerns. The “notice-and-choice model,” which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand.⁴ The “harm-based model,” which focused on protecting consumers from specific harms – physical security, economic injury, and unwarranted intrusions into their daily lives – had been criticized for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored.⁵ Participants noted that both of these privacy frameworks have struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers’ information in ways that often are invisible to consumers.⁶

Building on the record developed at the roundtables and on its own enforcement and policymaking expertise, FTC staff proposed for public comment a framework for approaching privacy. The proposed framework included three major components. It called on companies to treat privacy as their “default setting” by implementing “privacy by design” throughout their regular business operations. The concept of privacy by design includes limitations on data collection and retention, as well as reasonable security and data accuracy. By considering and addressing privacy at every stage of product and service development,

3 The first roundtable took place on December 7, 2009, the second roundtable on January 28, 2010, and the third roundtable on March 17, 2010. See FTC, *Exploring Privacy – A Roundtable Series*, <http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml>.

4 See, e.g., *1st Roundtable, Remarks of Fred Cate, Indiana University Maurer School of Law*, at 280-81; *1st Roundtable, Remarks of Lorrie Cranor, Carnegie Mellon University*, at 129; see also *Written Comment of Fred Cate, 2nd Roundtable, Consumer Protection in the Age of the ‘Information Economy,’* cmt. #544506-00057, at 343-79.

5 See, e.g., *1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center*, at 301; *1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 36-38; *1st Roundtable, Remarks of Susan Grant, Consumer Federation of America*, at 38-39.

6 See, e.g., *3rd Roundtable, Remarks of Kathryn Montgomery, American University School of Communication*, at 200-01; *2nd Roundtable, Remarks of Kevin Bankston, Electronic Frontier Foundation*, at 277.

companies can shift the burden away from consumers who would otherwise have to seek out privacy-protective practices and technologies. The proposed framework also called on companies to simplify consumer choice by presenting important choices – in a streamlined way – to consumers at the time they are making decisions about their data. As part of the call for simplified choice, staff asked industry to develop a mechanism that would allow consumers to more easily control the tracking of their online activities, often referred to as “Do Not Track.” Finally, the framework focused on improving consumer understanding of commercial data practices (“transparency”) and called on companies – both those that interact directly with consumers and those that lack a consumer interface – to improve the transparency of their practices. As discussed below, the Commission received a large number of thoughtful and informative comments regarding each of the framework’s elements. These comments have allowed the Commission to refine the framework and to provide further guidance regarding its implementation.

B. DEPARTMENT OF COMMERCE PRIVACY INITIATIVES

In a related effort to examine privacy, in May 2010, the Department of Commerce (“DOC” or “Commerce”) convened a public workshop to discuss how to balance innovation, commerce, and consumer privacy in the online context.⁷ Based on the input received from the workshop, as well as related research, on December 16, 2010, the DOC published for comment a strategy paper outlining privacy recommendations and proposed initiatives.⁸ Following the public comment period, on February 23, 2012, the Administration issued its final “White Paper” on consumer privacy. The White Paper recommends that Congress enact legislation to implement a Consumer Privacy Bill of Rights based on the Fair Information Practice Principles (“FIPPs”).⁹ In addition, the White Paper calls for a multistakeholder process to determine how to apply the Consumer Privacy Bill of Rights in different business contexts. Commerce issued a Notice of Inquiry on March 5, 2012, asking for public input on both the process for convening stakeholders on this project, as well as the proposed subject areas to be discussed.¹⁰

Staff from the FTC and Commerce worked closely to ensure that the agencies’ privacy initiatives are complementary. Personnel from each agency actively participated in both the DOC and FTC initiatives, and have also communicated regularly on how best to develop a meaningful, effective, and consistent approach to privacy protection. Going forward, the agencies will continue to work collaboratively to guide implementation of these complementary privacy initiatives.

7 See Press Release, Department of Commerce, Commerce Secretary Gary Locke Discusses Privacy and Innovation with Leading Internet Stakeholders (May 7, 2010), *available at* <http://www.commerce.gov/news/press-releases/2010/05/07/commerce-secretary-gary-locke-discusses-privacy-and-innovation-leadin>.

8 See Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

9 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>. The FIPPs as articulated in the Administration paper are: Transparency, Individual Control, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability.

10 See National Telecommunications and Information Administration, Request for Public Comment, Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13098 (Mar. 5, 2012).

C. LEGISLATIVE PROPOSALS AND EFFORTS BY STAKEHOLDERS

Since Commission staff released its preliminary report in December 2010, there have been a number of significant legislative proposals, as well as steps by industry and other stakeholders, to promote consumer privacy.

1. DO NOT TRACK

The preliminary staff report called on industry to create and implement a mechanism to allow consumers to control the collection and use of their online browsing data, often referred to as “Do Not Track.” Bills introduced in the House and the Senate specifically address the creation of Do Not Track mechanisms, and, if enacted, would mandate that the Commission promulgate regulations to establish standards for a Do Not Track regime.¹¹

In addition to the legislative proposals calling for the creation of Do Not Track, staff’s preliminary report recommendation triggered significant progress by various industry sectors to develop tools to allow consumers to control online tracking. A number of browser vendors – including Mozilla, Microsoft, and Apple – announced that the latest versions of their browsers permit consumers to instruct websites not to track their activities across websites.¹² Mozilla has also introduced a mobile browser for Android devices that enables Do Not Track.¹³ The online advertising industry has also established an important program. The Digital Advertising Alliance (“DAA”), an industry coalition of media and marketing associations, has developed an initiative that includes an icon embedded in behaviorally targeted online ads.¹⁴ When consumers click on the icon, they can see information about how the ad was targeted and delivered to them and they are given the opportunity to opt out of such targeted advertising. The program’s recent growth and implementation has been significant. In addition, the DAA has committed to preventing the use of consumers’ data for secondary purposes like credit and employment decisions. The DAA has also agreed to honor the choices about tracking that consumers make through settings on their web browsers. This will provide consumers two ways to opt out: through the DAA’s icon in advertisements or through their browser settings. These steps demonstrate the online advertising industry’s support for privacy and consumer choice.

11 See Do-Not-Track Online Act of 2011, S. 913, 112th Congress (2011); Do Not Track Me Online Act, H.R. 654, 112th Congress (2011).

12 See Press Release, Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9 (Dec. 7, 2010), *available at* <http://www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.aspx>; Mozilla Firefox 4 Beta, Now Including “Do Not Track” Capabilities, MOZILLA BLOG (Feb. 8, 2011), <http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/>; Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, WALL ST. J., Apr. 13, 2011, *available at* <http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html>. Google recently announced that it will also offer this capability in the next version of its browser. Gregg Kaizer, *FAQ: What Google’s Do Not Track Move Means*, COMPUTERWORLD (Feb. 24, 2012), *available at* http://www.computerworld.com/s/article/9224583/FAQ_What_Google_s_Do_Not_Track_move_means.

13 See Mozilla, Do Not Track FAQs, <http://dnt.mozilla.org>.

14 See Press Release, Interactive Advertising Bureau, Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control Over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410.

Finally, the World Wide Web Consortium (“W3C”)¹⁵ convened a working group to create a universal standard for Do Not Track. The working group includes DAA member companies, other U.S. and international companies, industry groups, and consumer groups. The W3C group has made substantial progress toward a standard that is workable in the desktop and mobile settings, and has published two working drafts of its standard documents. The group’s goal is to complete a consensus standard in the coming months.

2. OTHER PRIVACY INITIATIVES

Beyond the Do Not Track developments, broader initiatives to improve consumer privacy are underway in Congress, Federal agencies, and the private sector. For example, Congress is considering several general privacy bills that would establish a regulatory framework for protecting consumer privacy by improving transparency about the commercial uses of personal information and providing consumers with choice about such use.¹⁶ The bills would also provide the Commission rulemaking authority concerning, among other things, notice, consent, and the transfer of information to third parties.

In the House of Representatives, Members have introduced bipartisan legislation to amend the Children’s Online Privacy Protection Act¹⁷ (“COPPA”) and establish other protections for children and teens.¹⁸ The bill would prohibit the collection and use of minors’ information for targeted marketing and would require websites to permit the deletion of publicly available information of minors. Members of Congress also introduced a number of other bills addressing data security and data breach notification in 2011.¹⁹

-
- 15 The W3C is an international standard-setting body that works “to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web.” See W3C Mission, <http://www.w3.org/Consortium/mission.html>.
- 16 See Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Congress (2011); Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 611, 112th Congress (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Congress (2011).
- 17 Children’s Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506.
- 18 See Do Not Track Kids Act of 2011, H.R. 1895, 112th Congress (2011). In September 2011, the Commission issued a Notice of Proposed Rulemaking, proposing changes to the COPPA Rule to address changes in technology. See *FTC Children’s Online Privacy Protection Rule*, 76 Fed. Reg. 59804 (proposed Sep. 27, 2011), available at <http://www.ftc.gov/os/2011/09/110915coppa.pdf>.
- 19 See Personal Data Privacy and Security Act of 2011, S. 1151, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011); Data Breach Notification Act of 2011, S.1408, 112th Congress (2011); Data Security Act of 2011, S.1434, 112th Congress (2011); Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Congress (2011); Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Secure and Fortify Electronic Data Act, H.R. 2577, 112th Congress (2011).

Federal agencies have taken significant steps to improve consumer privacy as well. For its part, since issuing the preliminary staff report, the FTC has resolved seven data security cases,²⁰ obtained orders against Google, Facebook, and online ad networks,²¹ and challenged practices that violate sector-specific privacy laws like the Fair Credit Reporting Act (“FCRA”) and COPPA.²² The Commission has also proposed amendments to the COPPA Rule to address changes in technology. The comment period on the Proposed Rulemaking ran through December 23, 2011, and the Commission is currently reviewing the comments received.²³ Additionally, the Commission has hosted public workshops on discrete privacy issues such as child identity theft and the use of facial recognition technology.

Other federal agencies have also begun examining privacy issues. In 2011, the Federal Communications Commission (“FCC”) hosted a public forum to address privacy concerns associated with location-based services.²⁴ The Department of Health and Human Services (“HHS”) hosted a forum on medical identity theft, developed a model privacy notice for personal health records,²⁵ and is developing legislative recommendations on privacy and security for such personal health records. In addition, HHS recently launched an initiative to identify privacy and security best practices for using mobile devices in health care settings.²⁶

20 See *In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Jan. 18, 2012) (proposed consent order), available at <http://www.ftc.gov/os/caselist/1023116/index.shtm>; *In the Matter of ACRAnet, Inc.*, FTC Docket No. C-4331 (Aug. 17, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/0923088/index.shtm>; *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330 (Aug. 17, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/0823208/index.shtm>; *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/1023160/index.shtm>; *In the Matter of Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/1023076/index.shtm>; *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/0923093/index.shtm>; *In the Matter of Fajilan & Assocs., Inc.*, FTC Docket No. C-4332 (Aug. 17, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/0923089/index.shtm>.

21 See *In the Matter of Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/1023136/index.shtm> (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), available at <http://www.ftc.gov/os/caselist/0923184/index.shtm> (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Chitika, Inc.*, FTC Docket No. C-4324 (June 7, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/1023087/index.shtm> (requiring company’s behavioral advertising opt out to last for five years); *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 14, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/1023185/index.shtm> (requiring company to improve disclosure of its data collection practices and offer consumers a user-friendly opt out mechanism).

22 Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*; COPPA Rule, 16 C.F.R. Part 312; see also, e.g., *United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal. Sept. 8, 2011) (COPPA consent decree); *United States v. Teletrack, Inc.*, No. 11-CV-2060 (N.D. Ga. filed June 24, 2011) (FCRA consent decree); *United States v. Playdom, Inc.*, No. SACV-11-00724-AG (ANx) (C.D. Cal. May 24, 2011) (COPPA consent decree).

23 See Press Release, FTC Extends Deadline for Comments on Proposed Amendments to the Children’s Online Privacy Protection Rule Until December 23 (Nov. 18, 2011), available at <http://www.ftc.gov/opa/2011/11/coppa.shtm>.

24 See FCC Workshop, *Helping Consumers Harness the Potential of Location-Based Services* (June 28, 2011), available at <http://www.fcc.gov/events/location-based-services-forum>.

25 See The Office of the National Coordinator for Health Information Technology, Personal Health Record (PHR) Model Privacy Notice, http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__draft_phr_model_notice/1176.

26 See HHS Workshop, *Mobile Devices Roundtable: Safeguarding Health Information*, available at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__mobile_devices_roundtable/3815.

The private sector has taken steps to enhance user privacy and security as well. For example, Google and Facebook have improved authentication mechanisms to give users stronger protection against compromised passwords.²⁷ Also, privacy-enhancing technologies such as the HTTPS Everywhere browser add-on have given users additional tools to encrypt their information in transit.²⁸ On the mobile front, the Mobile Marketing Association released its Mobile Application Privacy Policy.²⁹ This document provides guidance on privacy principles for application (“app”) developers and discusses how to inform consumers about the collection and use of their data. Despite these developments, as explained below, industry still has more work to do to promote consumer privacy.

III. MAIN THEMES FROM COMMENTERS

The more than 450 comments filed in response to the preliminary staff report addressed three overarching issues: how privacy harms should be articulated; the value of global interoperability of different privacy regimes; and the desirability of baseline privacy legislation to augment self-regulatory efforts. Those comments, and the Commission’s analysis, are discussed below.

A. ARTICULATION OF PRIVACY HARMS

There was broad consensus among commenters that consumers need basic privacy protections for their personal information. This is true particularly in light of the complexity of the current personal data ecosystem. Some commenters also stated that the Commission should recognize a broader set of privacy harms than those involving physical and economic injury.³⁰ For example, one commenter cited complaints from consumers who had been surreptitiously tracked and targeted with prescription drug offers and other health-related materials regarding sensitive medical conditions.³¹

At the same time, some commenters questioned whether the costs of broader privacy protections were justified by the anticipated benefits.³² Relatedly, many commenters raised concerns about how wider privacy protections would affect innovation and the ability to offer consumers beneficial new products and services.³³

27 See *Advanced Sign-In Security For Your Google Account*, GOOGLE OFFICIAL BLOG (Feb. 10, 2011, 11:30 AM), <http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html#/2011/02/advanced-sign-in-security-for-your.html>; Andrew Song, *Introducing Login Approvals*, FACEBOOK BLOG (May 12, 2011, 9:58 AM), http://www.facebook.com/note.php?note_id=10150172618258920.

28 See *HTTPS Everywhere*, ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/https-everywhere>.

29 See Press Release, Mobile Marketing Association, Mobile Marketing Association Releases Final Privacy Policy Guidelines for Mobile Apps (Jan. 25, 2012), *available at* <http://mmaglobal.com/news/mobile-marketing-association-releases-final-privacy-policy-guidelines-mobile-apps>.

30 See *Comment of TRUSTe*, cmt. #00450, at 3; *Comment of Berlin Commissioner for Data Protection & Freedom of Information*, cmt. #00484, at 1.

31 See *Comment of Patient Privacy Rights*, cmt. #00470, at 2.

32 See *Comment of Technology Policy Institute*, cmt. #00301, at 5-8; *Comment of Experian*, cmt. #00398, at 9-11; *Comment of Global Privacy Alliance*, cmt. #00367, at 6-7.

33 See *Comment of Facebook, Inc.*, cmt. #00413, at 1-2, 7-8; *Comment of Google, Inc.*, cmt. #00417, at 4; *Comment of Global Privacy Alliance*, cmt. #00367, at 16.

The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties.³⁴ As one example, in the Commission's case against Google, the complaint alleged that Google used the information of consumers who signed up for Gmail to populate a new social network, Google Buzz.³⁵ The creation of that social network in some cases revealed previously private information about Gmail users' most frequent email contacts. Similarly, the Commission's complaint against Facebook alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful.³⁶ Like these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.³⁷

In terms of weighing costs and benefits, although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will benefit businesses by building consumer trust in the marketplace. Businesses frequently acknowledge the importance of consumer trust to the growth of digital commerce³⁸ and surveys support this view. For

34 One former FTC Chairman, in analyzing a spyware case, emphasized that consumers should have control over what is on their computers. Chairman Majoras issued the following statement in connection with the Commission's settlement against Sony BMG resolving claims about the company's installation of invasive tracking software: "Consumers' computers belong to them, and companies must adequately disclose unexpected limitations on the customary use of their products so consumers can make informed decisions regarding whether to purchase and install that content." Press Release, FTC, Sony BMG Settles FTC Charges (Jan. 30, 2007), *available at* <http://www.ftc.gov/opa/2007/01/sony.shtm>; *see also* Walt Mossberg, *Despite Others' Claims, Tracking Cookies Fit My Spyware Definition*, ALLTHINGS D (July 14, 2005, 12:01 AM), <http://allthingsd.com/20050714/tracking-cookies/> ("Suppose you bought a TV set that included a component to track what you watched, and then reported that data back to a company that used or sold it for advertising purposes. Only nobody told you the tracking technology was there or asked your permission to use it. You would likely be outraged at this violation of privacy. Yet that kind of Big Brother intrusion goes on everyday on the Internet . . . [with tracking cookies].").

35 *See In re Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcompt.pdf>.

36 *See In re Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* <http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf>.

37 Although the complaint against Google alleged that the company used deceptive tactics and violated its own privacy promises when it launched Google Buzz, even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm. *See* Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), *available at* <http://www.ftc.gov/opa/2011/03/google.shtm> (noting that in response to the Buzz launch, Google received thousands of complaints from consumers who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors).

38 *See, e.g.*, Statement of John M. Montgomery, GroupM Interaction, *The State of Online Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 112th Cong. (Mar. 16, 2011), *available at* http://www.iab.net/media/file/DC1DOCS1-432016-v1-John_Montgomery_-_Written_Testimony.pdf ("We at GroupM strongly believe in protecting consumer privacy. It is not only the right thing to do, but it is also good for business."); Statement of Alan Davidson, Director of Public Policy, Google Inc., *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the S. Subcomm. on Privacy, Tech., and the Law*, 112th Cong. (May 10, 2011), *available at* <http://www.judiciary.senate.gov/pdf/11-5-10%20Davidson%20Testimony.pdf> ("Protecting privacy and security is essential for Internet commerce.").

example, in the online behavioral advertising area, a recent survey shows that consumers feel better about brands that give them transparency and control over advertisements.³⁹

Companies offering consumers information about behavioral advertising and the tools to opt out of it have also found increased customer engagement. In its comment, Google noted that visitors to its Ads Preference Manager are far more likely to edit their interest settings and remain opted in rather than to opt out.⁴⁰ Similarly, another commenter conducted a study showing that making its customers aware of its privacy and data security principles – including restricting the sharing of customer data, increasing the transparency of data practices, and providing access to the consumer data it maintains – significantly increased customer trust in its company.⁴¹

In addition, some companies appear to be competing on privacy. For example, one company offers an Internet search service that it promotes as being far more privacy-sensitive than other search engines.⁴² Similarly, in response to Google's decision to change its privacy policies to allow tracking of consumers across different Google products, Microsoft encouraged consumers to switch to Microsoft's more privacy-protective products and services.⁴³

The privacy framework is designed to be flexible to permit and encourage innovation. Companies can implement the privacy protections of the framework in a way that is proportional to the nature, sensitivity, and amount of data collected as well as to the size of the business at issue. For example, the framework does not include rigid provisions such as specific disclosures or mandatory data retention and destruction periods. And, as discussed below, the framework streamlines communications for businesses and consumers alike by requiring consumer choice mechanisms only for data practices that are inconsistent with the context of a particular transaction or the business relationship with the consumer.⁴⁴

B. GLOBAL INTEROPERABILITY

Reflecting differing legal, policy, and constitutional regimes, privacy frameworks around the world vary considerably. Many commenters cited the value to both consumers and businesses of promoting more consistent and interoperable approaches to protecting consumer privacy internationally. These commenters stated that consistency between different privacy regimes reduces companies' costs, promotes international competitiveness, and increases compliance with privacy standards.⁴⁵

39 See *RESEARCH: Consumers Feel Better About Brands That Give Them Transparency and Control Over Ads*, EVIDON BLOG (Nov. 10, 2010), <http://blog.evidon.com/tag/better-advertising> ("when advertisers empower consumers with information and control over the ads they receive, a majority feels more positive toward those brands, and 36% even become more likely to purchase from those brands").

40 See *Comment of Google Inc.*, cmt. #00417, at 4.

41 See *Comment of Intuit, Inc.*, cmt. #00348, at 6-8 ("The more transparent (meaning open, simple and clear) the company is, the more customer trust increases. . .").

42 See DuckDuckGo, Privacy Policy, <https://duckduckgo.com/privacy.html>.

43 See Frank X. Shaw, *Gone Google? Got Concerns? We Have Alternatives*, THE OFFICIAL MICROSOFT BLOG (Feb. 1, 2012, 2:00 AM), http://blogs.technet.com/b/microsoft_blog/archive/2012/02/01/gone-google-got-concerns-we-have-alternatives.aspx.

44 See *infra* at Section IV.C.1.a.

45 See *Comment of AT&T Inc.*, cmt. #00420, at 12-13; *Comment of IBM*, cmt. #00433, at 2; see also *Comment of General Electric*, cmt. #00392, at 3 (encouraging international harmonization).

The Commission agrees there is value in greater interoperability among data privacy regimes as consumer data is increasingly transferred around the world. Meaningful protection for such data requires convergence on core principles, an ability of legal regimes to work together, and enhanced cross-border enforcement cooperation. Such interoperability is better for consumers, whose data will be subject to more consistent protection wherever it travels, and more efficient for businesses by reducing the burdens of compliance with differing, and sometimes conflicting, rules. In short, as the Administration White Paper notes, global interoperability “will provide more consistent protections for consumers and lower compliance burdens for companies.”⁴⁶

Efforts underway around the world to re-examine current approaches to protecting consumer privacy indicate an interest in convergence on overarching principles and a desire to develop greater interoperability. For example, the Commission’s privacy framework is consistent with the nine privacy principles set forth in the 2004 Asia-Pacific Economic Cooperation (“APEC”) Privacy Framework. Those principles form the basis for ongoing APEC work to implement a cross-border privacy rules system to facilitate data transfers among the 21 APEC member economies, including the United States.⁴⁷ In 2011, the Organization for Economic Cooperation and Development (“OECD”) issued a report re-examining its seminal 1980 Privacy Guidelines in light of technological changes over the past thirty years.⁴⁸ Further, the European Commission has recently proposed legislation updating its 1995 data protection directive and proposed an overhaul of the European Union approach that focuses on many of the issues raised elsewhere in this report as well as issues relating to international transfers and interoperability.⁴⁹ These efforts reflect a commitment to many of the high-level principles embodied in the FTC’s framework – increased transparency and consumer control, the need for privacy protections to be built into basic business practices, and the importance of accountability and enforcement. They also reflect a shared international interest in having systems that work better with each other, and are thus better for consumers.

46 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, ii, Foreword (Feb. 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

47 The nine principles in the APEC Privacy Framework are preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, accountability. Businesses have developed a code of conduct based on these nine principles and will obtain third-party certification of their compliance. A network of privacy enforcement authorities from participating APEC economies, such as the FTC, will be able to take enforcement actions against companies that violate their commitments under the code of conduct. See Press Release, FTC, FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region (Nov. 14, 2011), available at <http://www.ftc.gov/opa/2011/11/apec.shtm>.

48 See Organization for Economic Co-operation and Development, *The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines* (Apr. 2011), available at <http://www.oecd.org/dataoecd/22/25/47683378.pdf>.

49 European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (Jan. 25, 2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

C. LEGISLATION TO AUGMENT SELF-REGULATORY EFFORTS

Numerous comments, including those from large industry stakeholders, consumer and privacy advocates, and individual consumers supported some form of baseline privacy legislation that incorporates the FIPPs.⁵⁰ Business commenters noted that legislation would help provide legal certainty,⁵¹ serve as a key mechanism for building trust among customers,⁵² and provide a way to fill gaps in existing sector-based laws.⁵³ Consumer and privacy advocates cited the inability of self-regulation to provide comprehensive and long-lasting protection for consumers.⁵⁴ One such commenter cited the fact that many self-regulatory initiatives that arose in response to the Commission's 2000 recommendation for privacy legislation were short-lived and failed to provide long-term privacy protections for consumers.⁵⁵

At the same time, a number of commenters raised concerns about government action beyond providing guidance for self-regulatory programs.⁵⁶ Some cautioned the FTC about taking an approach that might impede industry's ability to innovate and develop new products and services in a rapidly changing marketplace. Others noted that a regulatory approach could lead to picking "winners and losers" among particular technologies and business models and called for a technology-neutral approach.⁵⁷ Commenters also argued that it might be impractical to craft omnibus standards or rules that would apply broadly across different business sectors.⁵⁸

The Commission agrees that, to date, self-regulation has not gone far enough. In most areas, with the notable exception of efforts surrounding Do Not Track, there has been little self-regulation. For example, the FTC's recent survey of mobile apps marketed to children revealed that many of these apps fail to provide any disclosure about the extent to which they collect and share consumers' personal data.⁵⁹ Similarly, efforts

50 See, e.g., *Comment of eBay*, cmt. #00374, at 2; *Comment of Intel Corp.*, cmt. #00246, at 3-7; *Comment of Microsoft Corp.*, cmt. #00395, at 4; *Comment of Intuit, Inc.*, cmt. #00348, at 13-14; *Comment of Center for Democracy & Technology*, cmt. #00469, at 1, 7; *Comment of Gregory Byrd*, cmt. #00144, at 1; *Comment of Ellen Klinefelter*, cmt. #00095, at 1.

51 See *Comment of Microsoft Corp.*, cmt. #00395, at 4.

52 See *Comment of Intel Corp.*, cmt. #00246, at 3.

53 See *Comment of Intuit, Inc.*, cmt. #00348, at 13.

54 See *Comment of Electronic Privacy Information Center*, cmt. #00386, at 2; *Comment of World Privacy Forum*, cmt. #00376, at 2-3, 8-17.

55 See *Comment of World Privacy Forum*, cmt. #00376, at 2-3, 8-17.

56 See *Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4-5; *Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 3; *Comment of Facebook, Inc.*, cmt. #00413, at 13-14; *Comment of Google Inc.*, cmt. #00417, at 8; *Comment of Verizon*, cmt. #00428, at 2-3, 6-7, 14-17; *Comment of Mortgage Bankers Ass'n*, cmt. #00308, at 2; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 3, 5, 7-13; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 15.

57 See *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 32-37; *Comment of USTelecom*, cmt. #00411, at 5-7; *Comment of Verizon*, cmt. #00428, at 4-6; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 5-6.

58 See *Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4-6; see also *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 8-11; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 13.

59 FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), available at http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; *FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack a Privacy Policy*, FUTURE OF PRIVACY FORUM, <http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/>.

of the data broker industry to establish self-regulatory rules concerning consumer privacy have fallen short.⁶⁰ These examples illustrate that even in some well-established markets, basic privacy concepts like transparency about the nature of companies' data practices and meaningful consumer control are absent. This absence erodes consumer trust.

There is also widespread evidence of data breaches and vulnerabilities related to consumer information.⁶¹ Published reports indicate that some breaches may have resulted from the unintentional release of consumer data, for which companies later apologized and took action to address.⁶² Other incidents involved planned releases or uses of data by companies that ultimately did not occur due to consumer and public backlash.⁶³ Still other incidents involved companies' failure to take reasonable precautions and resulted in FTC consent decrees. These incidents further undermine consumer trust, which is essential for business growth and innovation.⁶⁴

The ongoing and widespread incidents of unauthorized or improper use and sharing of personal information are evidence of two points. First, companies that do not intend to undermine consumer privacy simply lack sufficiently clear standards to operate and innovate while respecting the expectations of consumers. Second, companies that do seek to cut corners on consumer privacy do not have adequate legal incentives to curtail such behavior.

To provide clear standards and appropriate incentives to ensure basic privacy protections across all industry sectors, in addition to reiterating its call for federal data security legislation,⁶⁵ the Commission calls

60 See *Comment of Center for Democracy & Technology*, cmt. #00469, at 2-3; *Comment of World Privacy Forum*, cmt. #00376, at 2-3. Discussed more fully *infra* at Section IV.D.2.a.

61 See Grant Gross, *Lawmakers Question Sony, Epsilon on Data Breaches*, PC WORLD (June 2, 2011 3:40 PM), available at http://www.pcworld.com/businesscenter/article/229258/lawmakers_question_sony_epsilon_on_data_breaches.html; Dwight Silverman, *App Privacy: Who's Uploading Your Contact List?*, HOUSTON CHRONICLE (Feb. 15, 2012 8:10 AM), <http://blog.chron.com/techblog/2012/02/app-privacy-whos-uploading-your-contact-list/>; Dan Graziano, *Like iOS apps, Android Apps Can Secretly Access Photos Thanks to Loophole*, BGR (Mar. 1, 2012 3:45 PM), <http://www.bgr.com/2012/03/01/like-ios-apps-android-apps-can-also-secretly-access-photos-thanks-to-security-hole/>.

62 *CEO Apologizes After Path Social App Uploads Contact Lists*, KMOV.COM (Feb. 9, 2012 11:11AM), <http://www.kmov.com/news/consumer/CEO-apologizes-after-Path-uploads-contact-lists--139015729.html>; Daisuke Wakabayashi, *A Contrite Sony Vows Tighter Security*, WALL ST. J. May 1, 2011, available at <http://online.wsj.com/article/SB10001424052748704436004576296302384608280.html>.

63 Kevin Parrish, *OnStar Changes its Mind About Tracking Vehicles*, TOM'S GUIDE (Sept. 29, 2011 7:30 AM), <http://www.tomsguide.com/us/OnStar-General-motors-Linda-Marshall-GPS-Terms-and-conditions,news-12677.html>.

64 Surveys of consumer attitudes towards privacy conducted in the past year are illuminating. For example, a *USA Today*/Gallup poll indicated that a majority of the Facebook members or Google users surveyed were "very" or "somewhat concerned" about their privacy while using these services. Lymari Morales, *Google and Facebook Users Skew Young, Affluent, and Educated*, GALLUP (Feb. 17, 2011), available at <http://www.gallup.com/poll/146159/facebook-google-users-skew-young-affluent-educated.aspx>.

65 The Commission has long supported federal laws requiring companies to implement reasonable security measures and to notify consumers in the event of certain security breaches. See, e.g., Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (June 15, 2011), available at <http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf>; Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft: Hearing Before the H. Comm. on Ways and Means, Subcomm. on Social Security*, 112th Cong. (April 13, 2011), available at <http://www.ftc.gov/os/testimony/110411ssn-idtheft.pdf>; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), available at <http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf>; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), available at <http://www.idtheft.gov/reports/IDTReport2008.pdf>.

on Congress to consider enacting baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate. The Commission is prepared to work with Congress and other stakeholders to craft such legislation.

In their comments, many businesses indicated that they already incorporate the FIPPS into their practices. For these companies, a legislative mandate should not impose an undue burden and indeed, will “level the playing field” by ensuring that all companies are required to incorporate these principles into their practices.

For those companies that are not already taking consumer privacy into account – either because of lack of understanding or lack of concern – legislation should provide clear rules of the road. It should also provide adequate deterrence through the availability of civil penalties and other remedies.⁶⁶ In short, legislation will provide businesses with the certainty they need to understand their obligations and the incentive to meet those obligations, while providing consumers with confidence that businesses will be required to respect their privacy. This approach will create an environment that allows businesses to continue to innovate and consumers to embrace those innovations without sacrificing their privacy.⁶⁷ The Commission is prepared to work with Congress and other stakeholders to formulate baseline privacy legislation.

While Congress considers such legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission’s final privacy framework. Over the course of the next year, Commission staff will promote the framework’s implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- ◆ **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- ◆ **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures.⁶⁸ As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to

66 Former FTC Chairman Casper “Cap” Weinberger recognized the value of civil penalties as a deterrent to unlawful conduct. See *Hearings on H.R. 14931 and Related Bills before the Subcomm. on Commerce and Finance of the H. Comm. on Interstate and Foreign Commerce*, 91st Cong. 53, 54 (1970) (statement of FTC Chairman Caspar Weinberger); *Hearings on S. 2246, S. 3092, and S. 3201 Before the Consumer Subcomm. of the S. Comm. on Commerce*, 91st Cong. 9 (1970) (Letter from FTC Chairman Caspar W. Weinberger) (forwarding copy of House testimony).

67 With this report, the Commission is not seeking to impose civil penalties for privacy violations under the FTC Act. Rather, in the event Congress enacts privacy legislation, the Commission believes that such legislation would be more effective if the FTC were authorized to obtain civil penalties for violations.

68 See Press Release, FTC, FTC Seeks Input to Revising its Guidance to Businesses About Disclosures in Online Advertising (May 26, 2011), available at <http://www.ftc.gov/opa/2011/05/dotcom.shtm>.

consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

- ◆ **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker.⁶⁹ To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- ◆ **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers (“ISPs”), operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.
- ◆ **Promoting enforceable self-regulatory codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

⁶⁹ See Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).

IV. PRIVACY FRAMEWORK

In addition to the general comments described above, the Commission received significant comments on the scope of the proposed framework and each individual element. Those comments, as well as several clarifications and refinements based on the Commission's analysis of the issues raised, are discussed below.

A. SCOPE

Proposed Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device.

A variety of commenters addressed the framework's proposed scope. Some of these commenters supported an expansive reach while others proposed limiting the framework's application to particular types of entities and carving out certain categories of businesses. Commenters also called for further clarification regarding the type of data the framework covers and staff's proposed "reasonably linked" standard.

1. COMPANIES SHOULD COMPLY WITH THE FRAMEWORK UNLESS THEY HANDLE ONLY LIMITED AMOUNTS OF NON-SENSITIVE DATA THAT IS NOT SHARED WITH THIRD PARTIES.

Numerous commenters addressed whether the framework should apply to entities that collect, maintain, or use limited amounts of data. Several companies argued that the burden the framework could impose on small businesses outweighed the reduced risk of harm from the collection and use of limited amounts of non-sensitive consumer data.⁷⁰ These commenters proposed that the framework not apply to entities that collect or use non-sensitive data from fewer than 5,000 individuals a year where the data is used for limited purposes, such as internal operations and first-party marketing.⁷¹ As additional support for this position, these commenters noted that proposed privacy legislation introduced in the 111th Congress contained an exclusion to this effect.⁷²

Although one consumer and privacy organization supported a similar exclusion,⁷³ others expressed concern about exempting, *per se*, any types of businesses or quantities of data from the framework's scope.⁷⁴ These commenters pointed to the possibility that excluded companies would sell the data to third parties, such as advertising networks or data brokers.

The Commission agrees that the first-party collection and use of non-sensitive data (*e.g.*, data that is not a Social Security number or financial, health, children's, or geolocation information) creates fewer privacy

⁷⁰ See *Comment of eBay, Inc.*, cmt. #00374, at 3; *Comment of Microsoft Corp.*, cmt. #00395, at 4.

⁷¹ *Id.*

⁷² See BEST PRACTICES ACT, H.R. 5777, 111th Congress (2010); Staff Discussion Draft, H.R. ___, 111th Congress (2010), available at <http://www.nciss.org/legislation/BoucherStearnsprivacydiscussiondraft.pdf>.

⁷³ *Comment of the Center for Democracy & Technology*, cmt. #00469, at 1.

⁷⁴ See *Comment of the Electronic Frontier Foundation*, cmt. #00400, at 1; *Comment of the Consumer Federation of America*, cmt. #00358, at 2.

concerns than practices that involve sensitive data or sharing with third parties.⁷⁵ Accordingly, entities that collect limited amounts of non-sensitive consumer data from under 5,000 consumers need not comply with the framework, as long as they do not share the data with third parties. For example, consider a cash-only curb-side food truck business that offers to send messages announcing when it is in a given neighborhood to consumers who provide their email addresses. As long as the food truck business does not share these email addresses with third parties, the Commission believes that it need not provide privacy disclosures to its customers. This narrow exclusion acknowledges the need for flexibility for businesses that collect limited amounts of non-sensitive information. It also recognizes that some business practices create fewer potential risks to consumer information.

2. THE FRAMEWORK SETS FORTH BEST PRACTICES AND CAN WORK IN TANDEM WITH EXISTING PRIVACY AND SECURITY STATUTES.

The proposed framework's applicability to commercial sectors that are covered by existing laws generated comments primarily from representatives of the healthcare and financial services industries. These commenters noted that statutes such as the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the Gramm-Leach-Bliley Act ("GLBA") already impose privacy protections and security requirements through legal obligations on companies in these industries.⁷⁶ Accordingly, these commenters urged the Commission to avoid creating duplicative or inconsistent standards and to clarify that the proposed framework is intended to cover only those entities that are not currently covered by existing privacy and security laws. Another commenter, however, urged government to focus on fulfilling consumer privacy expectations across all sectors, noting that market evolution is blurring distinctions about who is covered by HIPAA and that consumers expect organizations to protect their personal health information, regardless of any sector-specific boundaries.⁷⁷

The Commission recognizes the concern regarding potentially inconsistent privacy obligations and notes that, to the extent Congress enacts any of the Commission's recommendations through legislation, such legislation should not impose overlapping or duplicative requirements on conduct that is already regulated.⁷⁸ However, the framework is meant to encourage best practices and is not intended to conflict with requirements of existing laws and regulations. To the extent that components of the framework exceed, but do not conflict with existing statutory requirements, entities covered by those statutes should view the framework as best practices to promote consumer privacy. For example, it may be appropriate for financial institutions covered by GLBA to incorporate elements of privacy by design, such as collection limitations, or

⁷⁵ See *infra* at Sections IV.C.1.b.(v) and IV.C.2.e.(ii), for a discussion of what constitutes sensitive data.

⁷⁶ See *Comment of the Confidentiality Coalition c/o the Healthcare Leadership Council*, cmt. #00349, at 1-4; *Comment of Experian*, cmt. #00398, at 8-10; *Comment of IMS Health*, cmt. #00380, at 2-3; *Comment of Medco Health Solutions, Inc.*, cmt. #00393, at 3; *Comment of SIFMA*, cmt. #00265, at 2-3.

⁷⁷ *Comment of The Markle Foundation*, cmt. #00456, at 3-10.

⁷⁸ Any baseline privacy law Congress may enact would likely consider the best way to take into account obligations under existing statutes.

to improve transparency by providing reasonable access to consumer data in a manner that does not conflict with their statutory obligations. In any event, the framework provides an important baseline for entities that are not subject to sector-specific laws like HIPAA or GLBA.⁷⁹

3. THE FRAMEWORK APPLIES TO OFFLINE AS WELL AS ONLINE DATA.

In addressing the framework's applicability to "all commercial entities," numerous commenters discussed whether the framework should apply to both online and offline data. Diverse commenters expressed strong support for a comprehensive approach applicable to both online and offline data practices.⁸⁰ Commenters noted that as a practical matter, many companies collect both online and offline data.⁸¹

Commenters also listed different offline contexts in which entities collect consumer data. These include instances where a consumer interacts directly with a business, such as through the use of a retail loyalty card, or where a non-consumer facing entity, such as a data broker, obtains consumer data from an offline third-party source.⁸² One commenter noted that, regardless of whether an entity collects or uses data from an online or an offline source, consumer privacy interests are equally affected.⁸³ To emphasize the importance of offline data protections, this commenter noted that while the behavioral advertising industry has started to implement self-regulatory measures to improve consumers' ability to control the collection and the use of their online data, in the offline context such efforts by data brokers and others have largely failed.⁸⁴

By contrast, a financial industry organization argued that the FTC should take a more narrow approach by limiting the scope of the proposed framework in a number of respects, including its applicability to offline data collection and use.⁸⁵ This commenter stated that some harms in the online context may not exist offline and raised concern about the framework's unintended consequences. For example, the commenter cited the significant costs that a requirement to provide consumers with access to data collected about them

79 There may be entities that operate within covered sectors but that nevertheless fall outside of a specific law's scope. For instance, a number of entities that collect health information are not subject to HIPAA. These entities include providers of personal health records – online portfolios that consumers can use to store and keep track of their medical information. In 2009, Congress passed the HITECH Act, which required HHS, in consultation with the FTC, to develop legislative recommendations on privacy and security requirements that should apply to these providers of personal health records and related entities. Health Information Technology ("HITECH") Provisions of American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D (Pub. L. 111-5, 123 Stat. 115, codified in relevant part at 42 U.S.C. §§ 17937 and 17954). FTC staff is consulting with HHS on this project.

80 See *Comment of the Center for Democracy & Technology*, cmt. #00469, at 2; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14; *Comment of Consumers Union*, cmt. #00362, at 4-5; *Comment of the Department of Veterans Affairs*, cmt. #00479, at 3; *Comment of Experian*, cmt. #00398, at 1; *Comment of Google Inc.*, cmt. #00417, at 7; *Comment of Microsoft Corp.*, cmt. #00395, at 4.

81 See *Comment of the Department of Veterans Affairs*, cmt. #00479, at 3 n.7; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14; *Comment of Consumers Union*, cmt. #00362, at 1.

82 See *Comment of the Department of Veterans Affairs*, cmt. #00479, at 3 n.7; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14.

83 *Comment of Center for Democracy & Technology*, cmt. #00469, at 2.

84 *Comment of Center for Democracy & Technology*, cmt. #00469, at 2-3.

85 *Comment of the Financial Services Forum*, cmt. #00381, at 8-9.

would impose on companies that collect and maintain data in paper rather than electronic form. Another commenter cited the costs of providing privacy disclosures and choices in an offline environment.⁸⁶

The Commission notes that consumers face a landscape of virtually ubiquitous collection of their data. Whether such collection occurs online or offline does not alter the consumer's privacy interest in his or her data. For example, the sale of a consumer profile containing the consumer's purchase history from a brick-and-mortar pharmacy or a bookstore would not implicate fewer privacy concerns simply because the profile contains purchases from an offline retailer rather than from an online merchant. Accordingly, the framework applies in all commercial contexts, both online and offline.

4. THE FRAMEWORK APPLIES TO DATA THAT IS REASONABLY LINKABLE TO A SPECIFIC CONSUMER, COMPUTER, OR DEVICE.

The scope issue that generated the most comments, from a wide range of interested parties, was the proposed framework's applicability to "consumer data that can be reasonably linked to a specific consumer, computer, or other device."

A number of commenters supported the proposed framework's application to data that, while not traditionally considered personally identifiable, is linkable to a consumer or device. In particular, several consumer and privacy groups elaborated on the privacy concerns associated with supposedly anonymous data and discussed the decreasing relevance of the personally identifiable information ("PII") label.⁸⁷ These commenters pointed to studies demonstrating consumers' objections to being tracked, regardless of whether the tracker explicitly learns a consumer name, and the potential for harm, such as discriminatory pricing based on online browsing history, even without the use of PII.⁸⁸

Similarly, the commenters noted, the ability to re-identify "anonymous" data supports the proposed framework's application to data that can be reasonably linked to a consumer or device. They pointed to incidents, identified in the preliminary staff report, in which individuals were re-identified from publicly released data sets that did not contain PII.⁸⁹ One commenter pointed out that certain industries extensively

86 *Comment of National Retail Federation*, cmt. #00419, at 6 (urging FTC to limit privacy framework to online collection of consumer data because applying it to offline collection would be onerous for businesses and consumers).

87 See *Comment of the Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Consumers Union*, cmt. #00362, at 4-5. In addition, in their comments both AT&T and Mozilla recognized that the distinction between PII and non-PII is blurring. *Comment of AT&T Inc.*, cmt. #00420, at 13; *Comment of Mozilla*, cmt. #00480, at 6.

88 *Comment of Center for Democracy & Technology*, cmt. #00469, at 3 (citing Edward C. Baig, *Internet Users Say, Don't Track Me*, USA TODAY, Dec. 14, 2010, available at http://www.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm); Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll*, THE PRECURSOR BLOG (June 8, 2010), <http://www.precursorblog.com/content/americans-want-online-privacy-new-zogby-poll>); *Comment of Consumers Union*, cmt. #00362, at 4 (discussing the potential for discriminatory pricing (citing Annie Lowery, *How Online Retailers Stay a Step Ahead of Comparison Shoppers*, WASH. POST, Dec. 12, 2010, available at <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121102435.html>)).

89 For a brief discussion of such incidents, see FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, at 38 (Dec. 2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

mine data for marketing purposes and that re-identification is a commercial enterprise.⁹⁰ This adds to the likelihood of data re-identification.

Some industry commenters also recognized consumers' privacy interest in data that goes beyond what is strictly labeled PII.⁹¹ Drawing on the FTC's roundtables as well as the preliminary staff report, one such commenter noted the legitimate interest consumers have in controlling how companies collect and use aggregated or de-identified data, browser fingerprints,⁹² and other types of non-PII.⁹³ Another company questioned the notion of distinguishing between PII and non-PII as a way to determine what data to protect.⁹⁴ Supporting a scaled approach rather than a bright line distinction, this commenter noted that all data derived from individuals deserves some level of protection.⁹⁵

Other commenters representing industry opposed the proposed framework's application to non-PII that can be reasonably linked to a consumer, computer, or device.⁹⁶ These commenters asserted that the risks associated with the collection and use of data that does not contain PII are simply not the same as the risks associated with PII. They also claimed a lack of evidence demonstrating that consumers have the same privacy interest in non-PII as they do with the collection and use of PII. Instead of applying the framework to non-PII, these commenters recommended the Commission support efforts to de-identify data.

Overall, the comments reflect a general acknowledgment that the traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine the data's privacy implications.⁹⁷ However, some commenters, including some of those cited above, argued that the proposed framework's "linkability" standard is potentially too open-ended to be practical.⁹⁸ One industry organization asserted, for instance, that if given enough time and resources, any data may be linkable to an

90 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 4 (citing Julia Angwin & Steve Stecklow, 'Scrapers' Dig Deep for Data on Web, WALL ST. J., Oct. 12, 2010, available at <http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html>); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011).

91 *Comment of Mozilla*, cmt. #00480, at 4-5; *Comment of Google Inc.*, cmt. #00417, at 8.

92 The term "browser fingerprints" refers to the specific combination of characteristics – such as system fonts, software, and installed plugins – that are typically made available by a consumer's browser to any website visited. These characteristics can be used to uniquely identify computers, cell phones, or other devices. Browser fingerprinting does not rely on cookies. See Erik Larkin, *Browser Fingerprinting Can ID You Without Cookies*, PCWORLD, Jan. 29, 2010, available at http://www.pcworld.com/article/188161/browser_fingerprinting_can_id_you_without_cookies.html.

93 *Comment of Mozilla*, cmt. #00480, at 4-5 (citing FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, at 36-37 (Dec. 2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>).

94 *Comment of Google Inc.*, cmt. #00417, at 8.

95 *Comment of Google Inc.*, cmt. #00417, at 8.

96 *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 13-14; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 13-17.

97 See *Comment of AT&T Inc.*, cmt. #00420, at 13-15; *Comment of Center for Democracy & Technology* (Feb. 18, 2011), cmt. #00469, at 3-4; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 3-4; *Comment of Consumers Union*, cmt. #00362, at 4-5; *Comment of Electronic Frontier Foundation*, cmt. #00400, at 1-4; *Comment of Google Inc.*, cmt. #00417, at 7-8; *Comment of Mozilla*, cmt. #00480, at 4-6; *Comment of Phorm Inc.*, cmt. #00353, at 3-4.

98 *Comment of AT&T Inc.*, cmt. #00420, at 13; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375 at 3-4; *Comment of Google Inc.*, cmt. #00417, at 8; *Comment of Phorm Inc.*, cmt. #00353, at 4.

individual.⁹⁹ In addition, commenters stated that requiring the same level of protection for all data would undermine companies' incentive to avoid collecting data that is more easily identified or to take steps to de-identify the data they collect and use.¹⁰⁰ Other commenters argued that applying the framework to data that is potentially linkable could conflict with the framework's privacy by design concept, as companies could be forced to collect more information about consumers than they otherwise would in order to be able to provide those consumers with effective notice, choice, or access.¹⁰¹ To address these concerns, some commenters proposed limiting the framework to data that is actually linked to a specific consumer, computer, or device.¹⁰²

One commenter recommended that the Commission clarify that the reasonably linkable standard means non-public data that can be linked with *reasonable effort*.¹⁰³ This commenter also stated that the framework should exclude data that, through contract or by virtue of internal controls, will not be linked with a particular consumer. Taking a similar approach, another commenter suggested that the framework should apply to data that is reasonably likely to relate to an identifiable consumer.¹⁰⁴ This commenter also noted that a company could commit through its privacy policy that it would only maintain or use data in a de-identified form and that such a commitment would be enforceable under Section 5 of the FTC Act.¹⁰⁵

The Commission believes there is sufficient support from commenters representing an array of perspectives – including consumer and privacy advocates as well as of industry representatives – for the framework's application to data that, while not yet linked to a particular consumer, computer, or device, may reasonably become so. There is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer, or device even if the individual pieces of data do not constitute PII.¹⁰⁶ Moreover, not only is it possible to re-identify non-PII data through various means,¹⁰⁷ businesses have strong incentives to actually do so.

In response to the comments, to provide greater certainty for companies that collect and use consumer data, the Commission provides additional clarification on the application of the reasonable linkability standard to describe how companies can take appropriate steps to minimize such linkability. Under the final

99 *Comment of GSI*, cmt. #00439, at 2.

100 *Comment of AT&T Inc.*, cmt. #00420, at 13-14; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 4; *Comment of Experian*, cmt. #00398, at 11; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 16.

101 *Comment of United States Council for International Business*, cmt. #00366, at 1; *Comment of Phorm Inc.*, cmt. #00353, at 3.

102 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 4; *Comment of Yahoo! Inc.*, cmt. #00444, at 3-4; *Comment of GSI*, cmt. #00439, at 3.

103 *Comment of AT&T Inc.*, cmt. #00420, at 13.

104 *Comment of Intel Corp.*, cmt. #00246, at 9.

105 *Comment of Intel Corp.*, cmt. #00246, at 9.

106 FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, 35-38 (Dec. 2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12. See *supra* note 89.

107 See FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, 21-24, 43-45 (Feb. 2009), available at <http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf>; Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1836-1848 (2011).

framework, a company's data would not be reasonably linkable to a particular consumer or device to the extent that the company implements three significant protections for that data.

First, the company must take reasonable measures to ensure that the data is de-identified. This means that the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device. Consistent with the Commission's approach in its data security cases,¹⁰⁸ what qualifies as a reasonable level of justified confidence depends upon the particular circumstances, including the available methods and technologies. In addition, the nature of the data at issue and the purposes for which it will be used are also relevant. Thus, for example, whether a company publishes data externally affects whether the steps it has taken to de-identify data are considered reasonable. The standard is not an absolute one; rather, companies must take reasonable steps to ensure that data is de-identified.

Depending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or modification of data fields, the addition of sufficient "noise" to data, statistical sampling, or the use of aggregate or synthetic data.¹⁰⁹ The Commission encourages companies and researchers to continue innovating in the development and evaluation of new and better approaches to de-identification. FTC staff will continue to monitor and assess the state of the art in de-identification.

Second, a company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data. Thus, if a company does take steps to re-identify such data, its conduct could be actionable under Section 5 of the FTC Act.

Third, if a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data. The company that transfers or otherwise makes the data available should exercise reasonable oversight to monitor compliance with these contractual provisions and take appropriate steps to address contractual violations.¹¹⁰

FTC staff's letter closing its investigation of Netflix, arising from the company's plan to release purportedly anonymous consumer data to improve its movie recommendation algorithm, provides a good illustration of these concepts. In response to the privacy concerns that FTC staff and others raised, Netflix revised its initial plan to publicly release the data. The company agreed to narrow any such release of data to certain researchers. The letter details Netflix's commitment to implement a number of "operational

108 The Commission's approach in data security cases is a flexible one. Where a company has offered assurances to consumers that it has implemented reasonable security measures, the Commission assesses the reasonableness based, among other things, on the sensitivity of the information collected, the measures the company has implemented to protect such information, and whether the company has taken action to address and prevent well-known and easily addressable security vulnerabilities.

109 See, e.g., Cynthia Dwork, *A Firm Foundation for Private Data Analysis*, 54 COMM. OF THE ACM 86-95 (2011), available at http://research.microsoft.com/pubs/116123/dwork_cacm.pdf, and references cited therein.

110 See *In the Matter of Superior Mortg. Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005), available at <http://www.ftc.gov/os/caselist/0523136/0523136.shtm> (alleging a violation of the GLB Safeguards Rule for, among other things, a failure to ensure that service providers were providing appropriate security for customer information and addressing known security risks in a timely manner).

safeguards to prevent the data from being used to re-identify consumers.”¹¹¹ If it chose to share such data with third parties, Netflix stated that it would limit access “only to researchers who contractually agree to specific limitations on its use.”¹¹²

Accordingly, as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework.¹¹³

This clarification of the framework’s reasonable linkability standard is designed to help address the concern that the standard is overly broad. Further, the clarification gives companies an incentive to collect and use data in a form that makes it less likely the data will be linked to a particular consumer or device, thereby promoting privacy. Additionally, by calling for companies to publicly commit to the steps they take, the framework promotes accountability.¹¹⁴

Consistent with the discussion above, the Commission restates the framework’s scope as follows.

Final Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.

B. PRIVACY BY DESIGN

Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

The preliminary staff report called on companies to promote consumer privacy throughout their organizations and at every stage of the development of their products and services. Although many companies already incorporate substantive and procedural privacy protections into their business practices, industry should implement privacy by design more systematically. A number of commenters, including those representing industry, supported staff’s call that companies “build in” privacy, with several of these commenters citing to the broad international recognition and adoption of privacy by design.¹¹⁵ The Commission is encouraged to see broad support for this concept, particularly in light of the increasingly global nature of data transfers.

¹¹¹ Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., FTC, to Reed Freeman, Morrison & Foerster LLP, Counsel for Netflix, 2 (Mar. 12, 2010), *available at* <http://www.ftc.gov/os/closings/100312netflixletter.pdf> (closing letter).

¹¹² *Id.*

¹¹³ To the extent that a company maintains and uses both data that is identifiable and data that it has taken steps to de-identify as outlined here, the company should silo the data separately.

¹¹⁴ A company that violates its policy against re-identifying data could be subject to liability under the FTC Act or other laws.

¹¹⁵ *Comment of Office of the Information and Privacy Commissioner of Ontario*, cmt. #00239, at 2-3; *Comment of Intel Corp.*, cmt. #00246, at 12-13; *Comment of CNIL*, cmt. #00298, at 2-3.

In calling for privacy by design, staff advocated for the implementation of substantive privacy protections – such as data security, limitations on data collection and retention, and data accuracy – as well as procedural safeguards aimed at integrating the substantive principles into a company’s everyday business operations. By shifting burdens away from consumers and placing obligations on businesses to treat consumer data in a responsible manner, these principles should afford consumers basic privacy protections without forcing them to read long, incomprehensible privacy notices to learn and make choices about a company’s privacy practices. Although the Commission has not changed the proposed “privacy by design” principles, it responds to a number of comments, as discussed below.

1. THE SUBSTANTIVE PRINCIPLES: DATA SECURITY, REASONABLE COLLECTION LIMITS, SOUND RETENTION PRACTICES, AND DATA ACCURACY.

Proposed Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.

a. Should Additional Substantive Principles Be Identified?

Responding to a question about whether the final framework should identify additional substantive protections, several commenters suggested incorporating the additional principles articulated in the 1980 OECD Privacy Guidelines.¹¹⁶ One commenter also proposed adding the “right to be forgotten,” which would allow consumers to withdraw data posted online about themselves at any point.¹¹⁷ This concept has gained importance as people post more information about themselves online without fully appreciating the implications of such data sharing or the persistence of online data over time.¹¹⁸ In supporting an expansive view of privacy by design, a consumer advocacy group noted that the individual elements and principles of the proposed framework should work together holistically.¹¹⁹

In response, the Commission notes that the framework already embodies all the concepts in the 1980 OECD privacy guidelines, although with some updates and changes in emphasis. For example, privacy by design includes the collection limitation, data quality, and security principles. Additionally, the framework’s simplified choice and transparency components, discussed below, encompass the OECD principles of purpose specification, use limitation, individual participation, and openness. The framework also adopts the

¹¹⁶ *Comment of CNIL*, cmt. #00298, at 2; *Comment of the Information Commissioner’s Office of the UK*, cmt. #00249, at 2; *Comment of World Privacy Forum*, cmt. #00369, at 7; *Comment of Intel Corp.*, cmt. #00246, at 4; see also Organisation for Economic Co-operation & Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 1980), available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00&cen-USS_01DBC.html (these principles include purpose specification, individual participation, accountability, and principles to govern cross-border data transfers). Another commenter called for baseline legislation based on the Fair Information Practice Principles and the principles outlined in the 1974 Privacy Act. *Comment of Electronic Privacy Information Center*, cmt. #00386, at 17-20.

¹¹⁷ *Comment of CNIL*, cmt. #00298, at 3.

¹¹⁸ The concept of the “right to be forgotten,” and its importance to young consumers, is discussed in more detail below in the Transparency Section, *infra* at Section IV.D.2.b.

¹¹⁹ *Comment of Consumers Union*, cmt. #00362, at 1-2, 5-9, 18-19.

OECD principle that companies must be accountable for their privacy practices. Specifically, the framework calls on companies to implement procedures – such as designating a person responsible for privacy, training employees, and ensuring adequate oversight of third parties – to help ensure that they are implementing appropriate substantive privacy protections. The framework also calls on industry to increase efforts to educate consumers about the commercial collection and use of their data and the available privacy tools. In addition, there are aspects of the proposed “right to be forgotten” in the final framework, which calls on companies to (1) delete consumer data that they no longer need and (2) allow consumers to access their data and in appropriate cases suppress or delete it.¹²⁰

All of the principles articulated in the preliminary staff report are intended to work together to shift the burden for protecting privacy away from consumers and to encourage companies to make strong privacy protections the default. Reasonable collection limits and data disposal policies work in tandem with streamlined notices and improved consumer choice mechanisms. Together, they function to provide substantive protections by placing reasonable limits on the collection, use, and retention of consumer data to more closely align with consumer expectations, while also raising consumer awareness about the nature and extent of data collection, use, and third-party sharing, and the choices available to them.

b. Data Security: Companies Must Provide Reasonable Security for Consumer Data.

It is well settled that companies must provide reasonable security for consumer data. The Commission has a long history of enforcing data security obligations under Section 5 of the FTC Act, the FCRA and the GLBA. Since 2001, the FTC has brought 36 cases under these laws, charging that businesses failed to appropriately protect consumers’ personal information. Since issuance of the preliminary staff report alone, the Commission has resolved seven data security actions against resellers of sensitive consumer report information, service providers that process employee data, a college savings program, and a social media service.¹²¹ In addition to the federal laws the FTC enforces, companies are subject to a variety of

120 See *In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* <http://www.ftc.gov/os/caselist/0923184/index.shtm> (requiring Facebook to make inaccessible within thirty days data that a user deletes); *see also* Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011).

121 *In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Jan. 18, 2012) (proposed consent order), *available at* <http://www.ftc.gov/os/caselist/1023116/index.shtm>; *In the Matter of ACRAnet, Inc.*, FTC Docket No. C-4331 (Aug. 17, 2011) (consent order), *available at* <http://ftc.gov/os/caselist/0923088/index.shtm>; *In the Matter of Fajilan & Assocs., Inc.*, FTC Docket No. C-4332 (Aug. 17, 2011) (consent order), *available at* <http://ftc.gov/os/caselist/0923089/index.shtm>; *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330 (Aug. 17, 2011) (consent order), *available at* <http://ftc.gov/os/caselist/0823208/index.shtm>; *In the Matter of Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* <http://www.ftc.gov/os/caselist/102376/index.shtm>; *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* <http://www.ftc.gov/os/caselist/1023160/index.shtm>; *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 11, 2011) (consent order), *available at* <http://www.ftc.gov/os/caselist/0923093/index.shtm>.

other federal and state law obligations. In some industries, such as banking, federal regulators have given additional guidance on how to define reasonable security.¹²²

The Commission also promotes better data security through consumer and business education. For example, the FTC sponsors OnGuard Online, a website to educate consumers about basic computer security.¹²³ Since the Commission issued the preliminary staff report there have been over 1.5 million unique visits to OnGuard Online and its Spanish-language counterpart Alerta en Línea. The Commission's business outreach includes general advice about data security as well as specific advice about emerging topics.¹²⁴

The Commission also notes that the private sector has implemented a variety of initiatives in the security area, including the Payment Card Institute Data Security Standards for payment card data, the SANS Institute's security policy templates, and standards and best practices guidelines for the financial services industry provided by BITS, the technology policy division of the Financial Services Roundtable.¹²⁵ These standards can provide useful guidance on appropriate data security measures that organizations should implement for specific types of consumer data or in specific industries. The Commission further calls on industry to develop and implement best data security practices for additional industry sectors and other types of consumer data.

Because this issue is important to consumers and because businesses have existing legal and self-regulatory obligations, many individual companies have placed great emphasis and resources on maintaining reasonable security. For example, Google has cited certain security features in its products, including default SSL encryption for Gmail and security features in its Chrome browser.¹²⁶ Similarly, Mozilla has noted that

122 See, e.g., Federal Financial Institutions Examination Council ("FFIEC"), *Information Society IT Examination Handbook* (July 2006), available at <http://ithandbook.ffiec.gov/it-booklets/information-security.aspx>; Letter from Richard Spillenkothen, Dir., Div. of Banking Supervision & Regulation, Bd. of Governors of the Fed. Reserve Sys., *SRO1-11: Identity Theft and Pretext Calling* (Apr. 26, 2011), available at <http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm> (guidance on pretexting and identity theft); Securities & Exchange Commission, *CF Disclosure Guidance: Topic No. 2, on Cybersecurity* (Oct. 13, 2011), available at <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>; U.S. Small Business Administration, Information Security Guidance, <http://www.sba.gov/content/information-security>; National Institute of Standards & Technology, Computer Security Division, *Computer Security Resource Center*, available at <http://csrc.nist.gov/groups/SMA/sbc/index.html>; HHS, Health Information Privacy, available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html> (guidance and educational materials for entities required to comply with the HIPAA Privacy and Security Rules); Centers for Medicare and Medicaid Services, *Educational Materials*, available at <http://www.cms.gov/EducationMaterials/> (educational materials for HIPAA compliance).

123 FTC, OnGuard Online, <http://onguardonline.gov/>.

124 See FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), available at <http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business>; see generally FTC, Bureau of Consumer Protection Business Center, Data Security Guidance, available at <http://business.ftc.gov/privacy-and-security/data-security>.

125 See PCI Security Standards Council, *PCI SSC Data Security Standards Overview*, available at https://www.pcisecuritystandards.org/security_standards/; SANS Institute, *Information Security Policy Templates*, available at <http://www.sans.org/security-resources/policies/>; BITS, *Financial Services Roundtable BITS Publications*, available at <http://www.bits.org/publications/index.php>; see also, e.g., Better Business Bureau, *Security and Privacy – Made Simpler: Manageable Guidelines to help You Protect Your Customers' Security & Privacy from Identity Theft & Fraud*, available at <http://www.bbb.org/us/storage/16/documents/SecurityPrivacyMadeSimpler.pdf>; National Cyber Security Alliance, *For Business*, <http://www.staysafeonline.org/for-business> (guidance for small and midsize businesses); Direct Marketing Association, *Information Security: Safeguarding Personal Data in Your Care* (May 2005), available at <http://www.the-dma.org/privacy/InfoSecData.pdf>; Messaging Anti-Abuse Working Group & Anti-Phishing Working Group, *Anti-Phishing Best Practices for ISPs and Mailbox Providers* (July 2006), available at <http://www.antiphishing.org/reports/bestpracticesforisps.pdf>.

126 *Comment of Google Inc.*, cmt. #00417, at 2-3.

its cloud storage system encrypts user data using SSL communication.¹²⁷ Likewise, Twitter has implemented encryption by default for users logged into its system.¹²⁸ The Commission commends these efforts and calls on companies to continue to look for additional ways to build data security into products and services from the design stage.

Finally, the Commission reiterates its call for Congress to enact data security and breach notification legislation. To help deter violations, such legislation should authorize the Commission to seek civil penalties.

c. Reasonable Collection Limitation: Companies Should Limit Their Collection of Data.

The preliminary staff report called on companies to collect only the data they need to accomplish a specific business purpose. Many commenters expressed support for the general principle that companies should limit the information they collect from consumers.¹²⁹ Despite the broad support for the concept, however, many companies argued for a flexible approach based on concerns that allowing companies to collect data only for existing business needs would harm innovation and deny consumers new products and services.¹³⁰ One commenter cited Netflix's video recommendation feature as an example of how secondary uses of data can create consumer benefits. The commenter noted that Netflix originally collected information about subscribers' movie preferences in order to send the specific videos requested, but later used this information as the foundation for generating personalized recommendations to its subscribers.¹³¹

In addition, commenters raised concerns about who decides what a "specific business purpose" is.¹³² For example, one purpose for collecting data is to sell it to third parties in order to monetize a service and provide it to consumers for free. Would collecting data for this purpose be a specific business purpose? If not, is the only alternative to charge consumers for the service, and would this result be better for consumers?

As an alternative to limiting collection to accomplish a "specific business purpose," many commenters advocated limiting collection to business purposes *that are clearly articulated*. This is akin to the Fair Information Practice Principle of "purpose specification," which holds that companies should specify to consumers all of the purposes for which information is collected at the time of collection. One commenter supported purpose specification statements in general categories to allow innovation and avoid making privacy policies overly complex.¹³³

¹²⁷ *Comment of Mozilla*, cmt. #00480, at 7.

¹²⁸ See Chloe Albanesius, *Twitter Adds Always-On Encryption*, PC MAGAZINE, Feb. 12, 2012, <http://www.pcmag.com/article2/0,2817,2400252,00.asp>.

¹²⁹ See, e.g., *Comment of Intel Corp.*, cmt. #00246, at 4-5, 7, 40-41; *Comment of Electronic Frontier Foundation*, cmt. #00400, at 4-6; *Comment of Center for Democracy & Technology*, cmt. #00469, at 4-5; *Comment of Electronic Privacy Information Center*, cmt. #00386, at 18.

¹³⁰ See, e.g., *Comment of Facebook, Inc.*, cmt. #00413, at 2, 7-8, 18; *Comment of Google Inc.*, cmt. #00417, at 4; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 14-15; *Comment of Intuit, Inc.*, cmt. #00348, at 5, 9; *Comment of TRUSTe*, cmt. #00450, at 9.

¹³¹ *Comment of Facebook, Inc.*, cmt. #00413, at 7-8.

¹³² See *Comment of SAS*, cmt. #00415, at 51; *Comment of Yahoo! Inc.*, cmt. #00444, at 5.

¹³³ *Comment of Yahoo! Inc.*, cmt. #00444, at 5.

The Commission recognizes the need for flexibility to permit innovative new uses of data that benefit consumers. At the same time, in order to protect consumer privacy, there must be some reasonable limit on the collection of consumer data. General statements in privacy policies, however, are not an appropriate tool to ensure such a limit because companies have an incentive to make vague promises that would permit them to do virtually anything with consumer data.

Accordingly, the Commission clarifies the collection limitation principle of the framework as follows: Companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law.¹³⁴ For any data collection that is inconsistent with these contexts, companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner – outside of a privacy policy or other legal document. This clarification of the collection limitation principle is intended to help companies assess whether their data collection is consistent with what a consumer might expect; if it is not, they should provide prominent notice and choice. (For a further discussion of this point, see *infra* Section IV.C.2.) This approach is consistent with the Administration's Consumer Privacy Bill of Rights, which includes a Respect for Context principle that limits the use of consumer data to those purposes consistent with the context in which consumers originally disclosed the data.¹³⁵

One example of a company innovating around the concept of privacy by design through collection limitation is the Graduate Management Admission Council ("GMAC"). This entity previously collected fingerprints from individuals taking the Graduate Management Admission Test. After concerns were raised about individuals' fingerprints being cross-referenced against criminal databases, GMAC developed a system that allowed for collection of palm prints that could be used solely for test-taking purposes.¹³⁶ The palm print technology is as accurate as fingerprinting but less susceptible to "function creep" over time than the taking of fingerprints, because palm prints are not widely used as a common identifier. GMAC received a privacy innovation award for small businesses for its work in this area.

d. Sound Data Retention: Companies Should Implement Reasonable Data Retention and Disposal Policies.

Similar to the concerns raised about collection limits, many commenters expressed concern about limiting retention of consumer data, asserting that such limits would harm innovation. Trade associations and businesses requested a flexible standard for data retention to allow companies to develop new products

¹³⁴ This approach mirrors the revised standard for determining whether a particular data practice warrants consumer choice (see *infra* at section IV.C.1.a.) and is consistent with a number of commenters' calls for considering the context in which a particular practice takes place. See, e.g., *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-4; *Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 5; *Comment of TRUSTe*, cmt. #00450, at 3.

¹³⁵ See White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 15-19, (Feb. 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>. For a further discussion of this point, see *infra* at Section IV.C.1.a.

¹³⁶ See Jay Cline, *GMAC: Navigating EU Approval for Advanced Biometrics*, INSIDE PRIVACY BLOG (Oct. 15, 2010), https://www.privacyassociation.org/publications/2010_10_20_gmac_navigating_eu_approval_for_advanced_biometrics (explaining GMAC's adoption of palm print technology); cf. Kashmir Hill, *Why 'Privacy by Design' is the New Corporate Hotness*, FORBES, July 28, 2011, available at <http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/>.

and other uses of data that provide benefits to consumers.¹³⁷ One company raised concerns about prescriptive retention periods, arguing that retention standards instead should be based on business need, the type and location of data at issue, operational issues, and legal requirements.¹³⁸ Other commenters noted that retention limits should be sufficiently flexible to accommodate requests from law enforcement or other legitimate business purposes, such as the need of a mortgage banker to retain information about a consumer's payment history.¹³⁹ Some commenters suggested that the Commission's focus should be on data security and proper handling of consumer data, rather than on retention limits.¹⁴⁰

In contrast, some consumer groups advocated specific retention periods. For example, one such commenter cited a proposal made by a consortium of consumer groups in 2009 that companies that collect data for online behavioral advertising should limit their retention of the data to three months and that companies that retained their online behavioral advertising data for only 24 hours may not need to obtain consumer consent for their data collection and use.¹⁴¹ Others stated that it might be appropriate for the FTC to recommend industry-specific retention periods after a public consultation.¹⁴²

The Commission confirms its conclusion that companies should implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected.¹⁴³ Retention periods, however, can be flexible and scaled according to the type of relationship and use of the data; for example, there may be legitimate reasons for certain companies that have a direct relationship with customers to retain some data for an extended period of time. A mortgage company will maintain data for the life of the mortgage to ensure accurate payment tracking; an auto dealer will retain data from its customers for years to manage service records and inform its customers of new offers. These long retention periods help maintain productive customer relationships. This analysis does not, however, apply to all data collection scenarios. A number of commenters noted that online behavioral advertising data often becomes stale quickly and need not be retained long.¹⁴⁴ For example, a consumer researching hotels in a particular city for an upcoming vacation is unlikely to be interested in continuing to see hotel advertisements after the trip is completed. Indefinite retention of data about the consumer's interest in finding a hotel for a particular weekend serves little purpose and could result in marketers sending the consumer irrelevant advertising.

137 See *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-4, 14; *Comment of American Catalog Mailers Ass'n*, cmt. #000424, at 5; *Comment of IBM*, cmt. #00433, at 4; *Comment of Intuit, Inc.*, cmt. #00348, at 9.

138 *Comment of Verizon*, cmt. #00428, at 10-11.

139 See, e.g., *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 14.

140 *Comment of Yahoo! Inc.*, cmt. #00444, at 6; see also *Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 3-4.

141 *Comment of Consumer Federation of America*, cmt. #00358, at 4 (citing *Legislative Primer: Online Behavioral Tracking and Targeting Concerns and Solutions from the Perspective of the Center for Digital Democracy and U.S. PIRG, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research group, The World Privacy Forum* (Sept. 2009), available at <http://www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf>).

142 *Comment of Center for Democracy & Technology*, cmt. #00469, at 6 ("Flexible approaches to data retention should not, however, give *carte blanche* to companies to maintain consumer data after it has outlived its reasonable usefulness.").

143 In the alternative, companies may consider taking steps to de-identify the data they maintain, as discussed above.

144 See *Comment of Consumers Union*, cmt. #00362, at 8.

In determining when to dispose of data, as well as limitations on collection described above, companies should also take into account the nature of the data they collect. For example, consider a company that develops an online interactive game as part of a marketing campaign directed to teens. The company should first assess whether it needs to collect the teens' data as part of the game, and if so, how it could limit the data collected, such as by allowing teens to create their own username instead of using a real name and email address. If the company decides to collect the data, it should consider disposing of it even more quickly than it would if it collected adults' data. Similarly, recognizing the sensitivity of data such as a particular consumer's real time location, companies should take special care to delete this data as soon as possible, consistent with the services they provide to consumers.

Although restrictions may be tailored to the nature of the company's business and the data at issue, companies should develop clear standards and train its employees to follow them. Trade associations and self-regulatory groups also should be more proactive in providing guidance to their members about retention and data destruction policies. Accordingly, the Commission calls on industry groups from all sectors – the online advertising industry, online publishers, mobile participants, social networks, data brokers and others – to do more to provide guidance in this area. Similarly, the Commission generally supports the exploration of efforts to develop additional mechanisms, such as the “eraser button” for social media discussed below,¹⁴⁵ to allow consumers to manage and, where appropriate, require companies to delete the information consumers have submitted.

e. Accuracy: Companies should maintain reasonable accuracy of consumers' data.

The preliminary staff report called on companies to take reasonable steps to ensure the accuracy of the data they collect and maintain, particularly if such data could cause significant harm or be used to deny consumers services. Similar to concerns raised about collection limits and retention periods, commenters opposed rigid accuracy standards,¹⁴⁶ and noted that the FCRA already imposes accuracy standards in certain contexts.¹⁴⁷ One commenter highlighted the challenges of providing the same levels of accuracy for non-identifiable data versus data that is identifiable.¹⁴⁸

To address these challenges, some commenters stated that a sliding scale approach should be followed, particularly for marketing data. These commenters stated that marketing data is not used for eligibility purposes and that, if inaccurate, the only harm a consumer may experience is an irrelevant advertisement.¹⁴⁹ Providing enhanced accuracy standards for marketing data would raise additional privacy and data security concerns,¹⁵⁰ as additional information may need to be added to marketing databases to increase accuracy.¹⁵¹

¹⁴⁵ See *infra* at Section IV.D.2.b.

¹⁴⁶ See *Comment of Experian*, cmt. #00398, at 2.

¹⁴⁷ See *Comment of SIFMA*, cmt. #00265, at 4.

¹⁴⁸ *Comment of Phorm Inc.*, cmt. #00353, at 4.

¹⁴⁹ *Comment of Experian*, cmt. #00398, at 11 (arguing against enhanced standards for accuracy, access, and correction for marketing data); see also *Comment of Yahoo! Inc.*, cmt. #00444, at 6-7.

¹⁵⁰ *Id.*

¹⁵¹ Cf. *Comment of Yahoo! Inc.*, cmt. #00444, at 7 (arguing that it would be costly, time consuming, and contrary to privacy objectives to verify the accuracy of user registration information such as gender, age or hometown).

The Commission agrees that the best approach to improving the accuracy of the consumer data companies collect and maintain is a flexible one, scaled to the intended use and sensitivity of the information. Thus, for example, companies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain. Companies using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy, including allowing consumers access to the data and the opportunity to correct erroneous information.¹⁵²

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

2. COMPANIES SHOULD ADOPT PROCEDURAL PROTECTIONS TO IMPLEMENT THE SUBSTANTIVE PRINCIPLES.

Proposed Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

In addition to the substantive principles articulated above, the preliminary staff report called for organizations to maintain comprehensive data management procedures, such as designating personnel responsible for employee privacy training and regularly assessing the privacy impact of specific practices, products, and services. Many commenters supported this call for accountability within an organization.¹⁵³ Commenters noted that privacy risk assessments promote accountability, and help identify and address privacy issues.¹⁵⁴ One commenter stated that privacy risk assessments should be an ongoing process, and findings should be used to update internal procedures.¹⁵⁵ The Commission agrees that companies should implement accountability mechanisms and conduct regular privacy risk assessments to ensure that privacy issues are addressed throughout an organization.

The preliminary staff report also called on companies to “consider privacy issues systemically, at all stages of the design and development of their products and services.” A range of commenters supported the principle of “baking” privacy into the product development process.¹⁵⁶ One commenter stated that this approach of including privacy considerations in the product development process was preferable to requiring

¹⁵² See *infra* at Section IV.D.2. The Commission notes that some privacy-enhancing technologies operate by introducing deliberate “noise” into data. The data accuracy principle is not intended to rule out the appropriate use of these methods, provided that the entity using them notifies any recipients of the data that it is inaccurate.

¹⁵³ See, e.g., *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 2-3; *Comment of Intel Corp.*, cmt. #00246, at 6; *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 3.

¹⁵⁴ *Comment of GS1*, cmt. #00439, at 3; *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 6.

¹⁵⁵ *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 7.

¹⁵⁶ *Comment of Intel Corp.*, cmt. #00246, at 6; *Comment of United States Council for International Business*, cmt. #00366, at 2; *Comment of Consumer Federation of America*, cmt. #00358, at 3.

after-the-fact reviews.¹⁵⁷ Another argued that privacy concerns should be considered from the outset, but observed that such concerns should continue to be evaluated as the product, service, or feature evolves.¹⁵⁸

The Commission's recent settlements with Google and Facebook illustrate how the procedural protections discussed above might work in practice.¹⁵⁹ In both cases, the Commission alleged that the companies deceived consumers about the level of privacy afforded to their data.

The FTC's orders will require the companies to implement a comprehensive privacy program reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of "covered information," defined broadly to mean *any* information the companies collect from or about a consumer.

The privacy programs that the orders mandate must, at a minimum, contain certain controls and procedures, including: (1) the designation of personnel responsible for the privacy program; (2) a risk assessment that, at a minimum, addresses employee training and management and product design and development; (3) the implementation of controls designed to address the risks identified; (4) appropriate oversight of service providers; and (5) evaluation and adjustment of the privacy program in light of regular testing and monitoring.¹⁶⁰ Companies should view the comprehensive privacy programs mandated by these consent orders as a roadmap as they implement privacy by design in their own organizations.

As an additional means of implementing the substantive privacy by design protections, the preliminary staff report advocated the use of privacy-enhancing technologies ("PETs") – such as encryption and anonymization tools – and requested comment on implementation of such technologies. One commenter stressed the need for "privacy-aware design," calling for techniques such as obfuscation and cryptography to reduce the amount of identifiable consumer data collected and used for various products and services.¹⁶¹ Another stressed that PETs are a better approach in this area than rigid technical mandates.¹⁶²

The Commission agrees that a flexible, technology-neutral approach towards developing PETs is appropriate to accommodate the rapid changes in the marketplace and will also allow companies to innovate on PETs. Accordingly, the Commission calls on companies to continue to look for new ways to protect consumer privacy throughout the life cycle of their products and services, including through the development and deployment of PETs.

Finally, Commission staff requested comment on how to apply the substantive protections articulated above to companies with legacy data systems. Many commenters supported a phase-out period for legacy data systems, giving priority to systems that contain sensitive data.¹⁶³ Another commenter suggested that

¹⁵⁷ *Comment of Intel Corp.*, cmt. #00246, at 6.

¹⁵⁸ *Comment of Zynga Inc.*, cmt. #00459, at 2.

¹⁵⁹ Of course, the privacy programs required by these orders may not be appropriate for all types and sizes of companies that collect and use consumer data.

¹⁶⁰ *In the Matter of Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* <http://www.ftc.gov/os/caselist/index.shtm>.

¹⁶¹ *Comment of Electronic Frontier Foundation*, cmt. #00400, at 5.

¹⁶² *Comment of Business Software Alliance*, cmt. #00389, at 7-9.

¹⁶³ *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 3; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 2; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 14.

imposing strict access controls on legacy data systems until they can be updated would enhance privacy.¹⁶⁴ Although companies need to apply the various substantive privacy by design elements to their legacy data systems, the Commission recognizes that companies need a reasonable transition period to update their systems. In applying the substantive elements to their legacy systems, companies should prioritize those systems that contain sensitive data and they should appropriately limit access to all such systems until they can update them.

Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

¹⁶⁴ *Comment of Yahoo! Inc.*, cmt. #00444, at 7.

DATA COLLECTION AND DISPOSAL CASE STUDY: MOBILE

The rapid growth of the mobile marketplace illustrates the need for companies to implement reasonable limits on the collection, transfer, and use of consumer data and to set policies for disposing of collected data. The unique features of a mobile phone – which is highly personal, almost always on, and travels with the consumer – have facilitated unprecedented levels of data collection. Recent news reports have confirmed the extent of this ubiquitous data collection. Researchers announced, for example, that Apple had been collecting geolocation data through its mobile devices over time, and storing unencrypted data files containing this information on consumers' computers and mobile devices.¹ The Wall Street Journal has documented numerous companies gaining access to detailed information – such as age, gender, precise location, and the unique ID associated with a particular mobile device – that can then be used to track and predict consumer behavior.² Not surprisingly, consumers are concerned: for example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.³ The Commission calls on companies to limit collection to data they need for a requested service or transaction. For example, a wallpaper app or an app that tracks stock quotes does not need to collect location information.⁴

The extensive collection of consumer information – particularly location information – through mobile devices also heightens the need for companies to implement reasonable policies for purging data.⁵ Without data retention and disposal policies specifically tied to the stated business purpose for the data collection, location information could be used to build detailed profiles of consumer movements over time that could be used in ways not anticipated by consumers.⁶ Location information is particularly useful for uniquely identifying (or re-identifying) individuals using disparate bits of data.⁷ For example, a consumer can use a mobile application on her cell phone to “check in” at a restaurant for the purpose of finding and connecting with friends who are nearby. The same consumer might not expect the application provider to retain a history of restaurants she visited over time. If the application provider were to share that information with third parties, it could reveal a predictive pattern of the consumer's movements thereby exposing the consumer to a risk of harm such as stalking.⁸ Taken together, the principles of reasonable collection limitation and disposal periods help to minimize the risks that information collected from or about consumers could be used in harmful or unexpected ways.

With respect to the particular concerns of location data in the mobile context, the Commission calls on entities involved in the mobile ecosystem to work together to establish standards that address data collection, transfer, use, and disposal, particularly for location data. To the extent that location data in particular is collected and shared with third parties, entities should work to provide consumers with more prominent notice and choices about such practices. Although some in the mobile ecosystem provide notice about the collection of geolocation data, not all companies have adequately disclosed the frequency or extent of the collection, transfer, and use of such data.

NOTES

- 1 See Jennifer Valentino-Devries, *Study: iPhone Keeps Tracking Data*, WALL ST. J., Apr. 21, 2011, *available at* <http://online.wsj.com/article/SB10001424052748704570704576275323811369758.html>.
- 2 See, e.g., Robert Lee Hotz, *The Really Smart Phone*, WALL ST. J., Apr. 22, 2011, *available at* <http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html> (describing how researchers are using mobile data to predict consumers' actions); Scott Thurm & Yukari Iwatane Kane, *Your Apps are Watching You*, WALL ST. J., Dec. 18, 2010, *available at* <http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html> (documenting the data collection that occurs through many popular smartphone apps).
- 3 *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location*, NIELSEN WIRE BLOG (Apr. 21, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/; see also Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* 7 (Mar. 2011), *available at* <http://aa-download.avg.com/filedir/other/Smartphone.pdf> (reporting that 64% of consumers worry about their location being tracked when using their smartphones).
- 4 Similarly, the photo-sharing app Path faced widespread criticism for uploading its users' iPhone address books without their consent. See, e.g., Mark Hachman, *Path Uploads Your Entire iPhone Contact List By Default*, PC MAGAZINE, Feb. 7, 2012, *available at* <http://www.pcmag.com/article2/0,2817,2399970,00.asp>.
- 5 The Commission is currently reviewing its COPPA Rule, including the application of COPPA to geolocation information. See FTC, Proposed Rule and Request for Public Comment, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (Sept. 15, 2011), *available at* <http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf>.
- 6 See ACLU of Northern California, *Location-Based Services: Time for a Privacy Check-In*, 14-15 (Nov. 2010), *available at* <http://dotrights.org/sites/default/files/lbs-white-paper.pdf>.
- 7 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 3.
- 8 Cf. *U.S. v. Jones*, 565 U.S. 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (noting that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

C. SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

As detailed in the preliminary staff report and in submitted comments, many consumers face challenges in understanding the nature and extent of current commercial data practices and how to exercise available choices regarding those practices. This challenge results from a number of factors including: (1) the dramatic increase in the breadth of consumer data collection and use, made possible by an ever-increasing range of technologies and business models; (2) the ability of companies, outside of certain sector-specific laws, to collect and use data without first providing consumer choice; and (3) the inadequacy of typical privacy policies as a means to effectively communicate information about the privacy choices that are offered to consumers.

To reduce the burden on those consumers who seek greater control over their data, the proposed framework called on companies that collect and use consumer data to provide easy-to-use choice mechanisms that allow consumers to control whether their data is collected and how it is used. To ensure that choice is most effective, the report stated that a company should provide the choice mechanism at a time and in a context that is relevant to consumers – generally at the point the company collects the consumer’s information. At the same time, however, in recognition of the benefits of various types of data collection and use, the proposed framework identified certain “commonly accepted” categories of commercial data practices that companies can engage in without offering consumer choice.

Staff posed a variety of questions and received numerous comments regarding the proposed framework’s simplified consumer choice approach. Two trade organizations argued that the framework should identify those practices for which choice is appropriate rather than making choice the general rule, subject to exceptions for certain practices.¹⁶⁵ The majority of commenters, however, did not challenge the proposed framework’s approach of setting consumer choice as the default.¹⁶⁶ Instead, these commenters focused on the practicality of staff’s “commonly accepted” formulation.¹⁶⁷ For example, several commenters questioned whether the approach was sufficiently flexible to allow for innovation.¹⁶⁸ Others discussed whether specific practices should fall within the categories enumerated in the preliminary staff report.¹⁶⁹ In addition, numerous commenters addressed the appropriate scope of the first-party marketing category and how to

¹⁶⁵ *Comment of Direct Marketing Ass’n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8-9.

¹⁶⁶ Several commenters expressed support for consumer choice generally. *See, e.g., Comment of Center for Democracy & Technology*, cmt. #00469, at 11-12; *Comment of Consumer Federation of America*, cmt. #00358, at 6-12. One governmental agency, for instance, expressly supported a general rule requiring consumer consent for the collection and any use of their information with only limited exceptions. *Comment of Department of Veteran Affairs*, cmt. #00479, at 5. Another commenter, supporting consumer choice, emphasized the importance of offering opportunities for choice beyond a consumer’s initial transaction. *Comment of Catalog Choice*, cmt. #00473, at 10-18.

¹⁶⁷ *Comment of Center for Democracy & Technology*, cmt. #00469, at 8-11; *Comment of Consumer Federation of America*, cmt. #00358, at 6-10.

¹⁶⁸ *Comment of Computer and Communications Industry Ass’n*, cmt. #00434, at 16; *Comment of BlueKai*, cmt. #00397, at 3-4; *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 5-7; *U.S. Chamber of Commerce*, cmt. #00452, at 5; *Comment of National Cable & Telecommunications Ass’n*, cmt. #00432, at 23-24; *Comment of Yahoo! Inc.*, cmt. #00444, at 9-10.

¹⁶⁹ *Comment of Phorm Inc.*, cmt. #00353, at 5; *Comment of Verizon*, cmt. #00428, at 11-13.

define specific business models. With respect to those practices that fall outside the “commonly accepted” categories, commenters also addressed the mechanics of providing choice at the relevant time and what types of practices require enhanced choice.

Consistent with the discussion and analysis set forth below, the Commission retains the proposed framework’s simplified choice model. Establishing consumer choice as a baseline requirement for companies that collect and use consumer data, while also identifying certain practices where choice is unnecessary, is an appropriately balanced model. It increases consumers’ control over the collection and use of their data, preserves the ability of companies to innovate new products and services, and sets clear expectations for consumers and industry alike. In order to better foster innovation and take into account new technologies and business models, however, the Commission is providing further clarification of the framework’s simplified choice concept.

1. PRACTICES THAT DO NOT REQUIRE CHOICE.

Proposed Principle: Companies do not need to provide choice before collecting and using consumers’ data for commonly accepted practices, such as product fulfillment.

The preliminary staff report identified five categories of data practices that companies can engage in without offering consumer choice, because they involve data collection and use that is either obvious from the context of the transaction or sufficiently accepted or necessary for public policy reasons. The categories included: (1) product and service fulfillment; (2) internal operations; (3) fraud prevention; (4) legal compliance and public purpose; and (5) first-party marketing. In response to the comments received, the Commission revises its approach to focus on the context of the consumer’s interaction with a company, as discussed below.

a. General Approach to “Commonly Accepted” Practices.

While generally supporting the concept that choice is unnecessary for certain practices, a variety of commenters addressed the issue of whether the list of “commonly accepted” practices was too broad or too narrow.¹⁷⁰ A number of industry commenters expressed concern that the list of practice categories was too narrow and rigid. These commenters stated that, by enumerating a list of specific practices, the proposed framework created a bright-line standard that freezes in place current practices and potentially could harm innovation and restrict the development of new business models.¹⁷¹ In addition, the commenters asserted that notions of what is “commonly accepted” can change over time with the development of new ways to collect or use data. They also stated that line-drawing in this context could stigmatize business practices that fall outside of the “commonly accepted” category and place companies that engage in them at a competitive

¹⁷⁰ *Comment of AT&T Inc.*, cmt. #00420, at 18-22; *Comment of Center for Democracy & Technology*, cmt. #00469, at 8-11; *Comment of Consumers Union*, cmt. #00362, at 9-12; *Comment of Consumer Federation of America*, cmt. #00358, at 6-10; *Comment of National Cable & Telecommunications Ass’n*, cmt. #00432, at 23-25.

¹⁷¹ *Comment of Computer and Communications Industry Ass’n*, cmt. #00434, at 16; *Comment of BlueKai*, cmt. #00397, at 4; *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 6-7; *Comment of Yahoo! Inc.*, cmt. #00444, at 9-12; *Comment of National Cable & Telecommunications Ass’n*, cmt. #00432, at 23-24.

disadvantage. To resolve these concerns, commenters called on the Commission to provide guidance on how future practices relate to the “commonly accepted” category.¹⁷² Similarly, one commenter suggested that the practices identified in the preliminary staff report should serve as illustrative guidelines rather than an exhaustive and final list.¹⁷³

Commenters also supported adding additional practices or clarifying that the “commonly accepted” category includes certain practices. Some industry commenters suggested, for example, expanding the concept of fraud prevention to include preventing security attacks, “phishing,”¹⁷⁴ and spamming or to protect intellectual property.¹⁷⁵ Other recommendations included adding analytical data derived from devices that are not tied to individuals, such as smart grid data used for energy conservation and geospatial data used for mapping, surveying or providing emergency services.¹⁷⁶ With respect to online behavioral advertising in particular, some trade associations recommended clarifying that the “commonly accepted” category of practices includes the use of IP addresses and third-party cookie data when used for purposes such as “frequency capping,” “attribution measurement,” and similar inventory or delivery measurements and to prevent click fraud.¹⁷⁷

More generally, some commenters discussed the “repurposing” of existing consumer data to develop new products or services. For example, one company supported expanding the “internal operations” category to include the practice of product and service improvement.¹⁷⁸ One commenter recommended treating any uses of data that consumers would “reasonably expect under the circumstances” as commonly accepted.¹⁷⁹ Another noted that, whether a new use of consumer data should be considered commonly accepted would depend upon a variety of factors, including the extent to which the new use is consistent with previously defined uses.¹⁸⁰

In contrast to the calls for expanding the “commonly accepted” practice categories to cover various practices, a number of consumer and privacy organizations advocated for a more restrictive approach to determining the practices that do not require consumer choice. Although agreeing that choice is not necessary for product and service fulfillment, one commenter stated that most of the other practices enumerated in the proposed framework – including internal operations, fraud prevention, and legal compliance and public purpose – were vague and required additional description. The commenter called on

172 *Comment of eBay*, cmt. #00374, at 6-7; *Comment of Phorm Inc.*, cmt. #00353, at 5.

173 *See Comment of AT&T Inc.*, cmt. #00420, at 18.

174 Phishing uses deceptive spam that appears to be coming from legitimate, well-known sources to trick consumers into divulging sensitive or personal information, such as credit card numbers, other financial data, or passwords.

175 *See Comment of Microsoft Corp.*, cmt. #00395, at 8 (security attacks, phishing schemes, and spamming); *Comment of Business Software Alliance*, cmt. #00389, at 5-6 (security access controls and user and employee authentication, cybercrime and fraud prevention and detection, protecting and enforcing intellectual property and trade secrets).

176 *See Comment of IBM*, cmt. #00433, at 5 (energy conservation); *Comment of Management Ass’n for Private Programming Surveyors*, cmt. #00205, at 2-3 (mapping, surveying or providing emergency services).

177 *See Comment of Online Publishers Ass’n*, cmt. #00315, at 5 (frequency capping, click fraud); *Comment of Interactive Advertising Bureau*, cmt. #00388, at 9 (attribution measurement).

178 *See Comment of AT&T Inc.*, cmt. #00420, at 18-19.

179 *See Comment of Microsoft Corp.*, cmt. #00395, at 8.

180 *See Comment of Future of Privacy Forum*, cmt. #00341, at 5.

the Commission to define these terms as narrowly as possible so that they would not become loopholes used to undermine consumer privacy.¹⁸¹

One privacy advocate expressed reservations about the breadth of the “internal operations” category of practices – specifically, the extent to which it could include product improvement and website analytics. This commenter stated that, if viewed broadly, product improvement could justify, for example, a mobile mapping application collecting precise, daily geolocation data about its customers and then retaining the data long after providing the service for which the data was necessary. Similarly, this commenter noted that companies potentially could use analytics programs to create very detailed consumer profiles to which many consumers might object, without offering them any choice. This commenter recommended that the Commission revise the proposed framework’s internal operations category to make it consistent with the “operational purpose” language contained in H.R. 611 from the 112th Congress, which would include, among other things, “basic business functions such as accounting, inventory and supply chain management, quality assurance, and internal auditing.”¹⁸²

The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary. However, the Commission also appreciates the concerns that the preliminary staff report’s definition of “commonly accepted practices” may have been both under-inclusive and over-inclusive. To the extent the proposed framework was interpreted to establish an inflexible list of specific practices, it risked undermining companies’ incentives to innovate and develop new products and services to consumers, including innovative methods for reducing data collection while providing valued services. On the other hand, companies could read the definition so broadly that virtually any practice could be considered “commonly accepted.”

The standard should be sufficiently flexible to allow for innovation and new business models but also should cabin the types of practices that do not require consumer choice. To strike that balance, the Commission refines the standard to focus on the *context of the interaction* between a business and the consumer. This new “context of the interaction” standard is similar to the concept suggested by some commenters that the need for choice should depend on reasonable consumer expectations,¹⁸³ but is intended to provide businesses with more concrete guidance. Rather than relying solely upon the inherently subjective test of consumer expectations, the revised standard focuses on more objective factors related to the consumer’s relationship with a business. Specifically, whether a practice requires choice turns on the extent

181 See *Comment of Consumer Federation of America*, cmt. #00358, at 6.

182 See *Comment of Center for Democracy & Technology*, cmt. #00469, at 8-9 (citing BEST PRACTICES Act, H.R. 611, 112th Congress § 2(5)(iii) (2011)).

183 See *Comment of Microsoft Corp.*, cmt. #00395, at 8; *Comment of National Cable & Telecommunications Ass’n*, cmt. #00432, at 23-26; *Comment of Pharmaceutical Research & Manufacturers of America*, cmt. #00477, at 13.

to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law.¹⁸⁴

The purchase of an automobile from a dealership illustrates how this standard could apply. In connection with the sale of the car, the dealership collects personal information about the consumer and his purchase. Three months later, the dealership uses the consumer's address to send him a coupon for a free oil change. Similarly, two years after the purchase, the dealership might send the consumer notice of an upcoming sale on the type of tires that came with the car or information about the new models of the car. In this transaction the data collection and subsequent use is consistent with the context of the transaction and the consumer's relationship with the car dealership. Conversely, if the dealership sells the consumer's personal information to a third-party data broker that appends it to other data in a consumer profile to sell to marketers, the practice would not be consistent with the car purchase transaction or the consumer's relationship with the dealership.

Although the Commission has revised the standard for evaluating when choice is necessary, it continues to believe that the practices highlighted in the preliminary staff report – fulfilment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing¹⁸⁵ – provide illustrative guidance regarding the types of practices that would meet the revised standard and thus would not typically require consumer choice. Further, drawing upon the recommendations of several commenters,¹⁸⁶ the Commission agrees that the fraud prevention category would generally cover practices designed to prevent security attacks or phishing; internal operations would encompass frequency capping and similar advertising inventory metrics; and legal compliance and public purpose would cover intellectual property protection or using location data for emergency services.¹⁸⁷ It should be noted, however, that even within these categories there may be practices that are inconsistent with the context of the interaction standard and thus warrant consumer choice. For instance, there may be contexts in which the “repurposing” of data to improve existing products or services would exceed the internal operations concept. Thus, where a product improvement involves additional sharing of consumer data with third parties, it would no longer be an “internal operation” consistent with the context of the consumer's interaction with a company. On the

184 As noted above, focusing on the context of the interaction is consistent with the Respect for Context principle in the Consumer Privacy Bill of Rights proposed by the White House. See White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, App. A. (Feb. 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>. The Respect for Context principle requires companies to limit their use of consumer data to purposes that are consistent with the company's relationship with the consumer and with the context in which the consumer disclosed the data, unless the company is legally required to do otherwise. If a company will use data for other purposes it must provide a choice at a prominent point, outside of the privacy policy.

185 See *supra* at Section IV.C.1.

186 See *supra* note 175.

187 With respect to use of geolocation data for mapping, surveying or similar purposes, if the data cannot reasonably be linked to a specific consumer, computer, or device, a company collecting or using the data would not need to provide a consumer choice mechanism. Similarly, if a company takes reasonable measures to de-identify smart grid data and takes the other steps outlined above, the company would not be obligated to obtain consent before collecting or using the data. See *supra* Section IV.A.4.

other hand, product improvements such as a website redesign or a safety improvement would be the type of “internal operation” that is generally consistent with the context of the interaction.¹⁸⁸

b. First-Party Marketing Generally Does Not Require Choice, But Certain Practices Raise Special Concerns.

The preliminary staff report’s questions regarding first-party marketing generated a large number of comments. As discussed, the Commission has revised the standard for determining whether a practice requires consumer choice but believes that most first-party marketing practices are consistent with the consumer’s relationship with the business and thus do not necessitate consumer choice. Nevertheless, as a number of the commenters discussed, there are certain practices that raise special concerns and therefore merit additional analysis and clarification.

(i) Companies Must Provide Consumers With A Choice Whether To Be Tracked Across Other Parties’ Websites.

Commenters raised questions about companies and other services that have first-party relationships with consumers, but may have access to behavioral activity data that extends beyond the context of that first-party relationship. For example, in response to the question in the preliminary staff report regarding the use of deep packet inspection (“DPI”),¹⁸⁹ a number of commenters cited the ability of ISPs to use DPI to monitor and track consumers’ movements across the Internet and use the data for marketing.¹⁹⁰ There appeared to be general consensus among the commenters that, based on the potential scope of the tracking, an ISP’s use of DPI for marketing purposes is distinct from other forms of marketing practices by companies that have a first-party relationship with consumers, and thus at a minimum requires consumer choice.¹⁹¹

Similarly, commenters cited the use of “social plugins” – such as the Facebook “Like” button – that allow social media services to track consumers across every website that has installed the plugin.¹⁹² The commenter stated that, as with DPI, consumers would not expect social media sites to track their visits to other websites or that the profiles created from such tracking could be used for marketing.

188 Moreover, even if a given practice does not necessitate consumer choice, the framework’s other elements – *e.g.*, data collection limits and disposal requirements, increased transparency – would still apply, thereby preventing a company from exploiting these categories.

189 Deep packet inspection (“DPI”) refers to the ability of ISPs to analyze the information, comprised of data packets, that traverses their networks when consumers use their services.

190 See *Comment of AT&T Inc.*, cmt. #00420, at 21-22 & n.34; *Comment of Berlin Commissioner for Data Protection & Freedom of Information*, cmt. #00484, at 2-3; *Comment of Computer & Communications Industry Ass’n*, cmt. #00434, at 15; *Comment of Phorm Inc.*, cmt. #00353, App. A at 3-4; *Comment of U.S. Public Policy Council of the Ass’n for Computing Machinery*, cmt. #00431, at 6.

191 See *Comment of Phorm Inc.*, cmt. #00353, App. A at 3-4; *Comment of Center for Democracy & Technology*, cmt. #00469, at 14-15; *Comment of AT&T Inc.*, cmt. #00420, at 21-22 & n.34.

192 See *Comment of Consumer Federation of America*, cmt. #00358, at 8 (citing Justin Brookman, *Facebook Pressed to Tackle Lingering Privacy Concerns*, Center for Democracy & Technology (June 16, 2010), available at <https://www.cdt.org/blogs/justin-brookman/facebook-pressed-tackle-lingering-privacy-concerns/>); *Comment of Berkeley Center for Law & Technology*, cmt. #00347, at 8; see also Arnold Roosendaal, *Facebook Tracks and Traces Everyone: Like This!*, (Nov. 30, 2010), available at http://papers.ssrn.com/so13/papers.cfm?abstract_id=1717563 (detailing how Facebook tracks consumers through the Like button, including non-Facebook members and members who have logged out of their Facebook accounts); Nik Cubrilovic, *Logging Out Of Facebook Is Not Enough*, NEW WEB ORDER (Sept. 25, 2011), <http://nikcub.appspot.com/posts/logging-out-of-facebook-is-not-enough>.

The Commission agrees that where a company that has a first-party relationship with a consumer for delivery of a specific service but also tracks the consumer's activities across other parties' websites, such tracking is unlikely to be consistent with the context of the consumer's first-party relationship with the entity. Accordingly, under the final framework, such entities should not be exempt from having to provide consumers with choices. This is true whether the entity tracks consumers through the use of DPI, social plug-ins, http cookies, web beacons, or some other type of technology.¹⁹³

As an example of how this standard can apply, consider a company with multiple lines of business, including a search engine and an ad network. A consumer has a "first-party relationship" with the company when using the search engine. While it may be consistent with this first-party relationship for the company to offer contextual ads on the search engine site, it would be inconsistent with the first-party search engine relationship for the company to use its third-party ad network to invisibly track the consumer across the Internet.

To use another example, many online retailers engage in the practice of "retargeting," in which the retailer delivers an ad to a consumer on a separate website based on the consumer's previous activity on the retailer's website.¹⁹⁴ Because the ad is tailored to the consumer's activity on the retailer's website, it could be argued that "retargeting" is a first-party marketing practice that does not merit consumer choice. However, because it involves tracking the consumer from the retailer's website to a separate site on which the retailer is a third party and communicating with the consumer in this new context, the Commission believes that the practice of retargeting is inconsistent with the context of consumer's first-party interaction with the retailer. Thus, where an entity has a first-party relationship with a consumer on its own website, and it engages in third-party tracking of the consumer across other websites the entity should provide meaningful choice to the consumer.

(ii) Affiliates Are Third Parties Unless The Affiliate Relationship Is Clear to Consumers.

Several trade organizations stated that first-party marketing should include the practice of data sharing among all of a particular entity's corporate affiliates and subsidiaries.¹⁹⁵ In contrast, a number of commenters – including individual companies and consumer advocates – took a more limited approach that would treat affiliate sharing as a first-party practice only if the affiliated companies share a trademark, are commonly-branded, or the affiliated relationship is otherwise reasonably clear to consumers.¹⁹⁶ One consumer advocate also suggested restricting data sharing to commonly-branded affiliates in the same line of business so that the data would be used in a manner that is consistent with the purpose for which the first party collected it.¹⁹⁷

193 See *infra* at Section IV.C.2.d. (discussing special concerns that arise by comprehensive tracking by large platform providers).

194 For example, a consumer visits an online sporting goods retailer, looks at but does not purchase running shoes, and then visits a different website to read about the local weather forecast. A first party engages in retargeting if it delivers an ad for running shoes to the consumer on the third-party weather site.

195 See *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 24.

196 See *Comment of Yahoo! Inc.*, cmt. #00444, at 11; *Comment of IBM*, cmt. #00433, at 6; *Comment of AT&T Inc.*, cmt. #00420, at 20; *Comment of Catalog Choice*, cmt. #00473, at 10; *Comment of Consumers Union*, cmt. #00362, at 10-11.

197 See *Comment of Consumers Union*, cmt. #00362, at 10-11.

The Commission maintains the view that affiliates are third parties, and a consumer choice mechanism is necessary unless the affiliate relationship is clear to consumers. Common branding is one way of making the affiliate relationship clear to consumers. By contrast, where an affiliate relationship is hidden – such as between an online publisher that provides content to consumers through its website and an ad network that invisibly tracks consumers’ activities on the site – marketing from the affiliate would not be consistent with a transaction on, or the consumer’s relationship with, that website. In this scenario consumers should receive a choice about whether to allow the ad network to collect data about their activities on the publisher’s site.

(iii) Cross-Channel Marketing Is Generally Consistent with the Context of a Consumer’s Interaction with a Company.

A variety of commenters also discussed the issue of whether the framework should require choice for cross-channel marketing, *e.g.*, where a consumer makes an in-store purchase and receives a coupon – not at the register, but in the mail or through a text message. These commenters stated that the framework should not require choice when a first party markets to consumers through different channels, such as the Internet, email, mobile apps, texts, or in the offline context.¹⁹⁸ In support of this conclusion, one commenter stated that restricting communications from a first party to the initial means of contact would impose costs on business without any consumer benefits.¹⁹⁹

The Commission agrees that the first-party marketing concept should include the practice of contacting consumers across different channels. Regardless of the particular means of contact, receipt of a message from a company with which a consumer has interacted directly is likely to be consistent with the consumer’s relationship with that company.²⁰⁰ At the same time, as noted above, if an offline or online retailer tracks a customer’s activities on a third-party website, this is unlikely to be consistent with the customer’s relationship with the retailer; thus, choice should be required.

(iv) Companies Should Implement Measures to Improve The Transparency of Data Enhancement.

A large number of commenters discussed whether the practice of data enhancement, by which a company appends data obtained from third-party sources to information it collects directly from consumers, should require choice. Some of these commenters specifically objected to allowing companies to enhance data without providing consumers choice about the practice.²⁰¹

For example, one academic organization characterized data enhancement without consumer choice as “trick[ing]” consumers into participating in their own profiling for the benefit of companies.²⁰² As

198 See *Comment of Yahoo! Inc.*, cmt. #00444, at 10; *Comment of IBM*, cmt. #00433, at 6; *Comment of AT&T Inc.*, cmt. #00420, at 20; *Comment of Catalog Choice*, cmt. #00473, at 9-10; *Comment of Direct Marketing Ass’n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8.

199 See *Comment of American Catalog Mailers Ass’n*, cmt. #00424, at 7.

200 Such marketing communications would, of course, still be subject to any existing restrictions, including the CAN-SPAM Act, 15 U.S.C. §§ 7701-7713 (2010).

201 See *Comment of Consumer Federation of America*, cmt. #00358, at 10; *Comment of Consumers Union*, cmt. #00362, at 11.

202 *Comment of Berkeley Center for Law & Technology*, cmt. #00347, at 9-10.

companies develop new means for collecting data about individuals, this commenter stated, consumers should have more tools to control data collection, not fewer.²⁰³

Similarly, a consumer organization explained that consumers may not anticipate that the companies with which they have a relationship can obtain additional data about them from other sources, such as social networking sites, and use the data for marketing.²⁰⁴ This commenter concluded that requiring companies to provide choice will necessitate better explanations of the practice, which will lead to improved consumer understanding.

Other stakeholders also raised concerns about data enhancement absent consumer choice. One company focused on the practice of enhancing online cookie data or IP addresses with offline identity data and stated that such enhancement should be subject to consumer choice.²⁰⁵ In addition, a data protection authority stated that consumers are likely to expect choice where the outcome of data enhancement could negatively affect the consumer or where the sources of data used for enhancement would be unexpected to the consumer.²⁰⁶

Alternatively, a number of industry commenters opposed requiring consumer choice for data enhancement in connection with first-party marketing. These commenters described data enhancement as a routine and longstanding practice that allows businesses to better understand and serve their consumers.²⁰⁷ Commenters enumerated a variety of benefits from the availability and use of third-party data, including: development of new or more relevant products and services; ensuring the accuracy of databases; reducing barriers to small firms seeking to enter markets; helping marketers identify the best places to locate retail stores; and reducing irrelevant marketing communications.²⁰⁸

One commenter noted that requiring content publishers such as newspapers to offer consumer choice before buying information from non-consumer-facing data brokers would impose logistical and financial challenges that would interfere with publishers' ability to provide relevant content or sell the advertising to support it.²⁰⁹ Other commenters claimed that, where the data used for enhancement comes from third-party sources, it was likely subject to choice at the point of collection from the consumer and therefore providing additional choice is unnecessary.²¹⁰ Taking a similar approach, one company noted that the third-party source of the data should be responsible for complying with the framework when it shares data, and the recipient should be responsible for any subsequent sharing of the enhanced data.²¹¹

203 *Id.*, at 8-10 (describing Williams-Sonoma's collection of consumers' zip codes in *Pineda v. Williams-Sonoma Stores, Inc.*, 246 P.3d 612 (Cal. 2011)).

204 *Comment of Consumer Federation of America*, cmt. #00358, at 10.

205 *See Comment of Phorm Inc.*, cmt. #00353, at 5.

206 *See Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 3.

207 *See Comment of Newspaper Ass'n of America*, cmt. #00383, at 7-8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 24-26; *Comment of Experian*, cmt. #00398, at 5-6; *Comment of Magazine Publishers of America*, cmt. #00332, at 4; *Consumer Data Industry Ass'n*, cmt. #00363, at 2-3.

208 *Comment of Experian*, cmt. #00398, at 6; *see Comment of Newspaper Ass'n of America*, cmt. #00383, at 6-8.

209 *Comment of Newspaper Ass'n of America*, cmt. #00383, at 7-8.

210 *Comment of Experian*, cmt. #00398, at 9 (citing the Direct Marketing Association's Guidelines for Ethical Business Practice); *Comment of Magazine Publishers of America*, cmt. #00332, at 5-6.

211 *Comment of Microsoft Corp.*, cmt. #00395, at 8.

The issue of whether a first-party marketer should provide choice for data enhancement is particularly challenging because the practice involves two separate and distinct types of consumer data collection. One involves the consumer-to-business transfer of data – for instance, where an online retailer collects information directly from the consumer by tracking the products the consumer purchased in the store or looked at while visiting the retailer’s website. The other involves a business-to-business transfer of data – such as where retailer purchases consumer data from a non-consumer-facing data broker.

As to the first type of data collection, for the reasons discussed above, if the first party does not share information with third parties or track consumers across third-party websites, the practice would be consistent with the context of the consumer’s interaction with the company.²¹² Therefore, the framework would not call for a consumer choice mechanism. In contrast, because the second type of data collection involves the transfer of data from one business to another and does not directly involve the consumer (and therefore is typically unknown to the consumer), it is unlikely to be consistent with a transaction or relationship between the consumer and the first party. The Commission nevertheless recognizes that it would be impractical to require the first-party marketer to offer a choice mechanism when it appends data from third-party sources to the data it collects directly from its consumers. As discussed in the comments, such a requirement would impose costs and logistical problems that could preclude the range of benefits that data enhancement facilitates.

Instead, full implementation of the framework’s other components should address the privacy concerns that commenters raised about data enhancement. First, companies should incorporate privacy by design concepts, including limiting the amount of data they collect from consumers and third parties alike to accomplish a specific business purpose, reducing the amount of time they retain such data, and adopting reasonable security measures. The framework also calls for consumer choice where a company shares with a third party the data it collects from a consumer. Thus, consumers will have the ability to control the flow of their data to third parties who might sell the data to others for enhancement. In addition, companies should improve the transparency of their practices by disclosing that they engage in data enhancement and educating consumers about the practice, identifying the third-party sources of the data, and providing a link or other contact information so the consumer can contact the third-party source directly. Finally, to further protect consumer privacy, the Commission recommends that first parties that obtain marketing data for enhancement should take steps to encourage their third-party data broker sources to increase their own transparency, including by participating in a centralized data broker website, discussed further below, where consumers could learn more information about data brokers and exercise choices.²¹³ The first parties may also consider contractually requiring their data broker sources to take these steps.

212 See *supra* Section IV.C.1.b.(i).

213 The concept of such a website is discussed, *infra*, Section IV.D.2.a.

DATA ENHANCEMENT CASE STUDY: FACIAL RECOGNITION SOFTWARE

Facial recognition technology¹ enables the identification of an individual based on his or her distinct facial characteristics. While this technology has been used in experiments for over thirty years, until recently it remained costly and limited under real world conditions.² However, steady improvements in the technology combined with increased computing power have shifted this technology out of the realm of science fiction and into the marketplace. As costs have decreased and accuracy improved, facial recognition software has been incorporated into a variety of commercial products. Today it can be found in online social networks and photo management software, where it is used to facilitate photo-organizing,³ and in mobile apps where it is used to enhance gaming.⁴

This surge in the deployment of facial recognition technology will likely boost the desire of companies to use data enhancement by offering yet another means to compile and link information about an individual gathered through disparate transactions and contexts. For instance, social networks such as Facebook and LinkedIn, as well as websites like Yelp and Amazon, all encourage users to upload profile photos and make these photos publicly available. As a result, vast amounts of facial data, often linked with real names and geographic locations, have been made publicly available. A recent paper from researchers at Carnegie Mellon University illustrated how they were able to combine readily available facial recognition software with data mining algorithms and statistical re-identification techniques to determine in many cases an individual's name, location, interests, and even the first five digits of the individual's Social Security number, starting with only the individual's picture.⁵

Companies could easily replicate these results. Today, retailers use facial *detection* software in digital signs to analyze the age and gender of viewers and deliver targeted advertisements.⁶ Facial detection does not uniquely identify an individual. Instead, it detects human faces and determines gender and approximate age range. In the future, digital signs and kiosks placed in supermarkets, transit stations, and college campuses could capture images of viewers and, through the use of facial *recognition* software, match those faces to online identities, and return advertisements based on the websites specific individuals have visited or the publicly available information contained in their social media profiles. Retailers could also implement loyalty programs, ask users to associate a photo with the account, then use the combined data to link the consumer to other online accounts or their in-store actions. This would enable the retailer to glean information about the consumer's purchase habits, interests, and even movements,⁷ which could be used to offer discounts on particular products or otherwise market to the consumer.

The ability of facial recognition technology to identify consumers based solely on a photograph, create linkages between the offline and online world, and compile highly detailed dossiers of information, makes it especially important for companies using this technology to implement privacy by design concepts and robust choice and transparency policies. Such practices should include reducing the amount of time consumer information is retained, adopting reasonable security measures, and disclosing to consumers that the facial data they supply may be used to link them to information from third parties or publicly available sources. For example, if a digital sign uses data enhancement to deliver targeted advertisements to viewers, it should immediately delete the data after the consumer has walked away. Likewise, if a kiosk is used to invite shoppers to register for a store loyalty program, the shopper should be informed that the photo taken by the kiosk camera and associated with the account may be combined with other data to market discounts and offers to the shopper. If a company received the data from other sources, it should disclose the sources to the consumer.

NOTES

- 1 The Commission held a facial recognition workshop on December 8, 2011. See FTC Workshop, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), <http://www.ftc.gov/bcp/workshops/facefacts/>.
- 2 See Alessandro Acquisti *et al.*, *Faces of Facebook: Privacy in the Age of Augmented Reality*, <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/>.
- 3 See Justin Mitchell, *Making Photo Tagging Easier*, THE FACEBOOK BLOG (June 30, 2011, 5:16 PM), <https://blog.facebook.com/blog.php?post=467145887130>; Matt Hickey, *Picasa Refresh Brings Facial Recognition*, TECHCRUNCH (Sept. 2, 2008), <http://techcrunch.com/2008/09/02/picasa-refresh-brings-facial-recognition/>.
- 4 See Tomio Geron, *Viewdle Launches 'Third Eye' Augmented Reality Game*, FORBES, June 22, 2011, available at <http://www.forbes.com/sites/tomiogeron/2011/06/22/viewdle-launches-third-eye-augmented-reality-game/>.
- 5 See Alessandro Acquisti *et al.*, *Faces of Facebook: Privacy in the Age of Augmented Reality*, <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/>.
- 6 See Shan Li & David Sarno, *Advertisers Start Using Facial Recognition to Tailor Pitches*, L.A. TIMES, Aug. 21, 2011, available at <http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821>.
- 7 For instance, many consumers use services such as Foursquare which allow them to use their mobile phone to “check in” at a restaurant to find friends who are nearby. See Foursquare, About Foursquare, <https://foursquare.com/about>.

(v) Companies Should Generally Give Consumers a Choice Before Collecting Sensitive Data for First-Party Marketing.

Commenters addressed whether companies that collect sensitive data²¹⁴ for their own marketing should offer consumer choice. A number of privacy and consumer organizations asserted that even where a business collects data in a first-party setting, any marketing based on sensitive data should require the consumer's affirmative express consent.²¹⁵ These commenters stated that the use of sensitive data for marketing could cause embarrassment for consumers or lead to various types of discriminatory conduct, including denial of benefits or being charged higher prices. One such commenter also noted that heightened choice for sensitive data is consistent with the FTC staff's Self-Regulatory Principles for Online Behavioral Advertising ("2009 OBA Report").²¹⁶

Rather than always requiring consent, an industry trade association pushed for a more flexible approach to the use of sensitive data in first-party marketing.²¹⁷ This commenter stated that the choice analysis should depend upon the particular context and circumstances in which the data is used. The commenter noted that, for example, with respect to sensitive location data, where a consumer uses a wireless service to find nearby restaurants and receive discounts, the consumer implicitly understands his location data will be used and consent can be inferred.

The Commission agrees with the commenters who stated that affirmative express consent is appropriate when a company uses sensitive data for any marketing, whether first- or third-party. Although, as a general rule, most first-party marketing presents fewer privacy concerns, the calculus changes when the data is sensitive. Indeed, when health or children's information is involved, for example, the likelihood that data misuse could lead to embarrassment, discrimination, or other harms is increased. This risk exists regardless of whether the entity collecting and using the data is a first party or a third party that is unknown to the consumer. In light of the heightened privacy risks associated with sensitive data, first parties should provide a consumer choice mechanism at the time of data collection.²¹⁸

At the same time, the Commission believes this requirement of affirmative express consent for first-party marketing using sensitive data should be limited. Certainly, where a company's business model is *designed to target* consumers based on sensitive data – including data about children, financial and health information, Social Security numbers, and certain geolocation data – the company should seek affirmative express consent before collecting the data from those consumers.²¹⁹ On the other hand, the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive

214 The Commission defines as sensitive, at a minimum, data about children, financial and health information, Social Security numbers, and certain geolocation data, as discussed below. See *infra* Section IV.C.2.e.(ii).

215 *Comment of Center for Democracy & Technology*, cmt. #00469, at 10; *Comment of Consumer Federation of America*, cmt. #00358, at 8-9; *Comment of Consumers Union*, cmt. #00362, at 12-13.

216 See *Comment of Center for Democracy & Technology*, cmt. #00469 at 10 (citing FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, 43-44 (2009), <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>).

217 *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 4-6.

218 Additional discussion regarding the necessary level of consent for the collection or use of sensitive data, as well as other practices that raise special privacy considerations, is set forth below. See *infra* Section IV.C.2.e.(ii).

219 These categories of sensitive data are discussed further below. See *infra* Section IV.C.2.e.(ii).

information. For example, the Commission has previously noted that online retailers and services such as Amazon.com and Netflix need not provide choice when making product recommendations based on prior purchases. Thus, if Amazon.com were to recommend a book related to health or financial issues based on a prior purchase on the site, it need not provide choice. However, if a health website is designed to target people with particular medical conditions, that site should seek affirmative express consent when marketing to consumers.

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company’s relationship with the consumer, or are required or specifically authorized by law.

2. FOR PRACTICES INCONSISTENT WITH THE CONTEXT OF THEIR INTERACTION WITH CONSUMERS, COMPANIES SHOULD GIVE CONSUMERS CHOICES.

Proposed Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.

For those practices for which choice is contemplated, the proposed framework called on companies to provide choice at a time and in a context in which the consumer is making a decision about his or her data. In response, commenters discussed a number of issues, including the methods for providing just in time choice, when “take-it-or-leave-it” choice may be appropriate, how to respond to the call for a Do Not Track mechanism that would allow consumers to control online tracking, and the contexts in which affirmative express consent is necessary.

The Commission adopts the proposed framework’s formulation that choice should be provided at a time and in a context in which the consumer is making a decision about his or her data. The Commission also adds new language addressing when a company should seek a consumer’s affirmative express consent.

a. Companies Should Provide Choices At a Time and In a Context in Which the Consumer Is Making a Decision About His or Her Data.

The call for companies to provide a “just in time” choice generated numerous comments. Several consumer organizations as well as industry commenters stressed the importance of offering consumer choice at the time the consumer provides – and the company collects or uses – the data at issue and pointed to examples of existing mechanisms for providing effective choice.²²⁰ One commenter stated that in order to make choice mechanisms meaningful to consumers, companies should incorporate them as a feature of a product or service rather than as a legal disclosure.²²¹ Using its vendor recommendation service as an example, this commenter suggested incorporating a user’s sharing preferences into the sign-up process instead of setting such preferences as a default that users can later adjust and personalize. Another

²²⁰ See *Comment of Consumer Federation of America*, cmt. #00358, at 10; *Comment of Center for Democracy & Technology*, cmt. #00469, at 23-24; *Comment of AT&T Inc.*, cmt. #00420, at 22-23; *Comment of Phorm Inc.*, cmt. #00353, at 9-10.

²²¹ *Comment of AT&T Inc.*, cmt. #00420, at 22-23.

commenter stated that choice options should occur in a “time-appropriate manner” that takes into account the “functional and aesthetic context” of the product or service.²²²

Others raised concerns about the practicality of providing choice prior to the collection or use of data in different contexts.²²³ For instance, a number of commenters discussed the offline retail context and noted that cashiers are typically unqualified to communicate privacy information or to discuss data collection and use practices with customers.²²⁴ One commenter further discussed the logistical problems with providing such information at the point of sale, citing consumer concerns about ease of transaction and in-store wait times.²²⁵ Other commenters described the impracticality of offering and obtaining advance consent in an offline mail context, such as a magazine subscription card or catalogue request that a consumer mails to a fulfillment center.²²⁶ In the online context, one commenter expressed concern that “pop-up” choice mechanisms complicate or clutter the user experience, which could lead to choice “fatigue.”²²⁷ Another commenter noted that where data collection occurs automatically, such as in the case of online behavioral advertising, obtaining consent before collection could be impractical.²²⁸

One theme that a majority of the commenters addressing this issue articulated is the need for flexibility so that companies can tailor the choice options to specific business models and contexts.²²⁹ Rather than a rigid reliance on advance consent, commenters stated that companies should be able to provide choice before collection, close to the time of collection, or a time that is convenient to the consumer.²³⁰ The precise method should depend upon context, the sensitivity of the data at issue, and other factors.²³¹ Citing its own best practices guidance, one trade organization recommended that the Commission focus not on the precise mechanism for offering choice, but on whether the consent is informed and based on sufficient notice.²³²

The Commission appreciates the concerns that commenters raised about the timing of providing choices. Indeed, the proposed framework was not intended to set forth a “one size fits all” model for designing consumer choice mechanisms. Staff instead called on companies to offer clear and concise choice

222 *Comment of Center for Democracy & Technology*, cmt. #00469, at 11.

223 *See Comment of Microsoft Corp.*, cmt. #00395, at 8-10, 14; *Comment of SIFMA*, cmt. #00265, at 5-6; *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 8-10.

224 *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 8; *Comment of Experian*, cmt. #00398, at 9.

225 *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 8.

226 *See Comment of Magazine Publishers of America*, cmt. #00332, at 4 (noting that the “blow-in cards” in magazines often used to solicit new subscriptions have very limited space, and including lengthy disclosures on these cards could render them unreadable); *Comment of American Catalogue Mailers Ass’n*, cmt. #00424, at 7.

227 *See Comment of Retail Industry Leaders Ass’n*, cmt. #00352 at 7; *see also Comment of Experian*, cmt. #00398, at 9 (noting that the proposed changes in notice and choice procedures would be inconvenient for consumers and would damage the consumer experience).

228 *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 8.

229 *Comment of Microsoft Corp.*, cmt. #00395, at 2; *Comment of AT&T Inc.*, cmt. #00420 at 3, 7; *Comment of Consumers Union*, cmt. #00362, at 5, 11-12; *Comment of Consumer Federation of America*, cmt. #00358, at 10.

230 *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 9.

231 *Comment of Facebook, Inc.*, cmt. #00413, at 10; *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 9; *see also Comment of Experian*, cmt. #00398, at 9 (generally disputing the need for “just-in-time” notice, but acknowledging that it might be justified for the transfer to non-affiliated third parties of sensitive information for marketing purposes).

232 *See Comment of CTIA - The Wireless Ass’n*, cmt. #00375, at 10 (describing the form of consent outlined in the CTIA’s “Best Practices and Guidelines for Location-Based Services”).

mechanisms that are easy to use and are delivered at a time and in a context that is relevant to the consumer's decision about whether to allow the data collection or use. Precisely how companies in different industries achieve these goals may differ depending on such considerations as the nature or context of the consumer's interaction with a company or the type or sensitivity of the data at issue.

In most cases, providing choice before or at the time of collection will be necessary to gain consumers' attention and ensure that the choice presented is meaningful and relevant. If a consumer is submitting his or her data online, the consumer choice could be offered, for example, directly adjacent to where the consumer is entering his or her data. In other contexts, the choice might be offered immediately upon signing up for a service, as in the case of a social networking website.

In some contexts, however, it may be more practical to communicate choices at a later point. For example, in the case of an offline retailer, the choice might be offered close to the time of a sale, but in a manner that will not unduly interfere with the transaction. This could include communicating the choice mechanism through a sales receipt or on a prominent poster at the location where the transaction takes place. In such a case, there is likely to be a delay between when the data collection takes place and when the consumer is able to contact the company in order to exercise any choice options. Accordingly, the company should wait for a disclosed period of time before engaging in the practices for which choice is being offered.²³³ The Commission also encourages companies to examine the effectiveness of such choice mechanisms periodically to determine whether they are sufficiently prominent, effective, and easy to use.

Industry is well positioned to design and develop choice mechanisms that are practical for particular business models or contexts, and that also advance the fundamental goal of giving consumers the ability to make informed and meaningful decisions about their privacy. The Commission calls on industry to use the same type of creativity industry relies on to develop effective marketing campaigns and user interfaces for consumer choice mechanisms. One example of such a creative approach is the online behavioral advertising industry's development of a standardized icon and text that is embedded in targeted advertisements. The icon and text are intended to communicate that the advertising may rely on data collected about consumers. They also serve as a choice mechanism to allow the consumer to exercise control over the delivery of such ads.²³⁴ Even though in most cases, cookie placement has already occurred, the in-ad disclosure provides a logical "teachable moment" for the consumer who is making a decision about his or her data.²³⁵

b. Take-it-or-Leave-it Choice for Important Products or Services Raises Concerns When Consumers Have Few Alternatives.

Several commenters addressed whether it is appropriate for a company to make a consumer's use of its product or service contingent upon the consumer's acceptance of the company's data practices. Two industry

²³³ The FTC recognizes that incorporating this delay period may require companies to make programming changes to their systems. As noted above, in the discussion of legacy data systems, see *supra* at Section IV.B.2., these changes may take time to implement.

²³⁴ As noted in Section IV.C.2.c., industry continues to consider ways to make the icon and opt out mechanism more usable and visible for consumers.

²³⁵ *But see Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 29 (criticizing visibility of the icon to consumers).

commenters suggested that “take-it-or-leave-it” or “walk away” choice is common in many business models, such as retail and software licensing, and companies have a right to limit their business to those who are willing to accept their policies.²³⁶ Another commenter stated that preventing companies from offering take-it-or-leave-it choice might be unconstitutional under the First Amendment.²³⁷ Other commenters, however, characterized walk away choice as generally inappropriate.²³⁸ Some argued that the privacy framework should prevent companies from denying consumers access to goods or services, including website content, where consumers choose to limit the collection or use of their data.²³⁹

Most of the commenters that addressed this issue took a position somewhere in between.²⁴⁰ In determining whether take-it-or-leave-it choice is appropriate, these commenters focused on three main factors. First, they noted that there must be adequate competition, so that the consumer has alternative sources to obtain the product or service in question.²⁴¹ Second, they stated that the transaction must not involve an essential product or service.²⁴² Third, commenters stated that the company offering take-it-or-leave-it choice must clearly and conspicuously disclose the terms of the transaction so that the consumer is able to understand the value exchange. For example, a company could clearly state that in exchange for receiving a service at “no cost,” it collects certain information about your activity and sells it to third parties.²⁴³ Expanding upon this point, commenters stressed that to ensure consumer understanding of the nature of the take-it-or-leave-it bargain, the disclosure must be prominent and not buried within a privacy policy.²⁴⁴

The Commission agrees that a “take it or leave it” approach is problematic from a privacy perspective, in markets for important services where consumers have few options.²⁴⁵ For such products or services, businesses should not offer consumers a “take it or leave it” choice when collecting consumers’ information in a manner inconsistent with the context of the interaction between the business and the consumer. Take,

236 *Comment of Performance Marketing Ass’n*, cmt. #00414, at 6; *Comment of Business Software Alliance*, cmt. #00389, at 11-12.

237 *Comment of Tech Freedom*, cmt. #00451, at 17.

238 *Comment of Consumer Federation of America*, cmt. #00358, at 11; *Comment of ePrio, Inc.*, cmt. #00267, at 4-5.

239 *Comment of Consumer Federation of America*, cmt. #00358, at 11; *see also Comment of Consumers Union*, cmt. #00362, at 12 (urging that consumers who choose to restrict sharing of their PII with unknown third parties should not be punished for that choice).

240 *See, e.g., Comment of Center for Democracy & Technology*, cmt. #00469, at 13 (stating that it has no objection to take-it-or-leave-it approaches, provided there is competition and the transaction does not involve essential services); *Comment of Microsoft Corp.*, cmt. #00395, at 10 (stating that take-it-or-leave-it choice is appropriate provided the “deal” is made clear to the consumer); *Comment of the Information Commissioner’s Office of the UK*, cmt. #00249, at 4 (stating that take-it-or-leave-it choice would be inappropriate where the consumer has no real alternative but to use the service); *Comment of Reed Elsevier, Inc.*, cmt. #00430, at 11 (stating that while acceptable for the websites of private industry, websites that provide a public service and may be the single source of certain information, such as outsourced government agency websites, should not condition their use on take-it-or-leave-it terms).

241 *Comment of Center for Democracy & Technology*, cmt. #00469, at 13; *Comment of the Information Commissioner’s Office of the UK*, cmt. #00249, at 4.

242 *Comment of Center for Democracy & Technology*, cmt. #00469, at 13; *Comment of Reed Elsevier, Inc.*, cmt. #00430, at 11.

243 *Comment of Microsoft Corp.*, cmt. #00395, at 10; *see also Comment of Center for Democracy & Technology*, cmt. #00469, at 13 (stating that the terms of the bargain should be clearly and conspicuously disclosed).

244 *Comment of TRUSTe*, cmt. #00450, at 11; *see also Comment of Center for Democracy & Technology*, cmt. #00469, at 13 (stating that terms should be “transparent and fairly presented”).

245 This Report is not intended to reflect Commission guidance regarding Section 5’s prohibition on unfair methods of competition.

for example, the purchase of an important product that has few substitutes, such as a patented medical device. If a company offered a limited warranty for the device only in exchange for the consumer's agreeing to disclose his or her income, religion, and other highly-personal information, the consumer would not have been offered a meaningful choice and a take-it-or-leave approach would be inappropriate.

Another example is the provision of broadband Internet access. As consumers shift more aspects of their daily lives to the Internet – shopping, interacting through social media, accessing news, entertainment, and information, and obtaining government services – broadband has become a critical service for many American consumers. When consumers have few options for broadband service, the take-it-or-leave-it approach becomes one-sided in favor of the service provider. In these situations, the service provider should not condition the provision of broadband on the customer's agreeing to, for example, allow the service provider to track all of the customer's online activity for marketing purposes. Consumers' privacy interests ought not to be put at risk in such one-sided transactions.

With respect to less important products and services in markets with sufficient alternatives, take-it-or-leave-it choice can be acceptable, provided that the terms of the exchange are transparent and fairly disclosed – e.g., “we provide you with free content in exchange for collecting information about the websites you visit and using it to market products to you.” Under the proper circumstances, such choice options may result in lower prices or other consumer benefits, as companies develop new and competing ways of monetizing their business models.

c. Businesses Should Provide a Do Not Track Mechanism To Give Consumers Control Over the Collection of Their Web Surfing Data.

Like the preliminary staff report, this report advocates the continued implementation of a universal, one-stop choice mechanism for online behavioral tracking, often referred to as Do Not Track. Such a mechanism should give consumers the ability to control the tracking of their online activities.

Many commenters discussed the progress made by industry in developing such a choice mechanism in response to the recommendations of the preliminary staff report and the 2009 OBA Report, and expressed support for these self-regulatory initiatives.²⁴⁶ These initiatives include the work of the online advertising industry over the last two years to simplify disclosures and improve consumer choice mechanisms; efforts by the major browsers to offer new choice mechanisms; and a project of a technical standards body to

²⁴⁶ See, e.g., *Comment of American Ass'n of Advertising Agencies et. al*, cmt. #00410, at 3 (describing the universal choice mechanisms used in the coalition's Self-Regulatory Principles for Online Behavioral Advertising Program); *Comment of BlueKai*, cmt. #00397, at 3 (describing its development of the NAI Opt-Out Protector for Firefox); *Comment of Computer & Communications Industry Ass'n*, cmt. #00434, at 17 (describing both company-specific and industry-wide opt-out mechanisms currently in use); *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 3 (stating that the Self-Regulatory Principles for Online Behavioral Advertising Program addresses the concerns that motivate calls for a “Do-Not-Track” mechanism); *Comment of Facebook, Inc.*, cmt. #00413, at 13 (describing behavioral advertising opt-out mechanisms developed by both browser makers and the advertising industry); *Comment of Future of Privacy Forum*, cmt. #00341, at 2-4 (describing the development of a browser-based Do-Not-Track header and arguing that the combined efforts of browser companies, ad networks, consumers, and government are likely to result in superior choice mechanisms); *Comment of Google, Inc.*, cmt. #00417, at 5 (describing its Ad Preferences Manager and Keep My Opt-Outs tools); *Comment of Interactive Advertising Bureau*, cmt. #00388, at 5-7 (describing the Self-Regulatory Principles for Online Behavioral Advertising Program); *Comment of Microsoft Corp.*, cmt. #00395, at 11-14 (describing a variety of browser-based and ad network-based choice tools currently available); *Comment of U.S. Chamber of Commerce*, cmt. #00452, at 5-6 (describing a variety of browser-based and ad network-based choice tools currently available).

standardize opt outs for online tracking.²⁴⁷ A number of commenters, however, expressed concerns that existing mechanisms are still insufficient. Commenters raised questions about the effectiveness and comprehensiveness of existing mechanisms for exercising choice and the legal enforceability of such mechanisms.²⁴⁸ Due to these concerns, some commenters advocated for legislation mandating a Do Not Track mechanism.²⁴⁹

The Commission commends recent industry efforts to improve consumer control over behavioral tracking and looks forward to final implementation. As industry explores technical options and implements self-regulatory programs, and Congress examines Do Not Track, the Commission continues to believe that in order to be effective, any Do Not Track system should include five key principles. First, a Do Not Track system should be implemented universally to cover all parties that would track consumers. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes.²⁵⁰ Finally, an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (*e.g.*, preventing click-fraud or collecting de-identified data for analytics purposes).²⁵¹

Early on the companies that make web browsers stepped up to the challenge to give consumers choice about how they are tracked online, sometimes known as the “browser header” approach. The browser header is transmitted to all types of entities, including advertisers, analytics companies, and researchers, that track consumers online. Just after the FTC’s call for Do Not Track, Microsoft developed a system to let users of Internet Explorer prevent tracking by different companies and sites.²⁵² Mozilla introduced a Do Not Track privacy control for its Firefox browser that an impressive number of consumers have adopted.²⁵³

²⁴⁷ See *supra* at Section II.C.1.

²⁴⁸ *Comment of American Civil Liberties Union*, cmt. #00425, at 12; *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 28; *Comment of Consumer Federation of America*, cmt. #00358, at 13; *Comment of Consumers Union*, cmt. #00362, at 14; see also *Comment of World Privacy Forum*, cmt. #00369, at 3 (noting prior failures of self-regulation in the online advertising industry).

²⁴⁹ *E.g.*, *Comment of Consumers Union*, cmt. #00362, at 14; *Comment of World Privacy Forum*, cmt. #00369, at 3.

²⁵⁰ For example, consumers may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked through Flash cookies or other mechanisms. The FTC recently brought an action against a company that told consumers they could opt out of tracking by exercising choices through their browsers; however, the company used Flash cookies for such tracking, which consumers could not opt out of through their browsers. *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 21, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/1023185/111221scanscoutdo.pdf>.

²⁵¹ Such a mechanism should be different from the Do Not Call program in that it should not require the creation of a “Registry” of unique identifiers, which could itself cause privacy concerns.

²⁵² *Comment of Microsoft Corp.*, cmt. #00395, at 12.

²⁵³ *Comment of Mozilla*, cmt. #00480, at 2; Alex Fowler, *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop*, MOZILLA PRIVACY BLOG, (Nov. 2, 2011), <http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/>.

Apple subsequently included a similar Do Not Track control in Safari.²⁵⁴ Google has taken a slightly different approach – providing consumers with a tool that persistently opts them out of most behavioral advertising.²⁵⁵

In another important effort, the online advertising industry, led by the DAA, has implemented a behavioral advertising opt-out program. The DAA's accomplishments are notable: it has developed a notice and choice mechanism through a standard icon in ads and on publisher sites; deployed the icon broadly, with over 900 billion impressions served each month; obtained commitments to follow the self-regulatory principles from advertisers, ad networks, and publishers that represent close to 90 percent of the online behavioral advertising market; and established an enforcement mechanism designed to ensure compliance with the principles.²⁵⁶ More recently, the DAA addressed one of the long-standing criticisms of its approach – how to limit secondary use of collected data so that the consumer opt out extends beyond simply blocking targeted ads to the collection of information for other purposes. The DAA has released new principles that include limitations on the collection of tracking data and prohibitions on the use or transfer of the data for employment, credit, insurance, or health care eligibility purposes.²⁵⁷ Just as important, the DAA recently moved to address some persistence and usability criticisms of its icon-based opt out by committing to honor the tracking choices consumers make through their browser settings.²⁵⁸

At the same time, the W3C Internet standards-setting body has gathered a broad range of stakeholders to create an international, industry-wide standard for Do Not Track. The group includes a wide variety of stakeholders, including DAA members; other U.S. companies; international companies; industry groups; and public-interest groups. The W3C group has done admirable work to flesh out the details required to make a Do Not Track system practical in both desktop and mobile settings. The group has issued two public working drafts of its standards. Some important details remain to be filled in, and the Commission encourages all of the stakeholders to work within the W3C group to resolve these issues.

While more work remains to be done on Do Not Track, the Commission believes that the developments to date are significant and provide an effective path forward. The advertising industry, through the DAA, has committed to deploy browser-based technologies for consumer control over online tracking, alongside its ubiquitous icon program. The W3C process, thanks in part to the ongoing participation of DAA member companies, has made substantial progress toward specifying a consensus consumer choice system for tracking

254 Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, WALL ST. J. Apr. 13, 2011, *available at* <http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html>.

255 *Comment of Google Inc.*, cmt. #00417, at 5.

256 Peter Kosmala, *Yes, Johnny Can Benefit From Transparency & Control*, SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, <http://www.aboutads.info/blog/yes-johnny-can-benefit-transparency-and-control> (Nov. 3, 2011); *see also* Press Release, Digital Advertising Alliance, White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumers Online Privacy, (Feb. 23, 2012), *available at* <http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf>.

257 Digital Advertising Alliance, *About Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), *available at* <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

258 Press Release, Digital Advertising Alliance, DAA Position on Browser Based Choice Mechanism (Feb. 22, 2012), *available at* <http://www.aboutads.info/resource/download/DAA.Commitment.pdf>.

that is practical and technically feasible.²⁵⁹ The Commission anticipates continued progress in this area as the DAA members and other key stakeholders continue discussions within the W3C process to work to reach consensus on a Do Not Track system in the coming months.

d. Large Platform Providers That Can Comprehensively Collect Data Across the Internet Present Special Concerns.

As discussed above, even if a company has a first-party relationship with a consumer in one setting, this does not imply that the company can track the consumer for purposes inconsistent with the context of the interaction across the Internet, without providing choice. This principle applies fully to large platform providers such as ISPs, operating systems, and browsers, who have very broad access to a user's online activities.

For example, the preliminary staff report sought comment on the use of DPI for marketing purposes. Many commenters highlighted the comprehensive nature of DPI.²⁶⁰ Because of the pervasive tracking that DPI allows, these commenters stated that its use for marketing should require consumers' affirmative express consent.²⁶¹ Privacy concerns led one commenter to urge the Commission to oppose DPI and hold workshops and hearings on the issue.²⁶² Another commenter argued that a lack of significant competition among broadband providers argues in favor of heightened requirements for consumer choice before ISPs can use DPI for marketing purposes.²⁶³

Two major ISPs emphasized that they do not use DPI for marketing purposes and would not do so without first seeking their customers' affirmative express consent.²⁶⁴ They cautioned against singling out DPI as a practice that presents unique privacy concerns, arguing that doing so would unfairly favor certain technologies or business models at the expense of others. One commenter also stated that the framework should not favor companies that use other means of tracking consumers.²⁶⁵ This commenter noted that various technologies – including cookies – allow companies to collect and use information in amounts similar to that made possible through DPI, and the framework's principles should apply consistently based

259 A system practical for both businesses and consumers would include, for users who choose to enable Do Not Track, significant controls on the collection and use of tracking data by third parties, with limited exceptions such as security and frequency capping. As noted above, first-party sharing with third parties is not consistent with the context of the interaction and would be subject to choice. Do Not Track is one way for users to express this choice.

260 *Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15; *Comment of Center for Democracy & Technology*, cmt. #00469, at 14-15.

261 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 14; *Comment of Phorm Inc.*, cmt. #00353, at 5; *see also Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15 (urging that heightened requirements for consumer choice apply for the use of DPI); *Comment of Online Trust Alliance*, cmt. #00299, at 6 ("The use of DPI and related technologies may also be permissible when consumers have the ability to opt-in and receive appropriate and proportional quantifiable benefits in return.")

262 *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 37.

263 *Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15.

264 *Comment of AT&T Inc.*, cmt. #00420, at 21; *see also Comment of Verizon*, cmt. #00428, at 7 n.6. Likewise, a trade association of telecommunications companies represented that ISPs have not been extensively involved in online behavioral advertising. *See Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 33.

265 *See Comment of Verizon*, cmt. #00428, at 7.

on the type of information collected and how it is used.²⁶⁶ Rather than isolating a specific technology, commenters urged the Commission to focus on the type of data collected and how it is used.²⁶⁷

ISPs serve as a major gateway to the Internet with access to vast amounts of unencrypted data that their customers send or receive over the ISP's network. ISPs are thus in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible. In addition, it may be difficult for some consumers to obtain alternative sources of broadband Internet access, and they may be inhibited from switching broadband providers for reasons such as inconvenience or expense. Accordingly, the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection.²⁶⁸

At the same time, the Commission agrees that any privacy framework should be technology neutral. ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.²⁶⁹ Consumers, moreover, might have limited ability to block or control such tracking except by changing their operating system or browser.²⁷⁰ Thus, comprehensive tracking by any such large platform provider may raise serious privacy concerns.

The Commission also recognizes that the use of cookies and social widgets to track consumers across unrelated websites may create similar privacy issues.²⁷¹ However, while companies such as Google and Facebook are expanding their reach rapidly, they currently are not so widespread that they could track a consumer's every movement across the Internet.²⁷² Accordingly, although tracking by these entities warrants consumer choice, the Commission does not believe that such tracking currently raises the same level of privacy concerns as those entities that can comprehensively track all or virtually of a consumer's online activity.

These are complex and rapidly evolving areas, and more work should be done to learn about the practices of all large platform providers, their technical capabilities with respect to consumer data, and their current and expected uses of such data. Accordingly, Commission staff will host a workshop in the second half

²⁶⁶ *Id.* at 7-8.

²⁶⁷ See, e.g., *Comment of Internet Commerce Coalition*, cmt. #00447, at 10; *Comment of KINDSIGHT*, cmt. #00344, at 7-8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 36; *Comment of Verizon*, cmt. #00428, at 7-8.

²⁶⁸ This discussion does not apply to ISPs' use of DPI for network management, security, or other purposes consistent with the context of a consumer's interaction with their ISP.

²⁶⁹ This discussion is not meant to imply that ISPs, operating systems, or browsers are currently building these profiles for marketing purposes.

²⁷⁰ ISPs, operating systems, and browsers have different access to users' online activity. A residential ISP can access unencrypted traffic from all devices currently located in the home. An operating system or browser, on the other hand, can access all traffic regardless of location and encryption, but only from devices on which the operating system or browser is installed. Desktop users have the ability to change browsers to avoid monitoring, but mobile users have fewer browser options.

²⁷¹ A social widget is a button, box, or other possibly interactive display associated with a social network that is embedded into another party's website.

²⁷² BrightEdge, *Social Share Report: Social Adoption Among Top Websites*, 3-4 (July 2011), available at <http://www.brightedge.com/resfiles/brightedge-report-socialshare-2011-07.pdf> (reporting that by mid-2011, the Facebook Like button appeared on almost 11% of top websites' front pages and Google's +1 button appeared on 4.5% of top websites' front pages); see also Justin Osofsky, *After f8: Personalized Social Plugins Now on 100,000+ Sites*, FACEBOOK DEVELOPER BLOG (May 11, 2010, 9:15 AM), <http://developers.facebook.com/blog/post/382/>.

of 2012 to explore the privacy issues raised by the collection and use of consumer information by a broad range of large platform providers such as ISPs, operating systems, browsers, search engines, and social media platforms as well as how competition issues may bear on appropriate privacy protection.²⁷³

e. Practices Requiring Affirmative Express Consent.

Numerous commenters focused on whether certain data collection and use practices warrant a heightened level of consent – *i.e.*, affirmative express consent.²⁷⁴ These practices include (1) making material retroactive changes to a company’s privacy representations; and (2) collection of sensitive data. These comments and the Commission’s analysis are discussed here.

(i) Companies Should Obtain Affirmative Express Consent Before Making Material Retroactive Changes To Privacy Representations.

The preliminary staff report reaffirmed the Commission’s bedrock principle that companies should provide prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection.²⁷⁵

Although many commenters supported the affirmative express consent standard for material retroactive changes,²⁷⁶ some companies called for an opt-out approach for material retroactive changes, particularly for changes that provide benefits to consumers.²⁷⁷ One example cited was the development of Netflix’s personalized video recommendation feature using information that Netflix originally collected in order to send consumers the videos they requested.²⁷⁸ Other companies sought to scale the affirmative consent requirement according to the sensitivity of the data and whether the data is personally identifiable.²⁷⁹ Many commenters sought clarification on when a change is material – for example, whether a change in data retention periods would be a material change requiring heightened consent.²⁸⁰ One company posited

273 See *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 37 (recommending FTC hold a workshop to address DPI).

274 Companies may seek “affirmative express consent” from consumers by presenting them with a clear and prominent disclosure, followed by the ability to opt in to the practice being described. Thus, for example, requiring the consumer to scroll through a ten-page disclosure and click on an “I accept” button would not constitute affirmative express consent.

275 In the preliminary report, this principle appeared under the heading of “transparency.” See, e.g., *In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004) (consent order) (alleging that Gateway violated the FTC Act by applying material changes to a privacy policy retroactively), available at <http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf>; see also FTC, *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), available at <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf> (noting the requirement that companies obtain affirmative express consent before making material retroactive changes to their privacy policies).

276 See *Comment of Consumers Union*, cmt. #00362, at 17; *Comment of Future of Privacy Forum*, cmt. #00341, at 5; *Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 21.

277 See *Comment of Facebook, Inc.*, cmt. #00413, at 11; see also *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 12; *Comment of AT&T Inc.*, cmt. #00420, at 29-30; *Comment of National Cable & Telecommunications Ass’n*, cmt. #00432, at 30-31.

278 *Comment of Facebook, Inc.*, cmt. #00413, at 8.

279 See *Comment of AT&T Inc.*, cmt. #00420, at 30; *Comment of Phorm Inc.*, cmt. #00353, at 1.

280 See *Comment of Future of Privacy Forum*, cmt. #00341, at 4; *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 12; *Comment of Microsoft Corp.*, cmt. #00395, at 17.

that the affirmative express consent standard would encourage vague disclosures at the outset to avoid the requirement for obtaining such consent.²⁸¹

The Commission reaffirms its commitment to requiring companies to give prominent disclosures and to obtain express affirmative consent for material retroactive changes. Indeed, the Commission recently confirmed this approach in its settlements with Google and Facebook. The settlement agreements mandate that the companies give their users clear and prominent notice and obtain affirmative express consent prior to making certain material retroactive changes to their privacy practices.²⁸²

In response to the request for clarification on what constitutes a material change, the Commission notes that, at a minimum, sharing consumer information with third parties after committing at the time of collection not to share the data would constitute a material change. There may be other circumstances in which a change would be material, which would have to be determined on a case-by-case basis, analyzing the context of the consumer's interaction with the business.

The Commission further notes that commenters' concerns that the affirmative express consent requirement would encourage vague disclosures at the outset should be addressed by other elements of the framework. For example, other elements of the framework call on companies to improve and standardize their privacy statements so that consumers can easily glean and compare information about various companies' data practices. The framework also calls on companies to give consumers specific information and choice at a time and in a context that is meaningful to consumers. These elements, taken together, are intended to result in disclosures that are specific enough to be meaningful to consumers.

The preliminary staff report posed a question about the appropriate level of consent for prospective changes to companies' data collection and use. One commenter cited the rollout of Twitter's new user interface – “new Twitter” – as a positive example of a set of prospective changes about which consumers received ample and adequate notice and ability to exercise choice.²⁸³ When “new Twitter” was introduced, consumers were given the opportunity to switch to or try out the new interface, or to keep their traditional Twitter profile. The Commission supports innovative efforts such as these to provide consumers with meaningful choices when a company proposes to change its privacy practices on a prospective basis.

(ii) Companies Should Obtain Consumers' Affirmative Express Consent Before Collecting Sensitive Data.

A variety of commenters discussed how to delineate which types of data should be considered sensitive. These comments reflect a general consensus that information about children, financial and health information, Social Security numbers, and precise, individualized geolocation data is sensitive and

281 *Comment of Facebook, Inc.*, cmt. #00413, at 10.

282 See *In the Matter of Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* <http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf>; *In the Matter of Facebook, Inc.*, FTC File No. 092-3184 (Nov. 29, 2011) (proposed consent order), *available at* <http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf>.

283 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 15.

merits heightened consent methods.²⁸⁴ In addition, some commenters suggested that information related to race, religious beliefs, ethnicity, or sexual orientation, as well as biometric and genetic data, constitute sensitive data.²⁸⁵ One commenter also characterized as sensitive information about consumers' online communications or reading and viewing habits.²⁸⁶ Other commenters, however, noted the inherent subjectivity of the question and one raised concerns about the effects on market research if the definition of sensitive data is construed too broadly.²⁸⁷

Several commenters focused on the collection and use of information from teens, an audience that may be particularly vulnerable. A diverse coalition of consumer advocates and others supported heightened protections for teens between the ages of 13 and 17.²⁸⁸ These commenters noted that while teens are heavy Internet users, they often fail to comprehend the long-term consequences of sharing their personal data. In order to better protect this audience, the commenters suggested, for example, limiting the amount of data that websites aimed at teens can collect or restricting the ability of teens to share their data widely through social media services.

Conversely, a number of industry representatives and privacy advocates objected to the establishment of different rules for teens.²⁸⁹ These commenters cited the practical difficulties of age verification and the potential that content providers will simply elect to bar teen audiences.²⁹⁰ Rather than requiring different choice mechanisms for this group, one company encouraged the FTC to explore educational efforts to address issues that are unique to teens.²⁹¹

Given the general consensus regarding information about children, financial and health information, Social Security numbers, and precise geolocation data, the Commission agrees that these categories of information are sensitive. Accordingly, before collecting such data, companies should first obtain affirmative express consent from consumers. As explained above, the Commission also believes that companies should

284 See, e.g., *Comment of Consumer Federation of America*, cmt. #00358, at 9; *Comment of CNIL*, cmt. #00298, at 4; *Comment of Massachusetts Office of the Attorney General*, cmt. #00429, at 3; *Comment of Kindsight*, cmt. #00344, at 11; *Comment of Experian*, cmt. #00398, at 9; *Comment of Center for Democracy & Technology*, cmt. #00469, at 14; *Comment of Office of the Information and Privacy Commissioner of Ontario*, cmt. #00239, at 2; see also *Comment of TRUSTe*, cmt. #00450, at 11 (agreeing that sensitive information should be defined to include information about children, financial and medical information, and precise geolocation information but urging that sensitive information be more broadly defined as “information whose unauthorized disclosure or use can cause financial, physical, or reputational harm”); *Comment of Facebook, Inc.*, cmt. #00413, at 23 (agreeing that sensitive information may warrant enhanced consent, but noting that enhanced consent may not be possible for activities such as the posting of status updates by users where those updates may include sensitive information such as references to an illness or medical condition).

285 See *Comment of Consumer Federation of America*, cmt. #00358, at 9; see also *Comment of CNIL*, cmt. #00298, at 4, *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 35.

286 See *Comment of Electronic Frontier Foundation*, cmt. #00400, at 7.

287 See *Comment of Marketing Research Ass'n*, cmt. #00405, at 6-7; *Comment of American Trucking Ass'ns*, cmt. #00368, at 2-3; *Comment of Microsoft Corp.*, cmt. #00395, at 10.

288 See *Comment of Institute for Public Representation*, cmt. #00346, at 4; *Comment of Consumers Union*, cmt. #00362, at 13.

289 See *Comment of Center for Democracy & Technology*, cmt. #00469, at 15; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 12-13; *Comment of Microsoft Corp.*, cmt. #00395, at 10; see also *Comment of Electronic Frontier Foundation*, cmt. #00400, at 14 (opposing the creation of special rules giving parents access to data collected about their teenaged children); *Comment of PrivacyActivism*, cmt. #00407, at 4 (opposing the creation of special rules giving parents access to data collected about their teenaged children).

290 See *Comment of Center for Democracy & Technology*, cmt. #00469, at 15; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 12-13; *Comment of Microsoft Corp.*, cmt. #00395, at 10.

291 See *Comment of Microsoft Corp.*, cmt. #00395, at 10.

follow this practice irrespective of whether they use the sensitive data for first-party marketing or share it with third parties.²⁹²

The Commission is cognizant, however, that whether a particular piece of data is sensitive may lie in the “eye of the beholder” and may depend upon a number of subjective considerations. In order to minimize the potential of collecting any data – whether generally recognized as sensitive or not – in ways that consumers do not want, companies should implement *all* of the framework’s components. In particular, a consumer’s ability to access – and in appropriate cases to correct or delete – data will allow the consumer to protect herself when she believes the data is sensitive but others may disagree.

With respect to whether information about teens is sensitive, despite the difficulties of age verification and other concerns cited in the comments, the Commission agrees that companies that target teens should consider additional protections. Although affirmative express consent may not be necessary in every advertising campaign directed to teens, other protections may be appropriate. For example, all companies should consider shorter retention periods for teens’ data.

In addition, the Commission believes that social networking sites should consider implementing more privacy-protective default settings for teens. While some teens may circumvent these protections, they can function as an effective “speed bump” for this audience and, at the same time, provide an opportunity to better educate teens about the consequences of sharing their personal information. The Commission also supports access and deletion rights for teens, as discussed below.²⁹³

Final Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

D. TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

Citing consumers’ lack of awareness of how, and for what purposes, companies collect, use, and share data, the preliminary staff report called on companies to improve the transparency of their data practices. Commission staff outlined a number of measures to achieve this goal. One key proposal, discussed in the previous section, is to present choices to consumers in a prominent, relevant, and easily accessible place at a time and in a context when it matters to them. In addition, Commission staff called on industry to make privacy statements clearer, shorter, and more standardized; give consumers reasonable access to their data; and undertake consumer education efforts to improve consumers’ understanding of how companies collect, use, and share their data.

²⁹² See *infra* at Section IV.C.1.b.(v).

²⁹³ See *infra* at Section IV.D.2.b.

Commenters offered proposals for how to achieve greater transparency and sought clarification on how they should implement these elements of the framework. Although the Commission adopts the proposed framework's transparency principle without change, it clarifies the application of the framework in response to these comments, as discussed below.

1. PRIVACY NOTICES

Proposed Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

The preliminary staff report highlighted the consensus among roundtable participants that most privacy policies are generally ineffective for informing consumers about a company's data practices because they are too long, are difficult to comprehend, and lack uniformity.²⁹⁴ While acknowledging privacy policies' current deficiencies, many roundtable participants agreed that the policies still have value – they provide an important accountability function by educating consumer advocates, regulators, the media, and other interested parties about the companies' data practices.²⁹⁵ Accordingly, Commission staff called on companies to provide clear and concise descriptions of their data collection and use practices. Staff further called on companies to standardize the format and the terminology used in privacy statements so that consumers can compare the data practices of different companies and exercise choices based on privacy concerns, thereby encouraging companies to compete on privacy.

Despite the consensus from the roundtables that privacy statements are not effective at communicating a company's data collection and use practices to consumers, one commenter disagreed that privacy notices need to be improved.²⁹⁶ Another commenter pointed out that providing more granular information about data collection and use practices could actually increase consumer confusion by overloading the consumer with information.²⁹⁷ Other industry commenters highlighted the work they have undertaken since the preliminary staff report to improve their own privacy statements.²⁹⁸

Many consumer groups supported staff's call to standardize the format and terminology used in privacy statements so that consumers could more easily compare the practices of different companies.²⁹⁹ Some commenters suggested a “nutrition label” approach for standardizing the format of privacy policies and cited

294 Recent research and surveys suggests that many consumers (particularly among lower income brackets and education levels) do not read or understand privacy policies, thus further heightening the need to make them more comprehensible. Notably, in a survey conducted by Zogby International, 93% of adults – and 81% of teens – indicated they would take more time to read terms and conditions for websites if they were shorter and written in clearer language. See *Comment of Common Sense Media*, cmt. #00457, at 1.

295 See *Comment of AT&T, Inc.*, cmt. #00420, at 17; *Comment of Center for Democracy & Technology*, cmt. #00469, at 24.

296 See *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 22.

297 See *Comment of United States Council for International Business*, cmt. #00366, at 3.

298 See *Comment of Google Inc.*, cmt. #00417, at 1; *Comment of Facebook, Inc.*, cmt. #00413, at 9; *Comment of AT&T Inc.*, cmt. #00420, at 24.

299 See *Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 15-16; *Comment of Consumer Federation of America*, cmt. #00358, at 16; *Comment of Consumer Watchdog*, cmt. #00402, at 2.

research underway in this area.³⁰⁰ Another suggested the “form builder” approach used for GLBA Short Notices to standardize the format of privacy notices outside the financial context.³⁰¹ One consumer group called for standardization of specific terms like “affiliate” and “anonymize” so that companies’ descriptions of their data practices are more meaningful.³⁰² A wide range of commenters suggested that different industry sectors come together to develop standard privacy notices.³⁰³ Other commenters opposed the idea of mandated standardized notices, arguing that the Commission should require only that privacy statements be clear and in plain language. These commenters stated that privacy statements need to take into account differences among business models and industry sectors.³⁰⁴

Privacy statements should account for variations in business models across different industry sectors, and prescribing a rigid format for use across all sectors is not appropriate. Nevertheless, the Commission believes that privacy statements should contain some standardized elements, such as format and terminology, to allow consumers to compare the privacy practices of different companies and to encourage companies to compete on privacy. Accordingly, Commission calls on industry sectors to come together to develop standard formats and terminology for privacy statements applicable to their particular industries. The Department of Commerce will convene multi-stakeholder groups to work on privacy issues; this could be a useful venue in which industry sectors could begin the exercise of developing more standardized, streamlined privacy policies.

Machine-readable policies,³⁰⁵ icons, and other alternative forms of providing notice also show promise as tools to give consumers the ability to compare privacy practices among different companies.³⁰⁶ In response to the preliminary staff report’s question on machine-readable policies, commenters agreed that such policies could improve transparency.³⁰⁷ One commenter proposed combining the use of machine-readable policies with icons and standardized policy statements (e.g., “we collect but do not share consumer data

300 See *Comment of Consumer Watchdog*, cmt. #00402, at 2; *Comment of Consumer Federation of America*, cmt. #00358, at 16; see also *Comment of Lorrie Faith Cranor*, cmt. #00453, at 2 n.7 (discussing P3P authorizing tools that enable automatic generation of “nutrition label” privacy notices).

301 See *Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 16.

302 See *Comment of Electronic Frontier Foundation*, cmt. #00400, at 6.

303 See *Comment of General Electric*, cmt. #00392, at 2; *Comment of the Information Commissioner’s Office of the UK*, cmt. #00249, at 4; *Comment of Consumers Union*, cmt. #00362, at 15-16; *Comment of Facebook, Inc.*, cmt. #00413, at 9.

304 See *Comment of AT&T Inc.*, cmt. #00420, at 25; *Comment of eBay*, cmt. #00374, at 10; *Comment of National Cable & Telecommunications Ass’n*, cmt. #00432, at 29; *Comment of Retail Industry Leaders Ass’n*, cmt. #00352, at 12; *Comment of Microsoft Corp.*, cmt. #00395, at 15.

305 A machine-readable privacy policy is a statement about a website’s privacy practices – such as the collection and use of data – written in a standard computer language (not English text) that software tools such as consumer’s web browser can read automatically. For example, when the browser reads a machine-readable policy, the browser can compare the policy to the consumer’s browser privacy preferences, and can inform the consumer when these preferences do not match the practices of the website he is visiting. If the consumer decides he does not want to visit websites that sell information to third parties, he might set up a rule that recognizes that policy and blocks such sites or display a warning upon visiting such a site. Machine-readable language will be the subject of an upcoming summit. See White House, National Archives & Records Administration, *Informing Consumers Through Smart Disclosures* (Mar. 1, 2012), available at http://www.nist.gov/ineap/upload/Summit_Invitation_to_Agencies_FINAL.pdf (describing upcoming summit).

306 Likewise, new tools like privacyscore.com may help consumers more readily compare websites’ data practices. See Tanzina Vega, *A New Tool in Protecting Online Privacy*, N.Y. TIMES, Feb. 12, 2012, available at <http://mediadecoder.blogs.nytimes.com/2012/02/12/a-new-tool-in-protecting-online-privacy/?scp=2&sq=privacy&st=cse>.

307 *Comment of Phorm Inc.*, cmt. #00353, at 9; *Comment of Lorrie Faith Cranor*, cmt. #00453, at 6.

with third parties”) to simplify privacy decision-making for consumers.³⁰⁸ Other commenters described how icons work or might work in different business contexts. One browser company described efforts underway to develop icons that might be used to convey information, such as whether a consumer’s data is sold or may be subject to secondary uses, in a variety of business contexts.³⁰⁹ Representatives from online behavioral advertising industry groups also described their steps in developing and implementing an icon to communicate that online behavioral advertising may be taking place.³¹⁰

Commenters also discussed the particular challenges associated with providing notice in the mobile context, noting the value of icons, summaries, FAQs, and videos.³¹¹ Indeed, some work already has been done in this area to increase the transparency of data practices. For example, the advocacy organization Common Sense Media reviews and rates mobile apps based on a variety of factors including privacy³¹² and a platform provider uses an icon to signal to consumers when a mobile application is using location information.³¹³ In addition, CTIA – a wireless industry trade group – in conjunction with the Entertainment Software Rating Board, recently announced plans to release a new rating system for mobile apps.³¹⁴ This rating system, which is based on the video game industry’s model, will use icons to indicate whether specific apps are appropriate for “all ages,” “teen,” or only “adult” audiences. The icons will also detail whether the app shares consumers’ personal information. Noting the complexity of the mobile ecosystem, which includes device manufacturers, operating system providers, mobile application developers, and wireless carriers, some commenters called for public workshops to bring together different stakeholders to develop a uniform approach to icons and other methods of providing notice.³¹⁵ Also, as noted above, the Mobile Marketing Association has released its Mobile Application Privacy Policy.³¹⁶

The Commission appreciates the complexities of the mobile environment, given the multitude of different entities that want to collect and use consumer data and the small space available for disclosures

308 *Comment of Lorrie Faith Cranor*, cmt. #00453, at 6 (explaining how icons combined with standard policies might work: “For example, a type I policy might commit to not collecting sensitive categories of information and not sharing personal data except with a company’s agents, while a type II policy might allow collection of sensitive information but still commit to not sharing them, a type III policy might share non-identified information for behavioral advertising, and so on. Companies would choose which policy type to commit to. They could advertise their policy type with an associated standard icon, while also providing a more detailed policy. Users would be able to quickly determine the policy for the companies they interact with.”).

309 *Comment of Mozilla*, cmt. #00480, at 12.

310 *Comment of American Ass’n of Advertising Agencies, American Advertising Federation, Ass’n of National Advertisers, Direct Marketing Ass’n, Inc., and Interactive Advertising Bureau*, cmt. #00410 at 2-3; *Comment of Digital Marketing Alliance*, cmt. #00449, at 18-24; *Comment of Evidon*, cmt. #00391, at 3-6; *Comment of Internet Advertising Bureau*, cmt. #00388, at 4.

311 *Comment of General Electric*, cmt. #00392, at 1-2; *Comment of CTIA - The Wireless Ass’n*, cmt. #00375, at 2-3; *Comment of Mozilla*, cmt. #00480, at 12.

312 See Common Sense Media, App Reviews, <http://www.common sense media.org/app-reviews>.

313 See Letter from Bruce Sewell, General Counsel & Senior Vice President of Legal and Governmental Affairs, Apple, to Hon. Edward J. Markey, U.S. House of Representatives (May 6, 2011), *available at* http://robert.accettura.com/wp-content/uploads/2011/05/apple_letter_to_ejm_05.06.11.pdf.

314 See Press Release, CTIA – The Wireless Ass’n, CTIA – The Wireless Ass’n to Announce Mobile Application Rating System with ESRB (Nov. 21, 2011), *available at* <http://www.ctia.org/media/press/body.cfm/prid/2145>.

315 *Comment of Consumer Federation of America*, cmt. #00358, at 16; *Comment of GSMA*, cmt. #00336, at 10.

316 Although this effort is promising, more work remains. The Mobile Marketing Association’s guidelines are not mandatory and there is little recourse against companies who elect not to follow them. More generally, there are too few players in the mobile ecosystem who are committed to self-regulatory principles and providing meaningful disclosures and choices.

on mobile screens. These factors increase the urgency for the companies providing mobile services to come together and develop standard notices, icons, and other means that the range of businesses can use to communicate with consumers in a consistent and clear way.

To address this issue, the Commission notes that it is currently engaged in a project to update its existing business guidance about online advertising disclosures.³¹⁷ In conjunction with this project, Commission staff will host a workshop later this year.³¹⁸ One of the topics to be addressed is mobile privacy disclosures: How can these disclosures be short, effective, and accessible to consumers on small screens? The Commission hopes that the discussions at the workshop will spur further industry self-regulation in this area.

Final Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

2. ACCESS

Proposed Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

There was broad agreement among a range of commenters that consumers should have some form of access to their data. Many of these commenters called for flexibility, however, and requested that access rights be tiered according to the sensitivity and intended use of the data at issue.³¹⁹ One commenter argued that access rights should be limited to sensitive data, such as financial account information, because a broader access right would be too costly for offline retailers.³²⁰ Some companies and industry representatives supported providing consumers full access to data that is used to deny benefits; several commenters affirmed the significance of the FCRA in providing access to information used for critical decisionmaking. For other less sensitive data, such as marketing data, they supported giving consumers a general notice describing the types of data they collect and the ability to suppress use of the data for future marketing.³²¹

One commenter raised concerns about granting access and correction rights to data files used to prevent fraudulent activity, noting that such rights would create risks of fraud and identity theft. This commenter also stated that companies would need to add sensitive identifying information to their marketing databases in order to authenticate a consumer's request for information, and that the integration of multiple databases would raise additional privacy and security risks.³²²

³¹⁷ See Press Release, FTC, FTC Seeks Input to Revising its Guidance to Business About Disclosures in Online Advertising (May 26, 2011), *available at* <http://www.ftc.gov/opa/2011/05/dotcom.shtm>.

³¹⁸ See Press Release, FTC, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012 (Feb. 29, 2012), *available at* <http://www.ftc.gov/opa/2012/02/dotcom.shtm>.

³¹⁹ *Comment of Intuit, Inc.*, cmt. #00348, at 12; *Comment of eBay*, cmt. #00374, at 10; *Comment of IBM*, cmt. #00433, at 3; *Comment of Consumers Union*, cmt. #00362, at 16.

³²⁰ *Comment of Meijer*, cmt. #00416, at 7.

³²¹ *Comment of Intel Corp.*, cmt. #00246, at 8; *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 8; *Comment of Experian*, cmt. #00398, at 11.

³²² *Comment of Experian*, cmt. #00398, at 10-11.

A number of commenters raised issues about the costs associated with providing access. One company suggested that access rights be flexible, taking into account the company's existing data infrastructure.³²³ Others argued that access be granted only to consumer information that is "reasonably accessible in the course of business"³²⁴ and one commenter said that companies should be able to charge for providing access where there are costs associated with retrieving and presenting data.³²⁵

Commenters also asserted that companies should tell consumers the entities with which their data has been shared.³²⁶ Citing California's "Shine the Light" law, one commenter stated that companies should not only identify the third parties with which they share consumer data but should also disclose how the third parties use the data for marketing.³²⁷ Another commenter pointed out that many marketers do not maintain records about data sold to other companies on an individual basis. Thus, marketers have the ability to identify the companies to which they have sold consumer data in general, but not the third parties with which they may have shared the information about any individual consumer.³²⁸

Some comments reflect support for requiring companies to identify for consumers the sources of data collected about them so that consumers can correct erroneous data at the source, if appropriate.³²⁹ One commenter noted that the DMA self-regulatory guidelines currently require that a marketer identify the sources of data maintained about consumers.³³⁰

The Commission agrees with the commenters who stated that consumer access should be proportional to the sensitivity and the intended use of the data at issue. Indeed, the comments generally support treating access in accordance with three categories that reflect different levels of data sensitivity: (1) entities that maintain data for marketing purposes; (2) entities subject to the FCRA; and (3) entities that may maintain data for other, non-marketing purposes that fall outside of the FCRA.

At one side of the spectrum are companies that maintain data for marketing purposes. For data used solely for marketing purposes, the Commission agrees with the commenters who stated that the costs of providing individualized access and correction rights would likely outweigh the benefits. The Commission continues to support the idea of businesses providing consumers with access to a list of the categories of consumer data they hold, and the ability to suppress the use of such data for marketing. This approach

323 *Comment of AT&T Inc.*, cmt. #00420, at 28-29.

324 *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 3; *Comment of Yahoo!, Inc.*, cmt. #00444, at 20; *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 5-6.

325 *Comment of U.S. Council for International Business*, cmt. #00366, at 3.

326 *Comment of Catalog Choice*, cmt. #00473, at 8-9; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 5.

327 *See Comment of Catalog Choice*, cmt. #00473, at 20. Under this law, businesses, upon request, must provide their customers, free of charge and within 30 days: (1) a list of the categories of personal information disclosed by the business to third parties for the third parties' marketing purposes, (2) the names and addresses of all of the third parties that received personal information from the business in the preceding calendar year, (3) and if the nature of the third parties' business cannot reasonably be determined from the third parties' name, examples of the products or services marketed by the third party. Cal. Civ. Code § 1798.83.

328 *Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7.

329 *Comment of Reputation.com, Inc.*, cmt. #00385, at 11-12; *see also Comment of Center for Democracy & Technology*, cmt. #00469, at 25.

330 *Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7.

will provide consumers with an important transparency tool without imposing significant new costs for businesses.³³¹

The Commission does, however, encourage companies that maintain consumer data for marketing purposes to provide more individualized access when feasible. One example of an innovation in this area is the advertising preference managers that companies such as Google and Yahoo! have implemented. Yahoo!, for example, offers consumers, through its Ad Interest Manager, the ability to access the specific interest categories that Yahoo! associates with individual consumers and allows them to suppress marketing based on some or all of these categories. Using this service, an elementary school teacher who conducted online research for pet food during the time she owned a dog, but continues to receive advertisements for dog food, could remove herself from the “Consumer Packaged Goods > Pets and Animals > Food and Supplies” category while still opting to remain part of the “Life Stages > Education > K to 12” category.³³² The Commission supports efforts by companies to provide consumers with these types of granular choices to give them greater control over the marketing materials and solicitations they receive.

At the other end of the spectrum are companies that assemble and evaluate consumer information for use by creditors, employers, insurance companies, landlords, and other entities involved in eligibility decisions affecting consumers. The preliminary staff report cited the FCRA as an important tool that provides consumers with the right to access their own data that has been used to make such decisions, and if it is erroneous, to correct it. Several commenters echoed this view.³³³

The FCRA recognizes the sensitivity of the data that consumer reporting agencies maintain and the ways in which various entities use it to evaluate whether a consumer is able to participate in so many activities central to modern life; therefore, it provides consumers with access and correction rights for information contained in consumer reports. Pursuant to the FCRA, consumer reporting agencies are required to disclose to consumers, upon request, all items in the consumer’s file, no matter how or where they are stored, as well as the entities with which the consumer reporting agency shared the information in a consumer’s report. When consumers identify information in their report that is incomplete or inaccurate, and report it to a consumer reporting agency, the agency must investigate and correct or delete such information in certain circumstances.

As more and more consumer data becomes available from a variety of sources, companies are increasingly finding new opportunities to compile, package, and sell that information. In some instances, companies could be compiling and selling this data to those who are making decisions about a consumer’s eligibility for credit, insurance, employment, and the like. To the extent companies are assembling data and marketing or selling it for such purposes, they are subject to the FCRA. For example, companies that compile social media information and provide it to employers for use in making hiring decisions are consumer reporting

331 As discussed above, in most cases the framework does not require companies to provide consumer choice for first-party marketing, although first parties may choose to provide such choice to meet consumer demand. Outside of the first-party marketing context, however, companies should provide consumers with the ability to suppress the use of their data for marketing.

332 See Yahoo!, Ad Interest Manager, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting.

333 *Comment of Consumer Data Industry Ass’n*, cmt. #00363, at 4 - 5; *Comment of Experian*, cmt. #00398, at 10.

agencies and thus required to provide consumers with access and correction rights under the FCRA.³³⁴ These companies would also be required to inform employers about their FCRA obligation to provide adverse action notices when, for example, employment is denied.

Even if a company is not compiling and sharing data for the specific purpose of making employment, credit, or insurance eligibility decisions, if the company has reason to believe the data will be used for such purposes, it would still be covered by the FCRA. For example, recently, the Commission issued warning letters to the developers of mobile apps that compiled public record information on individuals and created apps for the purposes of learning information about friends, co-workers, neighbors, or potential suitors.³³⁵ The Commission noted that if these apps marketed their services for employment purposes or otherwise had reason to believe that they were being used for employment purposes, the FCRA requirements would apply.

Finally, some businesses may maintain and use consumer data for purposes that do not fall neatly within either the FCRA or marketing categories discussed above. These businesses may encompass a diverse range of industry sectors. They may include businesses selling fraud prevention or risk management services, in order to verify the identities of customers. They may also include general search engines, media publications, or social networking sites. They may include debt collectors trying to collect a debt. They may also include companies collecting data about how likely a consumer is to take his or her medication, for use by health care providers in developing treatment plans.³³⁶

For these entities, the Commission supports the sliding scale approach, which several commenters endorsed,³³⁷ with the consumer's ability to access his or her own data scaled to the use and sensitivity of the data. At a minimum, these entities should offer consumers access to (1) the types of information the companies maintain about them;³³⁸ and (2) the sources of such information.³³⁹ The Commission believes that requiring companies to identify data sources would help consumers to correct erroneous information at the source. In appropriate circumstances the Commission urges companies to provide the names of the third parties with whom consumer information is shared.

In instances where data is more sensitive or may affect benefits, more individualized notice, access, and correction rights may be warranted. For example, if a company denies services to a consumer because it could not verify the consumer's identity, it may be appropriate for the company to disclose the name of the identity verification service used. This will allow the consumer to contact the data source, which can then provide the consumer with access to the underlying information, as well as any appropriate remedies, such

334 15 U.S.C. §§ 1681g-1681h. See Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy and Identity Prot., FTC, to Renee Jackson, Counsel for Social Intelligence Corp., (May 9, 2011) (closing letter), *available at* <http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf>.

335 See Press Release, FTC, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), *available at* <http://www.ftc.gov/opa/2012/02/mobileapps.shtm> (describing warning letters sent by the FTC to Everify, Inc., InfoPay, Inc., and Intelligator, Inc. on Jan. 25, 2012).

336 See Laura Landro, *Many Pills, Many Not Taken*, WALL ST. J., Oct. 10, 2011, *available at* <http://online.wsj.com/article/SB10001424052970203388804576616882856318782.html>.

337 *Comment of Consumers Union*, cmt. #00362, at 16; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 7; *Comment of Microsoft Corp.*, cmt. #00395, at 15-16.

338 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at Ex. A.

339 *Comment of Reputation.com, Inc.*, cmt. #00385, at 11-12. Of course, First Amendment protections would apply to journalists' sources, among other things, and the Commission's recommendations are not intended to apply in that area.

as the ability to correct the information.³⁴⁰ To ensure that the consumer knows that she has been denied a benefit based on her own data, as a best practice the company should notify the consumer of the denial and the information on which the denial was based.

Verifying the identity of users who seek access to their own information is an important consideration and should be approached from a risk management perspective, focusing on the likelihood of and potential harm from misidentification. Indeed, in the example of identity verification services described above, one would not want a criminal to be able to “correct” his or her own truthful data, and it would be appropriate to require somewhat more stringent safeguards and proof of identity before allowing access and correction. Certainly, consumer reporting agencies have developed procedures allowing them to verify the identity of requesting consumers using the multiple pieces of information they have about consumers to match information provided by the requesting consumer. Companies engaged in providing data for making eligibility determinations should develop best practices for authenticating consumers for access purposes.

On the other hand, the significantly reduced risks associated with providing the wrong person’s information contained in a marketing database that contains no sensitive information may justify less stringent authentication procedures.³⁴¹ As with other issues discussed in this Report, reasonableness should be the touchstone: the degree of authentication employed should be tied to the sensitivity of the information maintained and how such information is used.

a. Special Access Mechanism for Data Brokers

Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual’s identity, differentiating records, marketing products, and preventing financial fraud. Several commenters noted the lack of transparency about the practices of these entities, which often have a wealth of information about consumers but never interact directly with them.³⁴² Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.³⁴³ One commenter noted that data brokers may sell data to employers, background screeners, and law enforcement, among others, without the consumer’s knowledge.³⁴⁴ The Commission has monitored data brokers since the 1990s, hosting workshops, drafting reports, and testifying before Congress about

340 As noted above, companies should pay close attention to the types of eligibility determinations being made to ensure they comply with the FCRA, if warranted.

341 One commenter noted that when organizations collect and maintain sensitive information about individuals, such as for banking or issuance of credit, they will ask for authenticating information before an individual can access those records. This same commenter then stated that organizations holding less sensitive data may not require similarly rigorous authentication. *See Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7 n.6.

342 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 3; *Comment of Consumers Union*, cmt. #00362, at 11.

343 *See Comment of Consumer Federation of America*, cmt. #00358, at 17.

344 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 8.

the privacy implications of data brokers' practices.³⁴⁵ Following a Commission workshop, the data broker industry created the Individual References Services Group (IRSG), a self-regulatory organization for certain data brokers.³⁴⁶ Although industry ultimately terminated this organization, a series of public breaches – including one involving ChoicePoint – led to renewed scrutiny of the practices of data brokers.³⁴⁷ And, indeed, there have been few broad-based efforts to implement self-regulation in this area in the recent past.

The access rights discussed above will help to improve the transparency of companies' data practices generally, whether or not they have a direct consumer interface. Because most data brokers are invisible to consumers, however, the Commission makes two additional recommendations as to these entities.

First, since 2009, the Commission has supported legislation giving access rights to consumers for information held by data brokers. During the 111th Congress, the House approved a bill that included provisions to establish a procedure for consumers to access information held by data brokers.³⁴⁸ To improve the transparency of this industry's practices, the Commission has testified in support of the goals of this legislation³⁴⁹ and continues to support legislation in this area.³⁵⁰

Second, the Commission recommends that the data broker industry explore the idea of creating a centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options.³⁵¹ This website will improve transparency and give consumers control over the data practices of companies that maintain and share data about them for marketing purposes. It can also provide consumer-facing entities such as retailers a means for ensuring that the information brokers from which they purchase "enhancement" information have instituted appropriate transparency and control mechanisms. Indeed, the

345 See, e.g., Prepared Statement of the FTC, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. (Mar. 10, 2005), available at <http://www.ftc.gov/os/testimony/050310idtheft.pdf>; see also FTC Workshop, *The Information Marketplace: Merging & Exchanging Consumer Data* (Mar. 13, 2001), available at <http://www.ftc.gov/bcp/workshops/informktplace/index.shtml>; FTC Workshop, *Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information* (June 18, 2003), available at <http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.shtml>.

346 See FTC, *Individual Reference Services, A Report to Congress* (1997), available at <http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm>.

347 See Prepared Statement of the FTC, *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint: Hearing before H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection, Comm. on Energy and Commerce*, 109th Cong. (Mar. 15, 2005), available at <http://www.ftc.gov/os/2005/03/050315protectingconsumerdata.pdf>.

348 Data Accountability and Trust Act, H.R. 2221, 111th Congress (as passed by House, Dec. 8, 2009).

349 See, e.g., Prepared Statement of the FTC, *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection*, 111th Cong. (May 5, 2009), available at <http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf>.

350 See, e.g., Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (May 4, 2011), available at <http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf>; Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (June 15, 2011), available at <http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf>; Prepared Statement of the FTC, *Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (June 29, 2011), available at <http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf>.

351 See *Comment of World Privacy Forum*, cmt. #00376, at 6; *Comment of Consumer Federation of America*, cmt. #00358, at 17-18.

consumer-facing entities could provide consumers with a link to the centralized mechanism, after having made sure that the data brokers from which they buy data participate in such a system. The Commission will discuss with relevant industry members how this mechanism could be developed and implemented voluntarily, in order to increase the transparency of their data practices and give consumers tools to opt out.³⁵²

b. Access to Teen Data

One commenter proposed that teens be given regular access to whether and how their data has been shared because of their particular vulnerability to ubiquitous marketing messages and heavy use of social media and mobile devices.³⁵³ Others noted that teens in particular may not appreciate the persistence and future effects of data that they post about themselves online and thus need a “right to be forgotten.” In its comment, the French Data Protection authority advocated the “right to be forgotten,” which would allow consumers to withdraw data posted online about themselves at any point, for all users, but noted in particular the need to have control over information posted in one’s youth.³⁵⁴ In the United States, legislation has been introduced that would give teens an eraser button, which would allow them to erase certain material on social networking sites.³⁵⁵

The Commission generally supports exploration of the idea of an “eraser button,” through which people can delete content that they post online. Many companies already offer this type of feature,³⁵⁶ which is consistent with the principles of data access and suppression. Such an “eraser button” could be particularly useful for teens who might not appreciate the long-term consequences of their data sharing. Teens tend to be more impulsive than adults³⁵⁷ and, as a result, may voluntarily disclose more information online than they should, leaving them vulnerable to identity theft or adversely affecting potential employment or college admissions opportunities. In supporting an eraser button concept, the Commission notes that such a feature

352 The current website of the Direct Marketing Association (DMA) offers an instructive model for such a mechanism. The DMA – which consists of data brokers, retailers, and others – currently offers a service through which consumers can opt out of receiving marketing solicitations via particular channels, such as direct mail, from DMA member companies. See DMAChoice, <http://www.dmachoice.org/dma/member/home.action>.

353 See *Comment of Consumers Union*, cmt. #00362, at 13; see also *Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 39.

354 *Comment of CNIL*, cmt. #00298, at 3.

355 Do Not Track Kids Act of 2011, H.R. 1895, 112th Congress (2011).

356 See Facebook, How Do I Remove a Wall Post or Story?, available at <http://www.facebook.com/help/?page=174851209237562>; LinkedIn, Privacy Policy, http://www.linkedin.com/static?key=privacy_policy.

357 See, e.g., FTC, *Transcript of March 17, 2010, Privacy Roundtable, Panel 3: Addressing Sensitive Information*, 208-215, available at http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_March2010_Transcript.pdf; see also Chris Hoofnagle, Jennifer King, Su Li, & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (Apr. 14, 2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.

would have to be carefully crafted in order to avoid implicating First Amendment concerns.³⁵⁸ It would also need to be technically feasible and proportional to the nature, sensitivity, and amount of data collected.

Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

3. CONSUMER EDUCATION

Proposed Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

In its preliminary report, FTC staff called for all stakeholders to accelerate their efforts to raise consumer awareness about data practices and to provide additional transparency tools to consumers. Staff pointed out that consumers need more education about the privacy implications of various data practices so that they can make informed decisions about the trade-offs involved. Staff posed questions about how the range of interested stakeholders – companies, industry associations, consumer groups, and government – can do a better job of informing consumers about privacy. Many commenters expressed general support for the notion that consumer education is a vital component of improving privacy protections for consumers.³⁵⁹ One commenter suggested that businesses use their creative talents to make privacy more accessible for consumers, and as support, pointed to its own privacy game.³⁶⁰ The game teaches players about privacy by inviting them to tour a virtual small town in which the buildings represent different parts of the commenter's privacy policy.

Over the last few years, a number of other companies and industry and consumer groups have stepped up their efforts to educate consumers about privacy and their privacy choices.³⁶¹ The Commission encourages more such efforts, with an eye toward developing clear and accessible messages that consumers will see and understand.

358 While consumers should be able to delete much of the information they place on a particular social media site, there may be First Amendment constraints to requiring third parties to delete the same information. In the FTC's recent proposed settlement with Facebook, the company agreed to implement measures designed to prevent any third party from accessing information under Facebook's control within a reasonable time period, not to exceed thirty days, from the time the user has deleted such information. See *In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), available at <http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf>.

359 See, e.g., *Comment of Intuit Inc.*, cmt. #00348, at 12; *Comment of AT&T Inc.*, cmt. #00420, at 30-31; *Comment of Consumers Union*, cmt. #00362, at 18.

360 *Comment of Zynga Inc.*, cmt. #00459, at 4.

361 See, e.g., Common Sense Media, App Reviews, <http://www.common sense media.org/app-reviews> (listing reviews that evaluate privacy and safety concerns posed by common mobile applications designed for children); Google, Ad Preferences, Frequently Asked Questions, <http://www.google.com/ads/preferences/html/faq.html>; Interactive Advertising Bureau, Privacy Matters Campaign, <http://www.iab.net/privacymatters/campaign.php>; Kashmir Hill, *Zynga's PrivacyVille – It's Not Fun, But It Gets the Job Done*, FORBES, July 8, 2011, available at <http://www.forbes.com/sites/kashmirhill/2011/07/08/zyngas-privacyville-its-not-fun-but-it-gets-the-job-done/>.

A range of commenters suggested that the FTC explicitly endorse or sponsor various private sector-led consumer education efforts.³⁶² The Commission certainly supports private sector education efforts, and encourages private sector entities to freely use the FTC's extensive consumer and business education materials, under their own branding.

For example, the FTC encourages businesses to use information from its OnGuardOnline.gov website, which aims to help people be safe, secure and responsible online. The OnGuardOnline.gov campaign is a partnership of 15 federal agencies. The site includes articles, videos, games and tutorials to teach home users, small businesses or corporate employees about privacy-related topics like using Wi-Fi networks, peer-to-peer file sharing, mobile apps, and online tracking. The OnGuard Online Blog provides the latest cybersecurity news and practical tips from the FTC and other federal agencies. The FTC publishes this blog regularly and encourages companies to copy and disseminate it. Additionally, the FTC has continued its own consumer education efforts in the privacy area. Over the last year, the Commission released consumer education materials on a variety of topics including: using Wi-Fi hot spots; managing browser and "Flash" cookies; understanding mobile privacy; and protecting against child identity theft.³⁶³

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

V. CONCLUSION

The final privacy framework set forth in this Report reflects the extensive record developed through the Commission's privacy roundtables as well as the over 450 public comments received in response to the proposed framework issued in December of 2010. The FTC recommends that Congress consider baseline privacy legislation while industry implements the final privacy framework through individual company initiatives and through strong and enforceable self-regulatory initiatives. As discussed throughout the report, there are a number of specific areas where policy makers have a role in assisting with the implementation of the self-regulatory principles that make up the privacy framework. Areas where the FTC will be active over the course of the next year include the following.

- ◆ **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.

³⁶² *Comment of United States Council for International Business*, cmt. #00366, at 4; *Comment of IMS Health*, cmt. #00380, at 5; *Comment of The Privacy Projects*, cmt. #00482, at 2-3.

³⁶³ FTC, *Wise Up About Wi-Fi: Tips for Using Public Wireless Networks* (2011), <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt193.shtm>; FTC, *Cookies: Leaving a Trail on the Web*, <http://onguardonline.gov/articles/0042-cookies-leaving-trail-web>; FTC, *Understanding Mobile Apps*, <http://onguardonline.gov/articles/0018-understanding-mobile-apps>; FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft*, (July 12, 2011), <http://www.ftc.gov/bcp/workshops/stolenfutures/>.

- ◆ **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures.³⁶⁴ As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.
- ◆ **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker.³⁶⁵ To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- ◆ **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.
- ◆ **Promoting enforceable self-regulatory codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

In all other areas, the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the privacy framework, to the extent they have not already done so. For its part, the FTC will focus its policy efforts on the five areas identified above, vigorously enforce existing laws, work with industry on self-regulation, and continue to target its education efforts on building awareness of existing data collection and use practices and the tools to control them.

³⁶⁴ See Press Release, FTC, FTC Seeks Input to Revising its Guidance to Businesses About Disclosures in Online Advertising (May 26, 2011), *available at* <http://www.ftc.gov/opa/2011/05/dotcom.shtm>.

³⁶⁵ See Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).

FTC Privacy Milestones

FTC Privacy Milestones

● Laws & Rules	● Workshops
● Cases	● Education
● Reports	

1970	Fair Credit Reporting Act enacted
1972	First Fair Credit Reporting Act (FCRA) case: <u>In the Matter of Credit Bureau of Lorain</u>
1975	FTC sues tax preparer for improperly using customers' information to market its loans: <u>FTC v. Beneficial Corporation</u>
1970s	FTC brings 15 additional enforcement actions against credit bureaus and report users
1983	First FCRA case against a nationwide credit bureau: <u>FTC v. TransUnion</u>
1985	FCRA sweep against users of consumer reports
1990	Commission staff issues comprehensive commentary on the FCRA
1991	FTC sues TRW for FCRA violations: <u>FTC v. TRW</u>
1992	FCRA sweep against employers using credit reports
1995	FTC sues Equifax for FCRA violations: <u>In the Matter of Equifax Credit Information Services</u>
1996	First major revision of the Fair Credit Reporting Act
	FTC sponsors workshop: <i>Consumer Privacy on the Global Information Infrastructure</i>
1997	First spam case: <u>FTC v. Nia Cano</u>
	FTC hosts traveling workshops to discuss revisions of FCRA
	FTC sponsors workshop: <i>Consumer Information Privacy</i>
	FTC issues <i>Individual Reference Services: A Federal Trade Commission Report to Congress</i>
1998	FTC issues <i>Privacy Online: A Federal Trade Commission Report to Congress</i>
1999	First case involving children's privacy: <u>In the Matter of Liberty Financial</u>
	First consumer privacy case: <u>In the Matter of GeoCities</u>
	FTC issues <i>Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress</i>
	FTC sponsors workshop: <i>Online Profiling</i>
	FTC launches ID Theft website: consumer.gov/idtheft and ID Theft Online Complaint Form
	FTC's 877-ID-THEFT consumer helpline established
2000	Children's Online Privacy Protection Rule (COPPA) goes into effect
	Gramm-Leach-Bliley Financial Privacy Rule goes into effect
	Three nationwide consumer reporting agencies pay \$2.5 million in civil penalties for FCRA violations: <u>US v. Equifax Credit Information Services</u> , <u>US v. TransUnion</u> , and <u>US v. Experian Information Solutions</u>
	First COPPA case: <u>FTC v. Toysmart.com</u>
	FTC issues <i>Online Profiling: A Federal Trade Commission Report to Congress</i>
	FTC issues <i>Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress</i>

FTC Privacy Milestones

continued

2001	FTC sponsors workshop: <i>The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues</i>
	FTC publishes ID Theft booklet for victims: <i>When Bad Things Happen to Your Good Name</i>
	COPPA Safe Harbor Program begins
	First civil penalty cases under COPPA: <u>US v. Looksmart</u> , <u>US v. Monarch Services</u> , <u>US v. Bigmailbox</u>
2002	FTC sponsors workshops: <i>The Information Marketplace: Merging and Exchanging Consumer Data</i> ; <i>Gramm-Leach-Bliley Educational Program on Financial Privacy</i> ; and <i>Get Noticed: Effective Financial Privacy Notices: An Interagency Workshop</i>
	FTC publishes ID Theft Affidavit
	First data security case: <u>In the Matter of Eli Lilly & Company</u>
	FTC settles data security charges related to Microsoft's Passport service: <u>In the Matter of Microsoft</u>
	FTC sponsors workshop: <i>Consumer Information Security Workshop</i>
	FTC issues report on <i>Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues</i>
	FTC launches 10-minute educational ID Theft video
2003	FTC distributes over 1 million ID Theft booklets for victims
	Fair and Accurate Credit Transactions Act (FACTA) passed
	National Do Not Call Registry goes into effect
	Gramm-Leach-Bliley Safeguards Rule goes into effect
	FTC sues companies for sharing students' survey data with commercial marketers: <u>In the Matter of Education Research Center of America and Student Marketing Group</u>
	Guess settles FTC data security charges: <u>In the Matter of Guess?</u>
	FTC issues <i>Technologies for Protecting Personal Information: A Staff Workshop Report</i>
2004	FTC sponsors workshops: <i>Technologies for Protecting Personal Information</i> ; <i>Spam Forum</i> ; and <i>Costs and Benefits Related To the Collection and Use of Consumer Information</i>
	CAN-SPAM Rule goes into effect
	CAN-SPAM Adult Labeling Rule goes into effect
	Free Annual Credit Report Rule goes into effect
	First spyware case: <u>FTC v. Seismic Entertainment</u>
	FTC charges company with exposing consumers' purchases: <u>In the Matter of MTS (dba Tower Records)</u>
	FTC charges company with renting consumer information it had pledged to keep private: <u>In the Matter of Gateway Learning</u>

- Laws & Rules ● Workshops
- Cases ● Education
- Reports

	FTC issues <i>The CAN-SPAM Act of 2003: National Do Not Email Registry: A Federal Trade Commission Report to Congress</i>
	FTC sponsors workshops: <i>Monitoring Software on Your PC: Spyware, Adware and Other Software</i> ; <i>Radio Frequency IDentification: Applications and Implications for Consumers</i> ; and <i>Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues</i>
	FTC publishes <i>The CAN-SPAM Act: A Compliance Guide for Business</i>
2005	FACTA Disposal Rule goes into effect
	FACTA Pre-Screen Opt Out Rule goes into effect
	National Do Not Call Registry tops 100 million phone numbers
	First Do Not Call enforcement action: <u>FTC v. National Consumer Council</u>
	First Do Not Call civil penalty action: <u>US v. Braglia Marketing</u>
	Highest civil penalty in a Do Not Call case: <u>US v. DirecTV</u> (\$5.3 million)
	First enforcement actions under Gramm-Leach-Bliley Safeguards Rule: <u>In the Matter of Sunbelt Lending</u> and <u>In the Matter of Nationwide Mortgage Group</u>
	First unfairness allegation in a data security case: <u>In the Matter of BJ's Wholesale Club</u>
	FTC issues <i>RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission</i>
	FTC issues <i>Spyware Workshop: Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff</i>
	FTC launches online safety website: OnGuardOnline.gov
2006	FACTA Rule Limiting Marketing Solicitations from Affiliates goes into effect
	Highest civil penalty in a consumer protection case: <u>US v. ChoicePoint</u> (\$10 million civil penalty for violations of FCRA as well as \$5 million redress for victims)
	First adware case: <u>In the Matter of Zango</u>
	Highest civil penalty to date in a COPPA case: <u>US v. Xanga</u> (\$1 million)
	FTC settles charges against a payment processor that had experienced the largest breach of financial data to date: <u>In the Matter of CardSystems Solutions</u>
	FTC issues <i>Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report</i>
	FTC sponsors workshop: <i>Protecting Consumers in the Next Tech-Ade</i>
	FTC launches national educational campaign on identity theft and publishes <i>Deter, Detect, Defend: Avoid ID Theft</i> brochure

FTC Privacy Milestones

continued

2007	First Disposal Rule case: <u>US v. American United Mortgage Company</u>
	Adult-oriented online social networking operation settles FTC charges; unwitting consumers pelted with sexually graphic pop-ups: <u>FTC v. Various (dba AdultFriendFinder)</u>
	FTC issues <i>Spam Summit: The Next Generation of Threats and Solutions: A Staff Report by the Federal Trade Commission's Division of Marketing Practices</i>
	FTC issues <i>Implementing the Children's Online Privacy Protection Act: A Federal Trade Commission Report to Congress</i>
	FTC co-chairs President's Identity Theft Task Force (with DOJ) and issues Strategic Plan
	FTC sponsors workshops: <i>Security in Numbers: SSNs and ID Theft</i> ; <i>Behavioral Advertising: Tracking, Targeting, and Technology</i> ; and <i>Spam Summit: The Next Generation of Threats and Solutions</i>
	FTC publishes <i>Protecting Personal Information: A Guide for Business</i> and launches interactive tutorial
2008	Highest civil penalty in a CAN-SPAM case: <u>US v. ValueClick</u> (\$2.9 million)
	FTC settles charges against data broker Lexis Nexis and retailer TJX related to the compromise of hundreds of thousands of consumers' information: <u>In the Matter of Reed Elsevier and Seisent</u> and <u>In the Matter of TJX Companies</u>
	FTC issues <i>Protecting Consumers in the Next Tech-age: A Report by the Staff of the Federal Trade Commission</i>
	FTC issues <i>Security In Numbers: Social Security Numbers and Identity Theft – A Federal Trade Commission Report Providing Recommendations On Social Security Number Use In the Private Sector</i>
	President's Identity Theft Task Force Report released
	FTC sponsors workshops: <i>Protecting Personal Information: Best Practices for Business</i> (Chicago, Dallas, and Los Angeles); <i>Pay on the Go: Consumers and Contactless Payment</i> , <i>Transatlantic RFID Workshop on Consumer Privacy and Data Security</i> ; and <i>Beyond Voice: Mapping the Mobile Marketplace</i>
	U.S. Postal Service sends FTC ID Theft prevention brochure to every household in the country
2009	Robocall Rule goes into effect
	Health Breach Notification Rule goes into effect
	First case alleging failure to protect employee information: <u>In the Matter of CVS Caremark</u>
	First cases alleging six companies violated the EU-US Safe Harbor Agreement: <u>In the Matter of World Innovators</u> , <u>In the Matter of ExpatEdge Partners</u> , <u>In the Matter of Onyx Graphics</u> , <u>In the Matter of Directors Desk</u> , <u>In the Matter of Progressive Gaitways</u> , and <u>In the Matter of Collectify</u>
	FTC issues <i>Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology</i>

- Laws & Rules
- Cases
- Reports
- Workshops
- Education

	FTC sponsors workshops: <i>Exploring Privacy: A Roundtable Series</i> ; <i>Protecting Personal Information: Best Practices for Business</i> (New York); and <i>Securing Personal Data in the Global Economy</i>
	FTC publishes <i>Net Cetera: Chatting with Kids About Being Online</i>
2010	FTC jointly publishes Model Privacy Form under the Gramm-Leach-Bliley Act
	National Do Not Call Registry tops 200 million phone numbers
	First data security case involving social media: <u>In the Matter of Twitter</u>
	First case shutting down a rogue ISP: <u>FTC v. Pricewert</u>
	First data security case against an online seal provider: <u>FTC v. ControlScan</u>
	Highest judgment in a spyware case: <u>FTC v. Innovative Marketing</u> (\$163 million)
	Largest FTC-state coordinated settlement on privacy: <u>FTC v. Lifelock</u>
	FTC conducts sweep against companies for exposure of employee and/or customer data on peer-to-peer (P2P) file-sharing networks
	FTC releases Preliminary FTC Staff Report <i>Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers</i>
	FTC sponsors <i>COPPA Rule Review Roundtable</i>
	FTC publishes <i>Peer-to-Peer File Sharing: A Guide for Businesses</i> ; <i>Medical Identity Theft: How to Minimize Your Risk</i> ; and <i>Copier Data Security: A Guide for Businesses</i>
	FTC distributes 6+ million printed copies of <i>Deter, Detect, Defend: Avoid ID Theft</i> brochures and 5+ million printed copies of <i>Net Cetera: Chatting with Kids About Being Online</i>
2011	FTC seeks comment on proposed changes to COPPA rule
	First case alleging substantive Safe Harbor violation and imposing privacy assessment program and audit requirements: <u>In the Matter of Google</u>
	First case against an online advertising network for offering deceptive privacy controls: <u>In the Matter of Chitika</u>
	First COPPA case against a mobile application developer: <u>US v. W3 Innovations</u>
	First case alleging unfairness based on default privacy settings: <u>FTC v. Frostwire</u>
	Largest FTC privacy case to date: <u>In the Matter of Facebook</u>
	FTC releases report <i>40 Years of Experience with the Fair Credit Reporting Act</i>
	FTC co-hosts <i>Stolen Futures: A Forum on Child ID Theft</i>
	FTC hosts <i>Face Facts: A Forum on Facial Recognition</i> Workshop
	FTC publishes <i>Tips for Using Public Wireless Networks</i>
	FTC publishes <i>Facts from the FTC: What You Should Know About Mobile Apps</i>
	FTC publishes <i>Online Safety for Teens and Tweens</i>

FTC Privacy Milestones

continued

●

Laws & Rules

●

Cases

●

Reports

●

Workshops

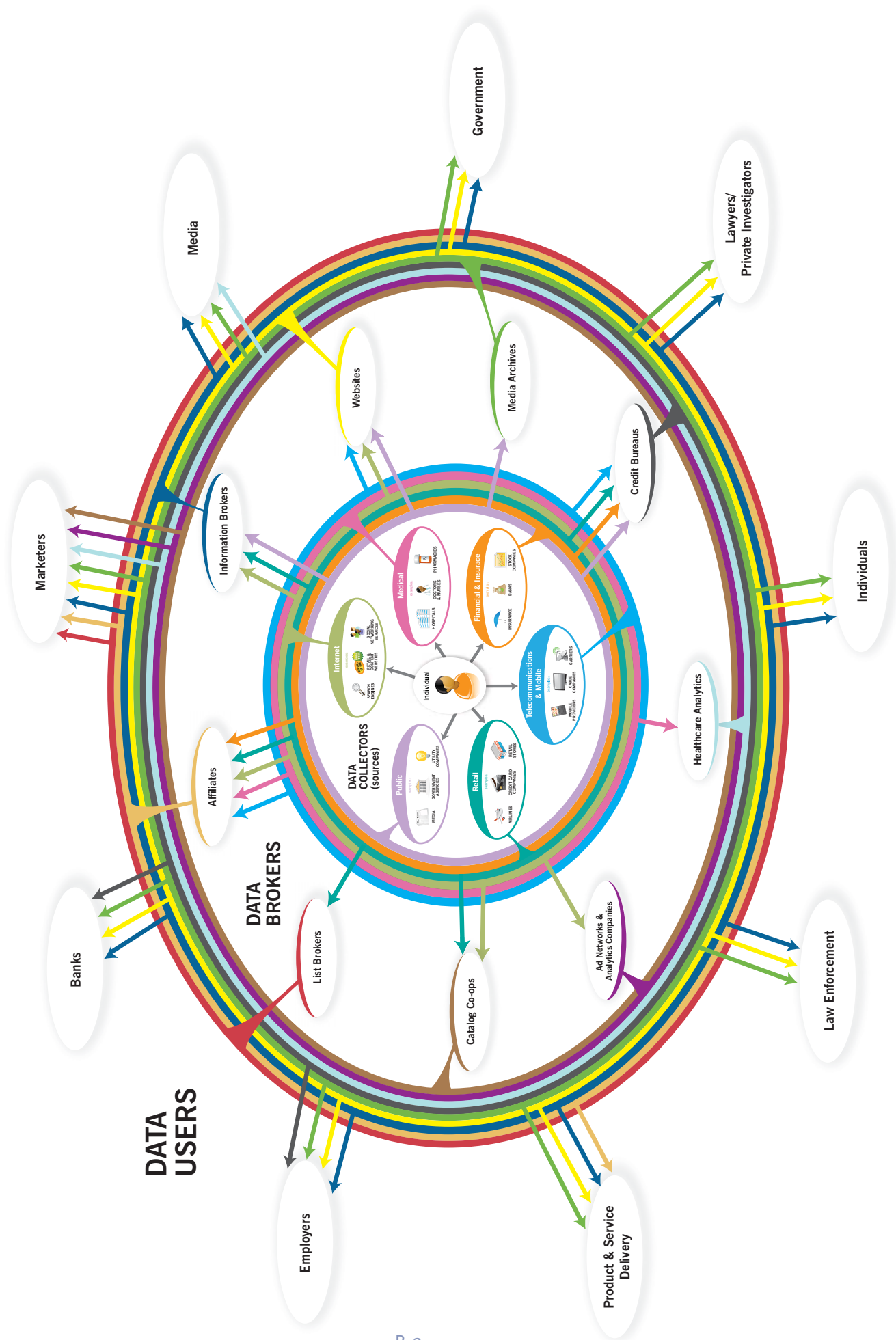
●

Education

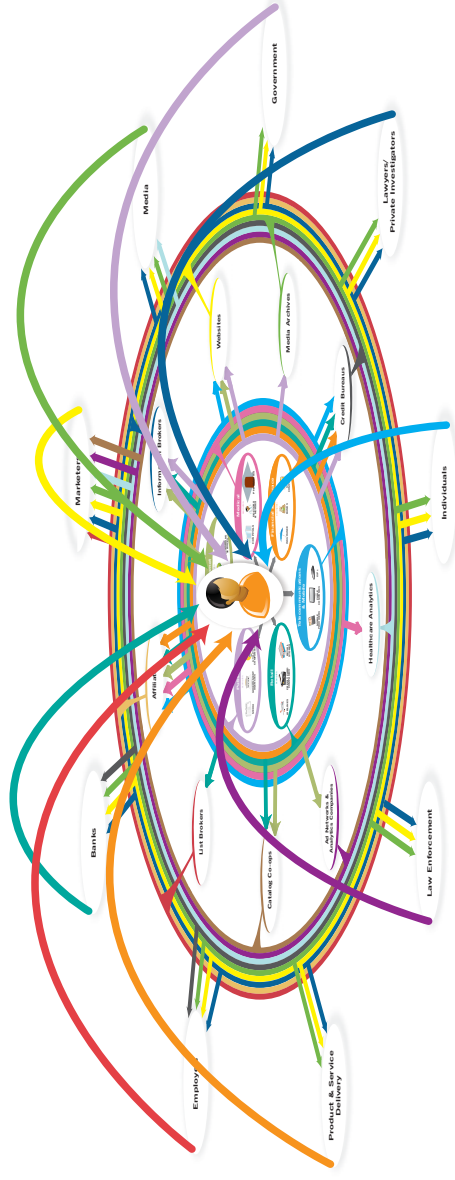
2012	FTC releases report <i>Using FACTA Remedies: An FTC Staff Report on a Survey of Identity Theft Victims</i>
	FTC releases report <i>Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing</i>
	FTC announces workshop: <i>Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments</i>
	FTC announces workshop to Explore Disclosures in Online and Mobile Media
	FTC publishes Blog Post: <i>FCRA & Mobile Apps: A Word of Warning</i>

Personal Data Ecosystem

Personal Data Ecosystem



DATA USES:



Examples of uses of consumer information in personally identifiable or aggregated form:

- Financial services, such as for banking or investment accounts
- Credit granting, such as for credit or debit cards; mortgage, automobile or specialty loans; automobile rentals; or telephone services
- Insurance granting, such as for health, automobile or life
- Retail coupons and special offers
- Catalog and magazine solicitations
- Web and mobile services, including content, e-mail, search, and social networking
- Product and service delivery, such as streaming video, package delivery, or a cable signal
- Attorneys, such as for case investigations
- Journalism, such as for fact checking
- Marketing, whether electronically, through direct mail, or by telephone
- Data brokers for aggregation and resale to companies and/or consumers
- Background investigations by employers or landlords
- Locating missing or lost persons, beneficiaries, or witnesses
- Law enforcement
- Research (e.g., health, financial, and online search data) by academic institutions, government agencies, and commercial companies
- Fraud detection and prevention
- Government benefits and services, such as licensing

Dissenting Statement of Commissioner J. Thomas Rosch

Introduction

I agree in several respects with what the “final” Privacy Report says. Specifically, although I disagree that the consumer has traditionally ever been given any “choice” about information collection practices (other than to “take-it-or-leave-it” after reviewing a firm’s privacy notice), I agree that consumers ought to be given a broader range of choices if for no other reason than to customize their privacy protection. However, I still worry about the constitutionality of banning take-it-or-leave-it choice (in circumstances where the consumer has few alternatives); as a practical matter, that prohibition may chill information collection, and thus impact innovation, regardless whether one’s privacy policy is deceptive or not.¹

I also applaud the Report’s recommendation that Congress enact “targeted” legislation giving consumers “access” to correct misinformation about them held by a data broker.² I also support the Report’s recommendation that Congress implement federal legislation that would require entities to maintain reasonable security and to notify consumers in the event of certain security breaches.³

Finally, I concur with the Report insofar as it recommends that information brokers who compile data for marketing purposes must disclose to consumers how they collect and use consumer data.⁴ I have long felt that we had no business counseling Congress or other agencies about privacy concerns without that information. Although I have suggested that compulsory process be used to obtain such information (because I am convinced that is the only way to ensure that our information is complete and accurate),⁵ a voluntary centralized website is arguably a step in the right direction.

Privacy Framework

My disagreement with the “final” Privacy Report is fourfold. First, the Report is rooted in its insistence that the “unfair” prong, rather than the “deceptive” prong, of the Commission’s Section 5 consumer protection statute, should govern information gathering practices (including “tracking”). “Unfairness” is an elastic and elusive concept. What is “unfair” is in the eye of the beholder. For example, most consumer advocacy groups consider behavioral tracking to be unfair, whether or not the information being tracked is personally identifiable (“PII”) and regardless of the circumstances under which an entity does the

1 *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (“Report”) at 50-52.

2 *Id.* at 14, 73.

3 *Id.* at 26. I also support the recommendation that such legislation authorize the Commission to seek civil penalties for violations. However, despite its bow to “targeted” legislation, the Report elsewhere counsels that the Commission support privacy legislation generally. *See, e.g., id.* at 16. To the extent that those recommendations are not defined, or narrowly targeted, I disagree with them.

4 *Id.* at 14, 68-70.

5 *See* J. Thomas Rosch, Comm’r, Fed. Trade Comm’n, Information and Privacy: In Search of a Data-Driven Policy, Remarks at the Technology Policy Institute Aspen Forum (Aug. 22, 2011), *available at* <http://www.ftc.gov/speeches/rosch/110822aspeninfospeech.pdf>.

tracking. But, as I have said, consumer surveys are inconclusive, and individual consumers by and large do not “opt out” from tracking when given the chance to do so.⁶ Not surprisingly, large enterprises in highly concentrated industries, which may be tempted to raise the privacy bar so high that it will disadvantage rivals, also support adopting more stringent privacy principles.⁷

The “final” Privacy Report (incorporating the preliminary staff report) repeatedly sides with consumer organizations and large enterprises. It proceeds on the premise that behavioral tracking is “unfair.”⁸ Thus, the Report expressly recommends that “reputational harm” be considered a type of harm that the Commission should redress.⁹ The Report also expressly says that privacy be the default setting for commercial data practices.¹⁰ Indeed, the Report says that the “traditional distinction between PII and non-PII has blurred,”¹¹ and it recommends “shifting the burdens away from consumers and placing obligations on businesses.”¹² To the extent the Report seeks consistency with international privacy standards,¹³ I would urge caution. We should always carefully consider whether each individual policy choice regarding privacy is appropriate for this country in all contexts.

That is not how the Commission itself has traditionally proceeded. To the contrary, the Commission represented in its 1980, and 1982, Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm.¹⁴ In other contexts, the Commission has tried, through its advocacy, to convince others that our policy judgments are sensible and ought to be adopted. And, as I stated in connection with the recent *Intel* complaint, in the competition context, one of the principal virtues

6 See Katy Bachman, *Study: Internet User Adoption of DNT Hard to Predict*, adweek.com, March 20, 2012, available at <http://www.adweek.com/news/technology/study-internet-user-adoption-dnt-hard-predict-139091> (reporting on a survey that found that what Internet users say they are going to do about using a Do Not Track button and what they are currently doing about blocking tracking on the Internet, are two different things); see also Concurring Statement of Commissioner J. Thomas Rosch, Issuance of Preliminary FTC Staff Report “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers” (Dec. 1, 2010), available at <http://www.ftc.gov/speeches/rosch/101201privacyreport.pdf>.

7 See J. Thomas Rosch, Comm’r, Fed. Trade Comm’n, Do Not Track: Privacy in an Internet Age, Remarks at Loyola Chicago Antitrust Institute Forum, (Oct. 14, 2011), available at <http://www.ftc.gov/speeches/rosch/111014-dnt-loyola.pdf>; see also Report at 9.

8 Report at 8 and n.37.

9 *Id.* at 2. The Report seems to imply that the Do Not Call Rule would support this extension of the definition of harm. See *id.* (“unwarranted intrusions into their daily lives”). However, it must be emphasized that the *Congress* granted the FTC underlying authority under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, to promulgate the Do Not Call provisions and other substantial amendments to the TSR. The Commission did not do so unilaterally.

10 *Id.*

11 *Id.* at 19.

12 *Id.* at 23, see also *id.* at 24.

13 *Id.* at 9-10. This does not mean that I am an isolationist or am impervious to the benefits of a global solution. But, as stated below, there is more than one way to skin this cat.

14 See Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), reprinted in International Harvester Co., 104 F.T.C. 949, 1070, 1073 (1984) (“Unfairness Policy Statement”) available at <http://www.ftc.gov/bcp/policystmt/ad-unfair.htm>; Letter from the FTC to Hon. Bob Packwood and Hon. Bob Kasten, Committee on Commerce, Science and Transportation, United States Senate, reprinted in FTC Antitrust & Trade Reg. Rep. (BNA) 1055, at 568-570 (“Packwood-Kasten letter”); and 15 U.S.C. § 45(n), which codified the FTC’s modern approach.

of applying Section 5 was that that provision was “self-limiting,” and I advocated that Section 5 be applied on a stand-alone basis only to a firm with monopoly or near-monopoly power.¹⁵ Indeed, as I have remarked, absent such a limiting principle, privacy may be used as a weapon by firms having monopoly or near-monopoly power.¹⁶

There does not appear to be any such limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report’s recommendations would instead apply to almost all firms and to most information collection practices. It would install “Big Brother” as the watchdog over these practices not only in the online world but in the offline world.¹⁷ That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).¹⁸ I would instead stand by what we have said and challenge information collection practices, including behavioral tracking, only when these practices are deceptive, “unfair” within the strictures of Section 5(n) and our commitments to Congress, or employed by a firm with market power and therefore challengeable on a stand-alone basis under Section 5’s prohibition of unfair methods of competition.

Second, the current self-regulation and browser mechanisms for implementing Do Not Track solutions may have advanced since the issuance of the preliminary staff Report.¹⁹ But, as the final Report concedes, they are far from perfect,²⁰ and they may never be, despite efforts to create a standard through the World Wide Web Consortium (“W3C”) for the browser mechanism.²¹

More specifically, as I have said before, the major browser firms’ interest in developing Do Not Track mechanisms begs the question of whether and to what extent those major browser firms will act strategically and opportunistically (to use privacy to protect their own entrenched interests).²²

In addition, the recent announcement by the Digital Advertising Alliance (DAA) that it will honor the tracking choices consumers make through their browsers raises more questions than answers for me. The Report is not clear, and I am concerned, about the extent to which this latest initiative will displace the standard-setting effort that has recently been undertaken by the W3C. Furthermore, it is not clear that all the interested players in the Do Not Track arena – whether it be the DAA, the browser firms, the W3C, or consumer advocacy groups – will be able to come to agreement about what “Do Not Track” even means.²³ It may be that the firms professing an interest in self-regulation are really talking about a “Do Not Target” mechanism, which would only prevent a firm from serving targeted ads, rather than a “Do Not Track”

15 See Concurring and Dissenting Statement of Commissioner J. Thomas Rosch, *In re Intel Corp.*, Docket No. 9341, (Dec. 16, 2009), available at <http://www.ftc.gov/os/adjpro/d9341/091216intelstatement.pdf>.

16 See Rosch, *supra* note 7 at 20.

17 See Report at 13.

18 Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312.

19 Report at 4, 52.

20 *Id.* at 53, 54; see *esp. id.* at 53 n.250.

21 *Id.* at 5, 54.

22 See Rosch, *supra* note 7 at 20-21.

23 Tony Romm, “What Exactly Does ‘Do Not Track’ Mean?,” Politico, Mar. 13, 2012, available at <http://www.politico.com/news/stories/0312/73976.html>; see also Report at 4 (DAA allows consumer to opt out of “targeted advertising”).

mechanism, which would prevent the collection of consumer data altogether. For example, the DAA's Self-Regulatory Principles for Multi-Site Data do not apply to data collected for "market research" or "product development."²⁴ For their part, the major consumer advocacy groups may not be interested in a true "Do Not Track" mechanism either. They may only be interested in a mechanism that prevents data brokers from compiling consumer profiles instead of a comprehensive solution. It is hard to see how the W3C can adopt a standard unless and until there is an agreement about what the standard is supposed to prevent.²⁵

It is also not clear whether or to what extent the lessons of the Carnegie Mellon Study respecting the lack of consumer understanding of how to access and use Do Not Track will be heeded.²⁶ Similarly, it is not clear whether and to what extent Commissioner Brill's concern that consumers' choices, whether it be "Do Not Collect" or merely "Do Not Target," will be honored.²⁷ Along the same lines, it is also not clear whether and to what extent a "partial" Do Not Track solution (offering nuanced choice) will be offered or whether it is "all or nothing." Indeed, it is not clear whether consumers can or will be given complete and accurate information about the pros and the cons of subscribing to Do Not Track before they choose it. I find this last question especially vexing in light of a recent study that indicated 84% of users polled prefer targeted advertising in exchange for free online content.²⁸

Third, I am concerned that "opt-in" will necessarily be selected as the *de facto* method of consumer choice for a wide swath of entities that have a first-party relationship with consumers but who can potentially track consumers' activities across unrelated websites, under circumstances where it is unlikely, because of the "context" (which is undefined) for such tracking to be "consistent" (which is undefined) with that first-party relationship:²⁹ 1) companies with multiple lines of business that allow data collection in different contexts (such as Google);³⁰ 2) "social networks," (such as Facebook and Twitter), which could potentially use "cookies," "plug-ins," applications, or other mechanisms to track a consumer's activities across

24 See *Self-Regulatory Principles for Multi-Site Data*, Digital Advertising Alliance, Nov. 2011, at 3, 10, 11, available at <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>; see also Tanzina Vega, *Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, New York Times, Feb. 26, 2012, available at <http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-web-tracking.html?pagewanted=all>.

25 See Vega, *supra* note 24.

26 "Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," Carnegie Mellon University CyLab, Oct. 31, 2011, available at http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf; see also *Search Engine Use 2012*, at 25, Pew Internet & American Life Project, Pew Research Center, Mar. 9, 2012, available at http://pewinternet.org/-/media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf ("[j]ust 38% of internet users say they are generally aware of ways they themselves can limit how much information about them is collected by a website").

27 See Julie Brill, Comm'r, Fed. Trade Comm'n, Big Data, Big Issues, Remarks at Fordham University School of Law (Mar. 2, 2012) available at <http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf>.

28 See Bachman, *supra* note 6.

29 Report at 41.

30 *Id.* Notwithstanding that Google's prospective conduct seems to fit perfectly the circumstances set forth on this page of the Report (describing a company with multiple lines of business including a search engine and ad network), where the Commission states "consumer choice" is warranted, the Report goes on to conclude on page 56 that Google's practices do not require affirmative express consent because they "currently are not so widespread that they could track a consumer's every movement across the Internet."

the Internet;³¹ and 3) “retargeters,” (such as Amazon or Pacers), which include a retailer who delivers an ad on a third-party website based on the consumer’s previous activity on the retailer’s website.³²

These entities might have to give consumers “opt-in” choice now or in the future: 1) regardless whether the entity’s privacy policy and notices adequately describe the information collection practices at issue; 2) regardless of the sensitivity of the information being collected; 3) regardless whether the consumer cares whether “tracking” is actually occurring; 4) regardless of the entity’s market position (whether the entity can use privacy strategically – *i.e.*, an opt-in requirement – in order to cripple or eliminate a rival); and 5) conversely, regardless whether the entity can compete effectively or innovate, as a practical matter, if it must offer “opt in” choice.³³

Fourth, I question the Report’s apparent mandate that ISPs, with respect to uses of deep packet inspection, be required to use opt-in choice.³⁴ This is not to say there is no basis for requiring ISPs to use opt-in choice without requiring opt-in choice for other large platform providers. But that kind of “discrimination” cannot be justified, as the Report says, because ISPs have “are in a position to develop highly detailed and comprehensive profiles of their customers.”³⁵ So does any large platform provider who makes available a browser or operating system to consumers.³⁶

Nor can that “discrimination” be justified on the ground that ISPs may potentially use that data to “track” customer behavior in a fashion that is contrary to consumer expectations. There is no reliable data establishing that most ISPs presently do so. Indeed, with a business model based on subscription revenue, ISPs arguably lack the same incentives as do other platform providers whose business model is based on attracting advertising and advertising revenue: ISPs assert that they track data only to perform operational and security functions; whereas other platform providers that have business models based on advertising revenue track data in order to maximize their advertising revenue.

What really distinguishes ISPs from most other “large platform providers” is that their markets can be highly concentrated.³⁷ Moreover, even when an ISP operates in a less concentrated market, switching costs can be, or can be perceived as being, high.³⁸ As I said in connection with the *Intel* complaint, a monopolist or near monopolist may have obligations which others do not have.³⁹ The only similarly situated platform provider may be Google, which, because of its alleged monopoly power in the search advertising market,

31 *Id.* at 40. *See also supra* note 30. That observation also applies to “social networks” like Facebook.

32 *Id.* at 41.

33 *See id.* at 60 (“Final Principle”).

34 *Id.* at 56 (“the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP’s interaction with a consumer, without express affirmative consent or more robust protection”).

35 *Id.*

36 *Id.*

37 Federal Communications Commission, *Connecting America: The National Broadband Plan, Broadband Competition and Innovation Policy*, Section 4.1, *Networks, Competition in Residential Broadband Markets* at 36, available at <http://www.broadband.gov/plan/4-broadband-competition-and-innovation-policy/>.

38 Federal Communications Commission Working Paper, *Broadband decisions: What drives consumers to switch – or stick with – their broadband Internet provider* (Dec. 2010), at 3, 8, available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1206/DOC-303264A1.pdf.

39 *See Rosch, supra* note 15.

has similar power. For any of these “large platform providers,” however, affirmative express consent should be required only when the provider *actually* wants to use the data in this fashion, not just when it *has the potential* to do so.⁴⁰

Conclusion

Although the Chairman testified recently before the House Appropriations Subcommittee chaired by Congresswoman Emerson that the recommendations of the final Report are supposed to be nothing more than “best practices,”⁴¹ I am concerned that the language of the Report indicates otherwise, and broadly hints at the prospect of enforcement.⁴² The Report also acknowledges that it is intended to serve as a template for legislative recommendations.⁴³ Moreover, to the extent that the Report’s “best practices” mirror the Administration’s privacy “Bill of Rights,” the President has specifically asked either that the “Bill of Rights” be adopted by the Congress or that they be distilled into “enforceable codes of conduct.”⁴⁴ As I testified before the same subcommittee, this is a “tautology;” either these practices are to be adopted voluntarily by the firms involved or else there is a federal requirement that they be adopted, in which case there can be no pretense that they are “voluntary.”⁴⁵ It makes no difference whether the federal requirement is in the form of enforceable codes of conduct or in the form of an act of Congress. Indeed, it is arguable that neither is needed if these firms feel obliged to comply with the “best practices” or face the wrath of “the Commission” or its staff.

40 See, e.g., Report at 56.

41 Testimony of Jon Leibowitz and J. Thomas Rosch, Chairman and Comm’r, FTC, *The FTC in FY2013: Protecting Consumers and Competition: Hearing on Budget Before the H. Comm. on Appropriations Subcomm. on Financial Services and General Government*, 112 th Cong. 2 (2012), text from CQ Roll Call, available from: LexisNexis® Congressional.

42 One notable example is found where the Report discusses the articulation of privacy harms and enforcement actions brought on the basis of *deception*. The Report then notes “[l]ike these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.” Report at 8. The accompanying footnote concludes that “even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm.” See also *infra* note 43.

43 *Id.* at 16 (“to the extent Congress enacts any of the Commission’s recommendations through legislation”); see also *id.* at 12-13 (“the Commission calls on Congress to develop baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate”).

44 See Letter from President Barack Obama, *appended to* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

45 See FTC Testimony, *supra* note 41.



)	
In the Matter of)	DOCKET NO. C-4426
)	
TRENDNET, INC.,)	
a corporation.)	
)	
)	

1. Respondent TRENDnet, Inc. (“TRENDnet” or “respondent”) is a California corporation with its principal office or place of business at 20675 Manhattan Place, Torrance, California 90501.
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

3. Respondent is a retailer that among other things, sells networking devices, such as routers, modems, and Internet Protocol (“IP”) cameras, to home users and to small- and medium-sized businesses. In 2010, respondent had approximately \$64 million in total revenue, and obtained approximately \$6.3 million of this amount from the sale of IP cameras. In 2011, respondent had approximately \$66 million in total revenue and obtained approximately \$5.28 million of this amount from the sale of its IP cameras. Similarly, in 2012, the company had approximately \$62 million in total revenue and obtained approximately \$7.4 million of this amount from the sale of IP cameras. During this time, the company had approximately 80 employees.

4. Respondent offers its IP cameras for consumers to conduct security monitoring of their homes or businesses, by accessing live video and audio feeds (“live feeds”) from their cameras over the Internet. In many instances, these cameras are marketed under the trade name “SecurView.” According to respondent, the IP cameras may be used to monitor “babies at home, patients in the hospital, offices and banks, and more.”
5. By default, respondent has required users to enter a user name and password (“login credentials”), in order to access the live feeds from their cameras over the Internet. In addition, since at least February 2010, respondent has provided users with a Direct Video Stream Authentication setting (“DVSA setting”), the same as or similar to the one depicted below. The DVSA setting allows users to turn off the login credentials requirement for their cameras, so that they can make their live feeds public. To remove the login credentials requirement, a user would uncheck the box next to the word “Enable,” and then “Apply” this selection.

TRENDnet Wireless Internet Camera Server TV-IP110W
Location: 2006/12/31 17:42:29

Basic » User

User Accounts

Administrator:	Password: <input type="text"/> Confirm Password: <input type="text"/> <input type="button" value="Modify"/>
General User:	User Name: <input type="text" value="user"/> Password: <input type="text"/> <input type="button" value="Add/Modify"/> UserList: <input type="text" value="user"/> <input type="button" value="Delete"/>
Guest:	User Name: <input type="text" value="guest"/> Password: <input type="text"/> <input type="button" value="Add/Modify"/> UserList: <input type="text" value="guest"/> <input type="button" value="Delete"/>

Direct Video Stream Authentication: ☒ Enable

Copyright © 2009 TRENDnet. All Rights Reserved.

6. Respondent also has provided software applications that enable users to access their live feeds from a mobile device (“mobile apps”), including its SecurView Mobile Android app, which respondent launched in January 2011, and its SecurView PRO Android app, which respondent launched in October 2012. Both apps require that a user enter login credentials the first time that the user employs the app on a particular mobile device. Both apps then store the user’s login credentials on that mobile device, so that the user will not be required to enter login credentials on that device in the future.

RESPONDENT'S STATEMENTS TO CONSUMERS

7. From at least January 1, 2010, until the present, in many instances, in marketing or offering for sale its IP cameras, respondent has:
- a. used the trade name SecurView:
 - i. in the product names and descriptions displayed on the cameras' packaging (*see, e.g.*, Exhs. A-J);
 - ii. in product descriptions on respondent's website and in other advertisements (*see, e.g.*, Exhs. K-L); and
 - iii. in the name of its SecurView Mobile and SecurView PRO Android apps, described in **Paragraph 6**.
 - b. described the IP cameras as "secure" or suitable for maintaining security, including through:
 - i. a sticker affixed to the cameras' packaging, the same as or similar to the one depicted below, which displays a lock icon and the word "security" (*see, e.g.*, Exhs. B, D, F-H, J);



- ii. a statement on the cameras' packaging that it may be used to "secure," or "protect" a user's home, family, property, or business (*see, e.g.*, Exhs. A, B, I); and
 - iii. product descriptions on respondent's website and in other advertisements (*see, e.g.*, Exhs. K-M);
- c. provided an authentication feature, which requires users to enter login credentials before accessing the live feeds from their IP cameras over the Internet; and

- d. provided the DVSA setting, described in **Paragraph 5**, which purports to allow users to choose whether login credentials will be required to access the live feeds from their IP cameras over the Internet.

**RESPONDENT'S FAILURE TO REASONABLY SECURE ITS IP CAMERAS
AGAINST UNAUTHORIZED ACCESS**

- 8. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to sensitive information, namely the live feeds from the IP cameras. Among other things:
 - a. since at least April 2010, respondent has transmitted user login credentials in clear, readable text over the Internet, despite the existence of free software, publicly available since at least 2008, that would have enabled respondent to secure such transmissions;
 - b. since January 2011, respondent has stored user login credentials in clear, readable text on a user's mobile device, despite the existence of free software, publicly available since at least 2008, that would have enabled respondent to secure such stored credentials;
 - c. since at least April 2010, respondent has failed to implement a process to actively monitor security vulnerability reports from third-party researchers, academics, or other members of the public, despite the existence of free tools to conduct such monitoring, thereby delaying the opportunity to correct discovered vulnerabilities or respond to incidents;
 - d. since at least April 2010, respondent has failed to employ reasonable and appropriate security in the design and testing of the software that it provided consumers for its IP cameras. Among other things, respondent, either directly or through its service providers, failed to:
 - i. perform security review and testing of the software at key points, such as upon the release of the IP camera or upon the release of software for the IP camera, through measures such as:
 - 1. a security architecture review to evaluate the effectiveness of the software's security;
 - 2. vulnerability and penetration testing of the software, such as by inputting invalid, unanticipated, or random data to the software;
 - 3. reasonable and appropriate code review and testing of the software to verify that access to data is restricted consistent with a user's privacy and security settings; and

- ii. implement reasonable guidance or training for any employees responsible for testing, designing, and reviewing the security of its IP cameras and related software.

RESPONDENT'S BREACH

9. As a result of the failures described in **Paragraph 8**, respondent has subjected its users to a significant risk that their sensitive information, namely the live feeds from its IP cameras, will be subject to unauthorized access. As a result of the failures described in **Paragraph 8(d)**, from approximately April 2010 until February 7, 2012, the DVSA setting, described in **Paragraph 5**, did not function properly for twenty models of respondent's IP cameras. (*See* Appendix A, listing the affected models.) In particular, the DVSA setting failed to honor a user's choice to require login credentials and allowed all users' live feeds to be publicly accessible, regardless of the choice reflected by a user's DVSA setting and with no notice to the user.
10. Hackers could and did exploit the vulnerability described in **Paragraph 9**, to compromise hundreds of respondent's IP cameras. Specifically, on approximately January 10, 2012, a hacker visited respondent's website and reviewed the software that respondent makes available for its cameras. The hacker was able to identify a web address that appeared to support the public sharing of users' live feeds, for those users who had made their feeds public. Because of the flaw in respondent's DVSA setting, however, the hacker could access all live feeds at this web address, without entering login credentials, even for users who had not made their feeds public. Thereafter, by typing the term "netcam" into a popular search engine that enables users to search for computers based on certain criteria, such as location or software, the hacker identified and obtained IP addresses for hundreds of respondent's IP cameras that could be compromised. The hacker posted information about the breach online; thereafter, hackers posted links to the live feeds for nearly 700 of respondent's IP cameras. Among other things, these compromised live feeds displayed private areas of users' homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities. The breach was widely reported in news articles online, many of which featured photos taken from the compromised live feeds or hyperlinks to access such feeds. Based on the cameras' IP addresses, news stories also depicted the geographical location (*e.g.*, city and state) of many of the compromised cameras.
11. Respondent learned of the breach on January 13, 2012, when a customer who had read about the breach contacted respondent's technical support staff to report the issue. Shortly thereafter, respondent made available new software to eliminate the vulnerability, and encouraged users to install the new software by posting notices on its website and sending emails to registered users.

THE IMPACT OF RESPONDENT'S FAILURES ON CONSUMERS

12. As demonstrated by the breach, respondent's failures to provide reasonable and appropriate security led to a significant risk that users' live feeds would be compromised, thereby causing significant injury to consumers.
13. The exposure of sensitive information through respondent's IP cameras increases the likelihood that consumers or their property will be targeted for theft or other criminal activity, increases the likelihood that consumers' personal activities and conversations or those of their family members, including young children, will be observed and recorded by strangers over the Internet. This risk impairs consumers' peaceful enjoyment of their homes, increases consumers' susceptibility to physical tracking or stalking, and reduces consumers' ability to control the dissemination of personal or proprietary information (*e.g.*, intimate video and audio feeds or images and conversations from business properties). Consumers had little, if any, reason to know that their information was at risk, particularly those consumers who maintained login credentials for their cameras or who were merely unwitting third parties present in locations under surveillance by the cameras.

COUNT 1

14. As described in **Paragraph 7**, respondent has represented, expressly or by implication, that respondent has taken reasonable steps to ensure that its IP cameras and mobile apps are a secure means to monitor private areas of a consumer's home or workplace.
15. In truth and in fact, as described in **Paragraphs 8-11**, respondent has not taken reasonable steps to ensure that its IP cameras are a secure means to monitor private areas of a consumer's home or workplace. Therefore, the representation set forth in **Paragraph 14** constitutes a false or misleading representation.

COUNT 2

16. As described in **Paragraphs 5 and 7**, respondent has represented, expressly or by implication, that respondent has taken reasonable steps to ensure that a user's security settings will be honored.
17. In truth and in fact, as described in **Paragraphs 8-11**, respondent has not taken reasonable steps to ensure that a user's security settings will be honored. Therefore, the representation set forth in **Paragraph 16** constitutes a false or misleading representation.

COUNT 3

18. As set forth in **Paragraphs 8-11**, respondent has failed to provide reasonable security to prevent unauthorized access to the live feeds from its IP cameras, which respondent offered to consumers for the purpose of monitoring and securing private areas of their homes and businesses. Respondent's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

19. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this sixteenth day of January, 2014, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL:

COMPLAINT APPENDIX A

1. TV-IP110 (Version A1.xR)
2. TV-IP110W (Version A1.xR)
3. TV-IP110WN (Versions A1.xR & V2.0R)
4. TV-IP121W (Version A1.xR)
5. TV-IP121WN (Versions V1.0R & V2.0R)
6. TV-IP212 (Version A1.xR)
7. TV-IP212W (Version A1.xR)
8. TV-IP252P (Version B1.xR)
9. TV-IP312 (Version A1.xR)
10. TV-IP312W (Version A1.xr)
11. TV-IP312WN (Version A1.xR)
12. TV-IP322P (Version V1.0R)
13. TV-IP410 (Version A1.XR)
14. TV-IP410W (Version A1.xR)
15. TV-IP410WN (Version V1.0R)
16. TV-IP422 (Versions A1.xR & A2.xR)
17. TV-IP422W (Versions A1.xR & A2.xR)
18. TV-IP422WN (Version V1.0R)
19. TV-VS1 (Version V1.0R)
20. TV-VS1P (Version V1.0R)

COMMISSIONERS: **Edith Ramirez, Chairwoman**
 Julie Brill
 Maureen K. Ohlhausen
 Joshua D. Wright

DOCKET No. C-4426

DECISION AND ORDER

The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 *et seq.*;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Decision and Order (“Order”):

1. Respondent TRENDnet, Inc. (“TRENDnet”) is a California corporation with its principal office or place of business at 20675 Manhattan Place, Torrance, California 90501.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. “Affected Consumers” shall mean persons who purchased and installed one of the following Cameras with software last updated prior to February 7, 2012: TV-IP110 (Version A1.xR); TV-IP110W (Version A1.xR); TV-IP110WN (Version A1.xR); TV-IP110WN (Version V2.0R); TV-IP121W (Version A1.xR); TV-IP121WN (Version V1.0R); TV-IP121WN (Version V2.0R); TV-IP212 (Version A1.xR); TV-IP212W (Version A1.xR); TV-IP252P (Version B1.xR); TV-IP312 (Version A1.xR); TV-IP312W (Version A1.xr); TV-IP312WN (Version A1.xR); TV-IP322P (Version V1.0R); TV-IP410 (Version A1.XR); TV-IP410W (Version A1.xR); TV-IP410WN (Version V1.0R); TV-IP422 (Versions A1.xR/A2.xR); TV-IP422W (Versions A1.xR/A2.xR); TV-IP422WN (Version V1.0R); TV-VS1 (Version V1.0R); and TV-VS1P (Version V1.0R).
2. “App” or “Apps” shall mean any software application or related code developed, branded, or provided by respondent for a mobile device, including, but not limited to, any iPhone, iPod touch, iPad, BlackBerry, Android, Amazon Kindle, or Microsoft Windows device.
3. “Cameras” shall mean any Internet Protocol (“IP”) camera, cloud camera, or other Internet-accessible camera advertised, developed, branded, or sold by respondent, or on behalf of respondent, or any corporation, subsidiary, division or affiliate owned or controlled by respondent that transmits, or allows for the transmission of Live Feed Information over the Internet.
4. “Clear(ly) and prominent(ly)” shall mean:
 - A. In textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
 - B. In communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;

- C. In communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subparagraph (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and
 - D. In all instances, the required disclosures (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any other statements or disclosures provided by respondent.
- 5. “Commerce” shall mean commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation, as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
 - 6. “Covered Device” shall mean: (1) any Internet-accessible electronic product or device, including but not limited to “Cameras,” advertised, developed, branded, or sold by respondent, or on behalf of respondent, or any corporation, subsidiary, division or affiliate owned or controlled by respondent that transmits or allows for the transmission of Covered Information over the Internet; and (2) any App or software advertised, developed, branded, or provided by respondent or any corporation, subsidiary, division or affiliate owned or controlled by respondent used to operate, manage, access, or view the product or device.
 - 7. “Covered Device Functionality” shall mean any capability of a Covered Device to capture, access, store, or transmit Covered Information.
 - 8. “Covered Information” shall mean individually-identifiable information from or about an individual consumer input into, stored on, captured with, accessed, or transmitted through a Covered Device, including but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as a user identifier or screen name; (d) photos; (e) videos; (f) pre-recorded and live-streaming audio; (g) an IP address, User ID or other persistent identifier; or (h) an authentication credential, such as a username or password.
 - 9. “Live Feed Information” shall mean video, audio, or audiovisual data.
 - 10. Unless otherwise specified, “respondent” shall mean TRENDnet, Inc., and its successors and assigns.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, other device, or an affiliate owned or controlled by respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

- A. The extent to which respondent or its products or services maintain and protect:
 - 1. The security of Covered Device Functionality;
 - 2. The security, privacy, confidentiality, or integrity of any Covered Information; and
- B. The extent to which a consumer can control the security of any Covered Information input into, stored on, captured with, accessed, or transmitted by a Covered Device.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this Order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks that could result in unauthorized access to or use of Covered Device Functionality, and (2) protect the security, confidentiality, and integrity of Covered Information, whether collected by respondent, or input into, stored on, captured with, accessed, or transmitted through a Covered Device. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device Functionality or Covered Information, including:

- A. The designation of an employee or employees to coordinate and be accountable for the security program;
- B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or use of Covered Device Functionality, and assessment of the sufficiency of any safeguards in place to control these risks;
- C. The identification of material internal and external risks to the security, confidentiality, and integrity of Covered Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent's possession or is input into, stored on, captured with, accessed, or transmitted through a Covered

Device, and assessment of the sufficiency of any safeguards in place to control these risks;

- D. At a minimum, the risk assessments required by Subparts B and C should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-party security vulnerability reports;
- E. The design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Information is restricted consistent with a user's security settings;
- F. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this Order, and requiring service providers, by contract, to establish and implement, and thereafter maintain, appropriate safeguards consistent with this Order; and
- H. The evaluation and adjustment of the security program in light of the results of the testing and monitoring required by Subpart F, any material changes to the respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this Order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Covered Devices or other similar Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Covered Devices or other similar Internet-accessible consumer-grade devices; or a similarly qualified person or organization; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal

Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the Order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the Order for the biennial Assessments. Each Assessment shall:

- A. Set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device Functionality or Covered Information;
- C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this Order; and
- D. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Device Functionality and the security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the Order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of TRENDnet, Inc.*, FTC File No. 1223090, Docket No. C-4426. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IV.

IT IS FURTHER ORDERED that respondent shall:

- A. Notify Affected Consumers, clearly and prominently, that their Cameras had a flaw that allowed third parties to access their Live Feed Information without inputting authentication credentials, despite their security setting choices; and provide instructions on how to remove this flaw. Notification shall include, but not be limited to, each of the following means:

1. On or before ten (10) days after the date of service of this Order and for two (2) years after the date of service of this Order, posting of a notice on its website;
 2. On or before ten (10) days after the date of service of this Order and for three (3) years after the date of service of this Order, informing Affected Consumers who complain or inquire about a Camera; and
 3. On or before ten (10) days after the date of service of this Order and for three (3) years after the date of service of this Order, informing Affected Consumers who register, or who have registered, their Camera with respondent; and
- B. Provide prompt and free support with clear and prominent contact information to help consumers update and/or uninstall a Camera. For two (2) years after the date of service of this Order, this support shall include toll-free, telephonic and electronic mail support.

V.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. For a period of five (5) years after the date of preparation of each Assessment required under Part III of this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Part III of this Order, for the compliance period covered by such Assessment;
- B. Unless covered by V.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this Order, including but not limited to:
1. All advertisements, promotional materials, installation and user guides, and packaging containing any representations covered by this Order, as well as all materials used or relied upon in making or disseminating the representation; and

2. Any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this Order.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this Order to all (1) current and future subsidiaries, (2) current and future principals, officers, directors, and managers, (3) current and future employees, agents, and representatives having responsibilities relating to the subject matter of this Order, and (4) current and future manufacturers and service providers of the Covered Products. Respondent shall deliver this Order to such current subsidiaries, personnel, manufacturers, and service providers within thirty (30) days after service of this Order, and to such future subsidiaries, personnel, manufacturers, and service providers within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this section.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this Order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of TRENDnet, Inc.*, FTC File No. 1223090, Docket No. C-4426. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VIII.

IT IS FURTHER ORDERED that respondent within sixty (60) days after the date of service of this Order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this Order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

IX.

This Order will terminate on January 16, 2034, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the Order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this Order that terminates in fewer than twenty (20) years;
- B. This Order's application to any respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: January 16, 2014

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Edith Ramirez, Chairwoman**
 Maureen K. Ohlhausen
 Terrell McSweeney

In the Matter of

DOCKET NO. C-4587

ASUSTeK Computer, Inc.,
a corporation.

COMPLAINT

The Federal Trade Commission, having reason to believe that ASUSTeK Computer, Inc. (“respondent”) has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent ASUSTeK Computer, Inc. is a Taiwanese corporation with its principal office or place of business at 15, Li-Te Rd., Peitou, Taipei 11259, Taiwan.
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT’S BUSINESS PRACTICES

3. Respondent ASUSTeK Computer, Inc. (“ASUS”) is a hardware manufacturer that, among other things, sells routers, and related software and services, intended for consumer use. ASUS designs the software for its routers, controls U.S. marketing and advertising for its routers, including on websites targeting U.S. consumers, and is responsible for developing and distributing software updates to remediate security vulnerabilities and other flaws in routers sold to U.S. consumers. ASUS sells its routers in the United States through a wholly owned U.S. subsidiary, which distributes the routers for sale through third-party retailers, in stores and online, throughout the United States.

RESPONDENT’S ROUTERS AND “CLOUD” FEATURES

4. Routers forward data packets along a network. In addition to routing network traffic, consumer routers typically function as a hardware firewall for the local network, and act as the first line of defense in protecting consumer devices on the local network, such as computers, smartphones, internet-protocol (“IP”) cameras, and other connected

appliances, against malicious incoming traffic from the internet. Respondent marketed its routers as including security features such as “SPI intrusion detection” and “DoS protection,” advertised that its routers could “protect computers from any unauthorized access, hacking, and virus attacks” (*see* Exh. A, p. 1 of 2), and instructed consumers to “enable the [router’s] firewall to protect your local network against attacks from hackers” (*see* Exh. A, p. 2 of 2).

5. Consumers set up and control the router’s configuration settings, including its security-related settings, through a web-based graphical user interface (the “admin console”). In order to configure these settings, consumers must log in to the admin console with a username and password, which ASUS preset on all of its routers to the default username “admin” and password “admin” (*see* Exh. B). The admin console also provides a tool that ostensibly allows consumers to check whether the router is using the latest available firmware – the software that operates the router.
6. Many of respondent’s routers include software features called AiCloud and AiDisk that allow consumers to wirelessly access and share files through their router. Depending on the model, respondent’s routers that include these “cloud” features have a list price in the range of \$69.99 to \$219.99. As of March 2014, respondent had sold over 918,000 of these routers to U.S. consumers.

AICLOUD

7. In August 2012, ASUS introduced and began marketing a feature known as AiCloud on its routers. Respondent publicized AiCloud as a “private personal cloud for selective file sharing” that featured “indefinite storage and increased privacy” (*see* Exh. C, p. 1 of 6). In the following months, ASUS provided software updates for certain older router models to add the AiCloud feature, which respondent touted as “the most complete, accessible, and secure cloud platform” (*see* Exh. C, p. 2 of 6).
8. Described as “your secure space,” AiCloud allows consumers to plug a USB storage device, such as an external hard drive, into the router, and then use web and mobile applications to access files on the storage device (*see* Exh. C, p. 3 of 6). For example, a consumer could save documents to the storage device using a desktop computer, and then later access those documents using a laptop, smartphone, or tablet. AiCloud also allows consumers to share specific files with others through a “secure URL,” manage shared files, and revoke file access (*see* Exh. C, pp. 3-6 of 6).

Multiple Vulnerabilities

9. The AiCloud web and mobile applications require consumers to log in with the router’s username and password (*see* Exh. D). However, the AiCloud web application included multiple vulnerabilities that would allow attackers to gain unauthorized access to consumers’ files and router login credentials. In order to exploit these vulnerabilities, an attacker would only need to know the router’s IP address – information that, as described in Paragraph 32, is easily discoverable.

10. First, attackers could exploit an authentication bypass vulnerability to access the consumer's AiCloud account without the consumer's login credentials. By sending a specific command, or simply entering a specific URL in a web browser, an attacker could bypass the AiCloud web application's authentication screen and gain unauthorized access to a consumer's files, even if the consumer had not designated any of these files for sharing.
11. Second, attackers could exploit a password disclosure vulnerability in the AiCloud web application to retrieve the consumer's router login credentials in clear, readable text. In addition to providing the attacker with access to the consumer's AiCloud account, attackers could also use these login credentials to gain unauthorized access to the router's configuration settings. For example, if a consumer had enabled the admin console's remote management feature, an attacker could use the login credentials to simply log into the consumer's admin account and modify any of the router's settings, including its firewall and other security settings. Even if this remote management feature was disabled, an attacker could use the credentials in conjunction with other well-known vulnerabilities that affected respondent's routers, such as the cross-site request forgery vulnerabilities described in Paragraphs 24-26, to force unauthorized changes to the router's security settings, placing the consumer's local network at risk.

Failure to Provide Timely Notice

12. Several individuals notified respondent about the AiCloud vulnerabilities in June 2013. Furthermore, in September 2013, a consumer complained to ASUS that his "entire life [was] hacked" due to the AiCloud vulnerabilities, and that he needed to obtain identity theft protection services as a result. Despite knowing about these serious vulnerabilities and their impact on respondent's customers, respondent failed to notify consumers about the vulnerabilities or advise them to take simple steps, such as disabling the AiCloud features, that would have mitigated the vulnerabilities.
13. Between July 2013 and September 2013, ASUS updated the firmware for affected routers in order to correct the AiCloud vulnerabilities. However, it was not until February 2014, eight months after respondent first learned of the vulnerabilities and after the events described in Paragraph 32, that respondent emailed registered customers notifying them that firmware updates addressing these and other security risks were available.

AiDisk

14. ASUS has offered another "cloud" feature on many of its routers called "AiDisk" since as early as 2009. Like AiCloud, AiDisk enables consumers to remotely access files on a USB storage device attached to the router, but does so through a file transfer protocol ("FTP") server. Despite the fact that FTP does not support transit encryption, since at least 2012 respondent has promoted AiDisk as a way to "safely secure and access your treasured data through your router" (*see* Exh. E). In addition to transferring files unencrypted, the AiDisk software included a number of other design flaws that placed consumers' sensitive personal information at risk.

Insecure Design

15. Consumers could set up an AiDisk FTP server in two ways. The first was through a set of menus called the “AiDisk wizard.” During setup, the AiDisk wizard asks the consumer to “Decide how to share your folders,” and presents three options: “limitless access rights,” “limited access rights,” and “admin rights.” Prior to January 2014, the AiDisk wizard did not provide consumers with sufficient information to evaluate these options, and pre-selected the “limitless access rights” option for the consumer (*see* Exh. F, p. 1 of 2). If the consumer completed setup with this default option in place, the AiDisk wizard created an FTP server that would provide anyone on the internet who had the router’s IP address with unauthenticated access to the consumer’s USB storage device.
16. The second way consumers could set up an AiDisk FTP server was through a submenu in the admin console called “USB Application – FTP Share.” The submenu did not provide consumers with any information regarding the default settings or the alternative settings that were available. If a consumer clicked on the option to “Enable FTP” (*see* Exh. G, p. 1 of 2), the software created an AiDisk FTP server that, by default, provided anyone on the internet who had the router’s IP address with unauthenticated access to the consumer’s USB storage device.
17. Neither set-up option provided any explanation that the default settings would provide anyone on the internet with unauthenticated access to all of the files saved on the consumer’s USB storage device. And in both cases, search engines could index any of the files exposed by these unauthenticated FTP servers, making them easily searchable online.
18. If a consumer wanted to prevent unauthenticated access through the AiDisk wizard, the consumer needed to deviate from the default settings and select “limited access rights.” The consumer would then be presented with the option to create login credentials for the FTP server. However, the AiDisk wizard recommended that the consumer choose weak login credentials, such as the preset username “Family” and password “Family” (*see* Exh. F, p. 2 of 2). In the alternative, the consumer could select “admin rights,” which would apply the same login credentials for the FTP server that the consumer used to log in to the router’s admin console. As described in Paragraphs 11 and 24, however, due to multiple password disclosure vulnerabilities, attackers could access these router login credentials in clear, readable text, undermining the protection provided by these credentials.
19. If a consumer wanted to prevent unauthenticated access through the “USB Application – FTP Share” submenu, the software provided no explanation or guidance as to how the consumer could change the default settings. The consumer would need to know to click on the “Share with account” option (*see* Exh. G, p. 1 of 2), which would allow the consumer to set up login credentials for the AiDisk FTP server. Confusingly, however, the software presented the consumer with a warning that implied that this option would expand, rather than restrict, access to the FTP server: “Enabling share with account enables multiple computers, with different access rights, to access the file resources. Are you sure you want to enable it?” (*see* Exh. G, p. 2 of 2). Through this misleading

warning, respondent discouraged consumers from taking steps that could have prevented unauthenticated access to their sensitive personal information.

Notice of Design Flaws and Failure to Mitigate

20. In June 2013, a security researcher publicly disclosed that, based on his research, more than 15,000 ASUS routers allowed for unauthenticated access to AiDisk FTP servers over the internet. In his public disclosure, the security researcher claimed that he had previously contacted respondent about this and other security issues. In November 2013, the security researcher again contacted respondent, warning that, based on his research, 25,000 ASUS routers now allowed for unauthenticated access to AiDisk FTP servers. The researcher suggested that respondent warn consumers about this risk during the AiDisk set up process. However, ASUS took no action at the time.
21. Two months later, in January 2014, several European media outlets published stories covering the security risks caused by the AiDisk default settings. At that time, a large European retailer requested that respondent update the AiDisk default settings. Although respondent had known about the security risks for months, it was only after this retailer's request that respondent took some steps to protect its customers. In response, ASUS began releasing updated firmware that changed the AiDisk wizard's default setting – for new set-ups – from “limitless access rights” to “limited access rights,” and displayed a warning message if consumers selected “limitless access rights” that “any user can access your FTP service without authentication!” However, respondent did not notify consumers about the availability of this firmware update.
22. Moreover, the January 2014 firmware update did not change the insecure default settings for consumers who had already set up AiDisk. Respondent did not notify those consumers that they would need to complete the AiDisk wizard process again in order for the new defaults to apply, or would need to manually change the settings.
23. It was not until February 2014 – following the events described in Paragraph 32 – that respondent sent an email to registered customers notifying them that firmware updates addressing these security risks and other security vulnerabilities were available. Furthermore, it was not until February 21, 2014 that ASUS released a firmware update that would provide some protection to consumers who had previously set up AiDisk. This firmware update forced consumers' routers to turn off unauthenticated access to the AiDisk FTP server.

OTHER VULNERABILITIES

24. ASUS's router firmware and admin console have also been susceptible to a number of other well-known and reasonably foreseeable vulnerabilities – including multiple password disclosure, cross-site scripting, cross-site request forgery, and buffer overflow vulnerabilities – that attackers could exploit to gain unauthorized administrative control over consumers' routers.

25. For example, the admin console has been susceptible to pervasive cross-site request forgery (“CSRF”) vulnerabilities that would allow an attacker to force malicious changes to any of the router’s security settings (*e.g.*, disabling the firewall, enabling remote management, allowing unauthenticated access to an AiDisk server, or configuring the router to redirect the consumer to malicious websites) without the consumer’s knowledge. Despite the serious consequences of these vulnerabilities, respondent did not perform pre-release testing for this class of vulnerabilities. Nor did respondent implement well-known, low-cost measures to protect against them, such as anti-CSRF tokens – unique values added to requests sent between a web application and a server that only the server can verify, allowing the server to reject forged requests sent by attackers.
26. Beginning in March 2013, respondent received multiple reports from security researchers regarding the CSRF vulnerabilities affecting respondent’s routers. Despite these reports, respondent took no action to fix the vulnerabilities for at least a year, placing consumers’ routers at risk of exploit. Indeed, in April 2015, a malware researcher discovered a large-scale, active CSRF exploit campaign that reconfigured vulnerable routers so that the attackers could control and redirect consumers’ web traffic. This exploit campaign specifically targeted numerous ASUS router models.

FIRMWARE UPGRADE TOOL

27. The admin console includes a tool that ostensibly allows consumers to check whether their router is using the most current firmware (“firmware upgrade tool”). When consumers click on the “Check” button, the tool indicates that the “router is checking the ASUS server for the firmware update” (*see* Exh. H).
28. In order for the firmware upgrade tool to recognize the latest available firmware, ASUS must update a list of available firmware on its server. On several occasions, ASUS has failed to update this list. In July 2013, respondent received reports that the firmware upgrade tool was not recognizing the latest available firmware from both a product review journalist and by individuals calling into respondent’s customer-support call center. Likewise, in February 2014, a security researcher notified respondent that the firmware upgrade tool did not recognize the latest available firmware, and detailed the reasons for the failure. In an internal email from that time, respondent acknowledged that, “if this list is not up to date when you use the check for update button in the [admin console,] the router doesn’t find an update and states it is already up to date.” Again, in October 2014 and January 2015, additional consumers reported to ASUS that the firmware upgrade tool still did not recognize the latest available firmware.
29. As a result, in many cases, respondent’s firmware upgrade tool inaccurately notifies consumers that the “router’s current firmware is the latest version” when, in fact, newer firmware with critical security updates is available.

RESPONDENT'S FAILURE TO REASONABLY SECURE ITS ROUTERS AND RELATED "CLOUD" FEATURES

30. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security in the design and maintenance of the software developed for its routers and related "cloud" features. Among other things, respondent failed to:

- a. perform security architecture and design reviews to ensure that the software is designed securely, including failing to:
 - i. use readily-available secure protocols when designing features intended to provide consumers with access to their sensitive personal information. For example, respondent designed the AiDisk feature to use FTP rather than a protocol that supports transit encryption;
 - ii. implement secure default settings or, at the least, provide sufficient information that would ensure that consumers did not unintentionally expose sensitive personal information;
 - iii. prevent consumers from using weak default login credentials to protect critical security functions or sensitive personal information. For example, respondent allowed consumers to retain the weak default login credentials username "admin" and password "admin" for the admin console, and username "Family" and password "Family" for the AiDisk FTP server;
- b. perform reasonable and appropriate code review and testing of the software to verify that access to data is restricted consistent with a user's privacy and security settings;
- c. perform vulnerability and penetration testing of the software, including for well-known and reasonably foreseeable vulnerabilities that could be exploited to gain unauthorized access to consumers' sensitive personal information and local networks, such as authentication bypass, clear-text password disclosure, cross-site scripting, cross-site request forgery, and buffer overflow vulnerabilities;
- d. implement readily-available, low-cost protections against well-known and reasonably foreseeable vulnerabilities, as described in (c), such as input validation, anti-CSRF tokens, and session time-outs;
- e. maintain an adequate process for receiving and addressing security vulnerability reports from third parties such as security researchers and academics;
- f. perform sufficient analysis of reported vulnerabilities in order to correct or mitigate all reasonably detectable instances of a reported vulnerability, such as those elsewhere in the software or in future releases; and
- g. provide adequate notice to consumers regarding (i) known vulnerabilities or security risks, (ii) steps that consumers could take to mitigate such vulnerabilities

or risks, and (iii) the availability of software updates that would correct or mitigate the vulnerabilities or risks.

THOUSANDS OF ROUTERS COMPROMISED

31. Due to the failures described in Paragraphs 7-30, respondent has subjected its customers to a significant risk that their sensitive personal information and local networks will be subject to unauthorized access.
32. For example, on or before February 1, 2014, a group of hackers used readily available tools to locate the IP addresses of thousands of vulnerable ASUS routers. Exploiting the AiCloud vulnerabilities and AiDisk design flaws, the hackers gained unauthorized access to the attached USB storage devices of thousands of consumers and saved a text file on the storage devices warning these consumers that their routers were compromised: “This is an automated message being sent out to everyone effected [sic]. Your Asus router (and your documents) can be accessed by anyone in the world with an internet connection.” The hackers then posted online a list of IP addresses for 12,937 vulnerable ASUS routers as well as the login credentials for 3,131 AiCloud accounts, further exposing these consumers to potential harm.
33. Numerous consumers reported having their routers compromised, based on their discovery of the text-file warning the hackers had saved to their attached USB storage devices. Some complained that a major search engine had indexed the files that the vulnerable routers had exposed, making them easily searchable online. Others claimed to be the victims of related identity theft. For example, one consumer claimed that identity thieves had gained unauthorized access to his USB storage device, which contained his family’s sensitive personal information, including login credentials, social security numbers, dates of birth, and tax returns. According to the consumer, in March 2014, identity thieves used this information to make thousands of dollars of fraudulent charges to his financial accounts, requiring him to cancel accounts and place a fraud alert on his credit report. Moreover, the consumer claimed that he had attempted to upgrade his router’s firmware on several occasions after he bought the device in December 2013, but that the firmware upgrade tool had erroneously indicated that his router was using the latest available firmware. Given the sensitivity of the stolen personal information, he and his family are at a continued risk of identity theft.
34. Even consumers who did not enable the AiCloud and AiDisk features have been at risk of harm due to numerous vulnerabilities in respondent’s router firmware and admin console. As described in Paragraphs 24-26, attackers could exploit these vulnerabilities to gain unauthorized control over a consumer’s router and modify its security settings without the consumer’s knowledge.

THE IMPACT OF RESPONDENT'S FAILURES ON CONSUMERS

35. As demonstrated by the thousands of compromised ASUS routers, respondent's failure to employ reasonable security practices has subjected consumers to substantial injury. Unauthorized access to sensitive personal information stored on attached USB storage devices, such as financial information, medical information, and private photos and videos, could lead to identity theft, extortion, fraud, or other harm. Unauthorized access and control over the router could also lead to the compromise of other devices on the local network, such as computers, smartphones, IP cameras, or other connected appliances. Finally, such unauthorized access and control could allow an attacker to redirect a consumer seeking, for example, a legitimate financial site to a fraudulent site, where the consumer would unwittingly provide the attacker with sensitive financial information. Consumers had little, if any, reason to know that their sensitive personal information and local networks were at risk.
36. Respondent could have prevented or mitigated these risks through simple, low-cost measures. In several instances, respondent could have prevented consumer harm by simply informing consumers about security risks, and advising them to disable or update vulnerable software. In other cases, respondent could have protected against vulnerabilities by implementing well-known and low-cost protections, such as input validation, anti-CSRF tokens, and session time-outs, during the software design process. Finally, simply preventing consumers from using weak default login credentials would have greatly increased the security of consumers' routers.

ROUTER SECURITY MISREPRESENTATIONS (Count 1)

37. As described in Paragraph 4, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its routers could protect consumers' local networks from attack.
38. In fact, as described in Paragraphs 11, 24-26, and 30, respondent did not take reasonable steps to ensure that its routers could protect consumers' local networks from attack. Therefore, the representation set forth in Paragraph 37 is false or misleading.

AICLOUD SECURITY MISREPRESENTATIONS (Count 2)

39. As described in Paragraphs 7-8, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its AiCloud feature is a secure means for a consumer to access sensitive personal information.
40. In fact, as described in Paragraphs 9-13 and 30, respondent did not take reasonable steps to ensure that its AiCloud feature is a secure means for a consumer to access sensitive personal information. Therefore, the representation set forth in Paragraph 39 is false or misleading.

AIDISK SECURITY MISREPRESENTATIONS
(Count 3)

41. As described in Paragraph 14, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its AiDisk feature is a secure means for a consumer to access sensitive personal information.
42. In fact, as described in Paragraphs 14-23 and 30, respondent did not take reasonable steps to ensure that its AiDisk feature is a secure means for a consumer to access sensitive personal information. Therefore, the representation set forth in Paragraph 41 is false or misleading.

FIRMWARE UPGRADE TOOL MISREPRESENTATIONS
(Count 4)

43. As described in Paragraph 27, respondent has represented, expressly or by implication, that consumers can rely upon the firmware upgrade tool to indicate accurately whether their router is using the most current firmware.
44. In fact, as described in Paragraphs 28-29, consumers cannot rely upon the firmware upgrade tool to indicate accurately whether their router is using the most current firmware. Therefore, the representation set forth in Paragraph 43 is false or misleading.

UNFAIR SECURITY PRACTICES
(Count 5)

45. As set forth in Paragraphs 4-36, respondent has failed to take reasonable steps to secure the software for its routers, which respondent offered to consumers for the purpose of protecting their local networks and accessing sensitive personal information. Respondent's actions caused or are likely to cause substantial injury to consumers in the United States that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.
46. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this eighteenth day of July, 2016, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Edith Ramirez, Chairwoman
Maureen K. Ohlhausen
Terrell McSweeney**

In the Matter of

**ASUSTeK Computer Inc.,
a corporation.**

DECISION AND ORDER

DOCKET NO. C-4587

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named above in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violation of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days, and duly considered the comments filed thereafter by interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

1. Respondent ASUSTeK Computer, Inc., is a Taiwanese corporation with its principal office or place of business at 15, Li-Te Rd., Peitou, Taipei 11259, Taiwan.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean ASUSTeK Computer, Inc., corporation, and its subsidiaries and divisions in the United States, and successors and assigns.
2. “Clear(ly) and conspicuous(ly)” means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
 - A. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication, even if the representation requiring the disclosure is made in only one means.
 - B. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
 - C. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 - D. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 - E. The disclosure must use diction and syntax understandable to ordinary consumers.
 - F. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 - G. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

3. “Commerce” shall mean commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation, as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
4. “Covered Device” shall mean (a) any router, or device for which the primary purpose is connecting other client devices to a network, developed by respondent, directly or indirectly, that is marketed to consumers in the United States and (b) the software used to access, operate, manage, or configure such router or other device subject to part (a) of this definition, including, but not limited to, the firmware, web or mobile applications, and any related online services, that are advertised, developed, branded, or provided by respondent, directly or indirectly, for use with, or as compatible with, the router or other device.
5. “Covered Information” shall mean any individually-identifiable information from or about an individual consumer collected by respondent through a Covered Device or input into, stored on, captured with, accessed, or transmitted through a Covered Device, including but not limited to (a) a first and last name; (b) a home or other physical address; (c) an email address or other online contact information; (d) a telephone number; (e) a Social Security number; (f) financial information; (g) an authentication credential, such as a username or password; (h) photo, video, or audio files; (i) the contents of any communication, the names of any websites sought, or the information entered into any website.
6. “Default Settings” shall mean any configuration option on a Covered Device that respondent preselects, presets, or prefills for the consumer.
7. “Software Update” shall mean any update designed to address a Security Flaw.
8. “Security Flaw” is a software vulnerability or design flaw in a Covered Device that creates a material risk of (a) unauthorized access to or modification of any Covered Device, (b) the unintentional exposure by a consumer of Covered Information, or (c) the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of Covered Information.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, in or affecting commerce, must not misrepresent in any manner, expressly or by implication:

- A. The extent to which respondent or its products or services maintain and protect:
 - 1. The security of any Covered Device;
 - 2. The security, privacy, confidentiality, or integrity of any Covered Information;
- B. The extent to which a consumer can use a Covered Device to secure a network; and
- C. The extent to which a Covered Device is using up-to-date software.

II.

IT IS FURTHER ORDERED that respondent must, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing Covered Devices, and (2) protect the privacy, security, confidentiality, and integrity of Covered Information. Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device's function or the Covered Information, including:

- A. The designation of an employee or employees to coordinate and be accountable for the security program;
- B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or unauthorized modification of a Covered Device, and assessment of the sufficiency of any safeguards in place to control these risks;
- C. The identification of material internal and external risks to the privacy, security, confidentiality, and integrity of Covered Information that could result in the unintentional exposure of such information by consumers or the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;
- D. At a minimum, the risk assessments required by Subparts B and C must include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing, including for Default Settings; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

- E. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security testing techniques, such as (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Devices and Covered Information is restricted consistent with a user's security settings;
- F. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards consistent with this order; and
- H. The evaluation and adjustment of respondent's security program in light of the results of the testing and monitoring required by Subpart F, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of the security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent must obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments must be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Internet-accessible consumer-grade devices; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. The reporting period for the Assessments must cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment must:

- A. Set forth the specific controls and procedures that respondent has implemented and maintained during the reporting period;
- B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device's function or the Covered Information;

- C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and
- D. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Devices and the privacy, security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

Each Assessment must be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent must provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments must be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In re ASUSTek Computer Inc.*, FTC File No. 142 3156.

IV.

IT IS FURTHER ORDERED that respondent must:

- A. Notify consumers, Clearly and Conspicuously, when a Software Update is available, or when respondent is aware of reasonable steps that a consumer could take to mitigate a Security Flaw. The notice must explain how to install the Software Update, or otherwise mitigate the Security Flaw, and the risks to the consumer's Covered Device or Covered Information if the consumer chooses not to install the available Software Update or take the recommended steps to mitigate the Security Flaw. Notice must be provided through at least each of the following means:
 - 1. Posting of a Clear and Conspicuous notice on at least the primary, consumer-facing website of respondent and, to the extent feasible, on the user interface of any Covered Device that is affected;
 - 2. Directly informing consumers who register, or who have registered, a Covered Device with respondent, by email, text message, push notification, or another similar method of providing notifications directly to consumers; and
 - 3. Informing consumers who contact respondent to complain or inquire about any aspect of the Covered Device they have purchased.

- B. Provide consumers with an opportunity to register an email address, phone number, device, or other information during the initial setup or configuration of a Covered Device, in order to receive the security notifications required by this Part. The consumer's registration of such information must not be dependent upon or defaulted to an agreement to receive non-security related notifications or any other communications, such as advertising. Notwithstanding this requirement, respondent may provide an option for consumers to opt-out of receiving such security-related notifications.

V.

IT IS FURTHER ORDERED that respondent must maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. For a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Part III of this order, for the compliance period covered by such Assessment;
- B. Unless covered by V.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:
 - 1. All advertisements, promotional materials, installation and user guides, and packaging containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation;
 - 2. All notifications required by Part IV of this order; and
 - 3. Any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order.

VI.

IT IS FURTHER ORDERED that respondent must deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order. Respondent must deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such

position or responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery must be at least ten (10) days prior to the change in structure.

VII.

IT IS FURTHER ORDERED that respondent must notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however*, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent must notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In re ASUSTek Computer Inc.*, FTC File No. 142 3156.

VIII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, must file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it must submit additional true and accurate written reports.

IX.

This order will terminate on July 18, 2036, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in fewer than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: July 18, 2016