Privacy in M&A Transactions: Navigating the Traps

By Daniel Ilan, Emmanuel Ronco, Natascha Gerlach, and Jane Rosen

I. Introduction

One aspect of mergers and acquisitions that is receiving growing attention is the relevance of privacy issues[1] under U.S. and EU laws as well as under the laws of a growing number of other jurisdictions.[2] This article discusses the principal M&A-related privacy risks and highlights certain "traps" that are often overlooked. In Part I we discuss risks associated with a target's pre-closing privacy-related liabilities and consider ways to mitigate these risks through adequate diligence and representations in M&A agreements. In Part II, we discuss the risks associated with transferring or disclosing personally identifiable information ("personal data") of an M&A target (or a seller) to a purchaser (or prospective purchaser). In Part III, we discuss risks associated with the purchaser's post-acquisition use of such personal data.

II. Risks Associated with the Target's Pre-Closing Privacy-Related Liabilities

In M&A transactions, purchasers often assume the liabilities of the target, including for past noncompliance with privacy laws, which may result in fines, damages arising from private actions, significant harm to a company's goodwill and, in some cases, criminal liability.[3] Yet privacy-related diligence and related representations often just skim the surface.

A. Privacy Due Diligence: Key Areas of Inquiry

As part of the due diligence process, it is important to consider all applicable laws, the target's privacy policies and contractual commitments, the existing privacy standards in the target's industry and, most importantly, the target's actual practices (and its compliance with all of the foregoing).

1. Identifying the Applicable Laws

The first step in privacy diligence is ascertaining which federal, state, and non-U.S. laws might apply to the target's business. This requires an in-depth understanding of the business of the target and knowledge of the relevant laws. While many countries have enacted privacy laws, U.S. state and federal laws and EU laws, including the EU's restrictions on cross-border transfer of personal data, are most often implicated in cross-border M&A deals.

The U.S. legislative privacy framework is fragmented—no comprehensive federal legislation exists. Section 5 of the Federal Trade Commission (FTC) Act, which prohibits unfair or deceptive acts or practices, has been enforced against companies that failed to safeguard personal data or comply with posted privacy policies; various other federal laws apply to select industries or to particular categories of information (and empower various federal agencies to promulgate regulations). In addition, states have passed their own privacy laws applicable to entities that operate in those states or collect personal data about individuals residing in the state. Thus, in the United States the task of simply ascertaining all laws applicable to a particular target may be a complicated endeavor. There are also industry standards and guidelines issued by industry groups, which are not legally enforceable but are considered "best practices."

EU law may apply, even to targets outside of the EU, if their data processing activities make use of equipment situated within the EU. In addition, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which will come into force on May 25, 2018, also will apply to non-EU targets that process personal data of EU-based individuals ("data subjects"), without regard to where the related equipment is situated.[4]

- ***Trap***: *An M&A target often will be subject to privacy laws in jurisdictions beyond those in which the target and its subsidiaries are incorporated. A purchaser should ascertain the jurisdictions in which the target has branches or sales offices and the jurisdictions in which it collects or stores (in local servers) personal data. Within each jurisdiction, more than one set of privacy-related laws may apply, depending on the target's business.*

2. Published Privacy Policies

An important component of privacy due diligence under U.S. law involves determining whether the target has put in place adequate privacy policies and/or terms of use and investigating whether it is in full compliance with such published policies (whether posted online or otherwise provided to customers). The FTC is the key U.S. agency regulating privacy and data security practices, and its rulings, interpretations, and opinions must be examined to understand the requirements and restrictions. The FTC has made clear that companies must make their policies describing their practices with respect to personal data publicly available and that it views failure to comply with such policies to be a violation of Section 5 of the FTC Act.[5]

EU law stipulates certain minimum information that must be provided to data subjects in order for the

Daniel Ilan is a partner in Cleary Gottlieb Steen & Hamilton's New York Office. **Emmanuel Ronco** is counsel in the firm's Paris office, **Natascha Gerlach** is senior attorney in the Brussels office, and **Jane Rosen** is an associate in the firm's New York Office. A version of this article was first published at www.clearymawatch.com/2016/10/privacy-ma-transactions-navigating-traps.

processing of their personal data to be deemed fair and lawful. Such information is often supplied by companies through a privacy policy. The data protection authorities (DPAs) of each EU member state are tasked with monitoring compliance with EU law, including the principles of fair and lawful processing. For example, the UK's DPA, the Information Commissioner's Office, has issued detailed guidance as to how a privacy policy should be drafted.[6] A target's privacy policy should be assessed by reference to such local standards or published guidance in each Member State.[7]

However, assessing whether a target's privacy policies are adequate and whether the target is in compliance with these policies requires identification of those policies that apply to the personal data in question, and that may not be a simple task:

- *Different policies applicable to different data sources.* The target may publish several different privacy policies that govern the use of personal data collected through various mechanisms (for example, through its online platform, its mobile application, or in materials sent via mail).
- *Different policies applicable to different subsidiaries, business lines, or divisions.* The target may consist of several subsidiaries or business lines, and their privacy policies may vary (including as a result of the fact that some subsidiaries or business lines were acquired from third parties, and their pre-acquisition privacy policies were maintained).
- *Updates or changes to the privacy policy.* A privacy policy may have changed over time. However, statements made in old policies (or in prior versions of the current policy) with which the target currently does not comply still may give rise to liability because the applicable privacy policy governing a particular set of personal data is the one that was made available to the persons from whom the personal data was collected when the data was collected. It thus is important to identify the policy that was in effect when the personal data concerned was collected. For example, in 2004 the FTC alleged in a complaint against Gateway Learning Corp. that it was an unfair practice for Gateway to apply the terms of a new privacy policy to information it had collected from consumers under an earlier policy ("Respondent's retroactive application of its revised privacy policy caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.").[8] Similarly, in 2011, Borders sold its customer personal data (including personal data of approximately 45 million customers) to Barnes & Noble in a bankruptcy auction. The FTC sent a letter to the court-appointed consumer privacy ombudsman stating its view that any transfer of personal data in connection with the bankruptcy should be subject to significant restrictions. The FTC specifically noted that Borders' privacy policy had changed over time, initially stating "we do not rent or sell your information to third parties" and that "we will only disclose your email address or other personal data to third parties if you expressly consent to such disclosure" and later being amended to state that customer information may be transferred if Borders engages in an M&A transaction.[9]

Once the relevant policies are identified, they should be carefully reviewed. Such diligence should focus on two main areas. First, the policies should be reviewed to determine whether they contain all the information required to be published under applicable law. Examples of the types of information that privacy laws in various jurisdictions may require include the precise categories of personal data collected; the purposes for which customers' personal data is intended to be used; the categories of third parties with whom the personal data is shared; and information about, and a mechanism to obtain consent to the use of, cookies. Second, the policies should be reviewed to determine whether they contain statements or promises with which the target does not comply. This inquiry obviously requires diligence of the target's actual practices.

Finally, if the target does not have an online privacy policy, it is important to determine whether it is required to have one. Absence of a published policy may violate a contractual obligation or give rise to violation of law. (For example, California's privacy laws require all operators of commercial websites or online services that collect personal data about individual consumers residing in California to post privacy policies.)

- ***Trap 1:*** *A purchaser should not stop inquiring even after receiving a copy of a company's privacy policy. A company can have multiple privacy policies in effect at any given time (for different platforms and/or business lines), and each of those policies could lead to privacy-related liabilities. Policies from prior years (or past versions of the current policy) also may be relevant to the extent they are different from the current ones.*
- ***Trap 2:*** *A purchaser should not be lulled into a false sense of security by a target's privacy policy that provides detailed promises regarding data security (e.g., use of firewall, encryption, and/or Secure Socket Layer technology) or personal data handling (e.g., claiming that servers reside only in a certain jurisdiction). This may indicate that the target is privacy-savvy and equipped to deal with associated risks, but it also increases the risk of non-compliance with such promises, so it should encourage further diligence.*

3. Contractual Obligations

A final area of inquiry is the target's contracts with third parties (other than its published online or offline

policies). When the target is a service provider that has entered into agreements containing privacy-related requirements, assessment of compliance with such contractual obligations may be important. A particular area of concern in this context is the target's indemnification obligations and the extent to which its liabilities under each contract may be capped or otherwise limited. The nature of privacy-related exposure is such that a significant portion of the potential liability is associated with third-party claims, where users and customers bring actions (including class actions) for privacy breaches.

One area that is often overlooked in privacy diligence is the existence of contractual obligations to comply with the published policies of third-party platforms through which the target's goods or services are provided. In particular, more and more products and services are offered via third-party online platforms (including Facebook, Android and iOS apps, and Amazon Web Services), and usage of these platforms may require compliance with their privacy standards. Similarly, many third-party services used in connection with apps, such as Google Analytics and Google AdSense, require such compliance as part of their terms of service.

Finally, under EU law, when a data "controller" (an entity that determines the purposes and means of the processing of personal data) enters into a contractual arrangement with a data "processor" (a third party that processes personal data on behalf of the controller, such as a service provider), the contract must (i) be enshrined in a written agreement; (ii) require that the data processor act only on the instructions of the controller; and (iii) require the processor to comply with security obligations equivalent to those imposed on the controller under applicable national legislation. Under U.S. federal law, the Gramm-Leach-Bliley Act, as implemented by various federal agencies, generally requires companies that offer financial products or services to individuals to (i) take reasonable steps to select and retain third-party service providers capable of maintaining appropriate safeguards for the protection of non-public records and information and (ii) contractually require such service providers to implement and maintain such safeguards. Similar requirements exist in some cases under U.S. state law (e.g., Massachusetts and Maryland, where companies must require by contract that service providers implement and maintain appropriate data security measures). New York's proposed cybersecurity regulations, which would apply to certain entities operating under a license, registration, charter, certificate, permit, accreditation, or similar authorization under New York banking, insurance, or financial services laws, require such entities to have a policy of including preferred data security provisions in their agreements with third-party service providers.[10] It is therefore important to confirm that the target's agreements with third-party service providers contain provisions that comply with such laws.

- ***Trap:*** *When the target's business provides products/services through third-party platforms or relies on third-party service providers, the target may be required to comply not only with its own privacy policies but also with privacy policies and online terms of service published by these third parties.*

4. Internal Practices, Policies, and Security Measures

Review of the target's published privacy policies and contractual commitments, and the applicable privacy laws to which it is subject, is certainly necessary in order to identify the privacy-related requirements with which the target must comply. However, only an examination of the target's practices and internal policies (including those provided to employees) regarding collection, processing, storage, protection, use, disclosure, transmission, transfer, retention, and disposal of personal data can provide meaningful insight into the target's privacy-related exposure. In addition, a technical overview (even if high level) of the security measures actually employed by the target (such as encryption and breach detection), as well as any procedures and preparedness for breach notification, may be advisable in certain personal data-focused industries.

- ***Trap:*** *A purchaser should be sure to confirm that the target's actions match its words. A target that has sophisticated internal privacy policies and breach procedures still may have significant privacy exposure if it does not make sure that such policies and procedures are notified to all relevant employees and enforced across all of the target's businesses, subsidiaries, or locations.*

B. Privacy-Related Representations in M&A Agreements

Practitioners often rely on a general "compliance with laws" representation to address privacy-related risks, but such a representation does not always provide sufficient protection for a purchaser against privacy and data security risks. The "compliance with laws" representation is often heavily qualified and covers a limited period of time (e.g., the target's operation during the year prior to the transaction), which may not be appropriate for privacy matters. The representation also fails to cover certain issues of concern in the privacy context.

Privacy-specific representations can cover not only compliance with privacy laws but also compliance with contractual obligations (and terms of use) relating to personal data and implementation of data security measures that are not necessarily required by law or contract, such as industry-standard security measures (e.g., payment card industry standards), disaster recovery plans and procedures, and backup equipment and facilities. Such representations may also cover threatened enforcement actions and privacy-related complaints, as well as loss of or unauthorized access to personal data in the past (whether or not constituting a violation of law at

the time), given the reputational damage to which such issues can give rise. Finally, while a "compliance with laws" representation does not include any disclosure requirements, a privacy representation can serve to force the target to disclose information about its policies and practices that is crucial to understanding the magnitude of the privacy risks.

Privacy-specific representations, tailored to include the foregoing matters as appropriate, should be considered whenever the risks discussed in this article are present.

- ***Trap:*** *A purchaser should not assume the "compliance with laws" representation will necessarily cover privacy matters adequately. A privacy representation that is tailored to the risks associated with the target's handling of personal data can be used, when appropriate, to cover important areas beyond mere compliance with applicable law.*

"A word of caution: privacy-related representations in M&A agreements can offer a certain level of comfort to a purchaser, and they should therefore be negotiated carefully, but they are often qualified by knowledge and/or materiality, and any indemnity for breach of the representations is subject to significant limitations."

A word of caution: privacy-related representations in M&A agreements can offer a certain level of comfort to a purchaser, and they should therefore be negotiated carefully, but they are often qualified by knowledge and/or materiality, and any indemnity for breach of the representations is subject to significant limitations. And even if damages are awarded as a result of an indemnity claim relating to breach of privacy-related representations, they may not be sufficient to compensate for the type of public relations and customer relationship damage often associated with privacy failures.

III. Risks Associated with Transferring or Disclosing Target's (or Seller's) Personal Data to Purchaser

M&A transactions often involve the disclosure or transfer of personal data from a seller to a purchaser. This normally includes personal data associated with the acquired target (or acquired assets), such as data relating to employees, customers, users, contractors, suppliers, and business partners. While most personal data is transferred at closing, some disclosures also may occur between signing and closing.

A. Risks Associated with Disclosure Between Signing and Closing

M&A lawyers are not always aware of the risks associated with disclosure of personal data between signing and closing (when signing and closing are not simultaneous). In particular, M&A agreements often contain a clause providing for access to books and records between signing and closing, enabling the purchaser to request certain types of data it reasonably needs, including for purposes of integration planning. But it is a mistake to assume that because a deal is signed, personal data relating to the target business may be shared freely between the purchaser and the seller. While some M&A agreements state that the seller need not provide access to information prior to closing if providing such access would be in violation of applicable law, such a carve-out is not necessarily applied in practice and, in any case, understanding whether a particular disclosure is in violation of privacy laws may be difficult.

1. U.S. Law

Under U.S. law, the pre-closing disclosure of personal data must comply with all relevant state laws, contractual restrictions, and any promises made about the treatment of personal data in the target's published privacy policy. As discussed in Part I, the FTC has made clear that it views failure to comply with published privacy policies as a violation of Section 5 of the FTC Act, which bars unfair or deceptive acts or practices. Relevant state laws include the California Online Privacy Protection Act of 2003, which requires all operators of commercial websites and online services that collect California residents' personal data through a website to identify categories of third-party persons or entities with which the operator may share the personal data.

Ideally, the target's privacy policy will contain a clear statement that a transfer or disclosure of personal data may occur in connection with an M&A transaction, including prior to consummation of the transaction (it may not suffice to state that personal data may be shared "upon" or "following" a merger or sale of the company or its businesses, given that prior to closing the transaction is not consummated). In addition, it will be important to ensure that the purchaser safeguards the information to the extent required by applicable law;[11] does not further disclose the personal data; and does not use it in any way

that violates the applicable privacy policy (including any use that is not necessary for integration planning or consummation of the M&A transaction). It therefore may be advisable for the seller to enter into a "data protection agreement" with the purchaser with respect to such obligations. A data protection agreement also can include requirements to abide by any restrictions contained in the seller's/target's contracts with third parties to the extent related to the personal data shared prior to closing.

2. EU Law

Under EU law, the disclosure of data relating to data subjects must comply with the laws implementing EU Directive 95/46/EC of October 24, 1995 (the "Directive") in each Member State.[12] Generally, for the "processing" (a broad concept that includes transfer or disclosure) of personal data to be permitted, it must be based on one of the grounds enumerated in the Directive, among which the most relevant to a pre-closing M&A-related disclosure are:

- *Legitimate interest of the data controller or the data recipient, provided it is not incompatible with the interests or the fundamental rights and liberties of the data subject*. The so-called "legitimate interest" ground is frequently relied on in M&A transactions since it is open-ended, making it possible to argue that it is in the legitimate interest of the purchaser to receive the data (i.e., to prepare for the acquisition). However, certain data subjects may claim to have an interest in keeping their data confidential, at least until the transaction is close to completion. In practice, it is often advisable to try to wait until all or most of the conditions to closing of the transaction have been satisfied before transferring personal data based on this ground.

- *Consent of the data subject.* In an M&A context, it often is impractical to rely on the consent of the data subjects. The "consent" ground is therefore only used when just a few individuals are concerned, and they have reason to be aware of the contemplated transaction (e.g., major customers whose approval is required in order to assign the customer contracts to the purchaser). Note that the data subject's consent to the transfer may be required in certain circumstances, including when "sensitive data" are involved (e.g., where health, religion, or union membership appear in, or can be deduced from, employee records).[13]

- *Performance of a contract with the data subject*. This ground is typically used in the M&A context when the assets sold include contracts and personal data that must be transferred for these contracts to continue to be performed.

In addition to the existence of one the foregoing grounds for pre-closing disclosure, compliance with EU law generally also would require that the personal data transferred to the purchaser prior to closing not be inadequate or excessive. In other words, the only data fields that should be transferred before closing are those that are necessary for the new employer to prepare for completion of the transaction (such as, in the case of data obtained for HR-related purposes, positions and salaries but potentially not home addresses or bank account details).

Finally, certain additional steps may be required in the EU, particularly notice, inclusion of the European Commission's standard contractual clauses (the "Model Clauses"), and potential Data Protection Authorities ("DPAs") filings. Since these steps are generally similar whether the disclosure/transfer occurs prior to or at closing, we discuss them in Part II.B below.

- ***Trap**: It is a mistake to assume that sharing personal data is allowed once an M&A deal is signed and before it is consummated. In the United States, language in privacy policies may not be broad enough to fully address this situation, and the purchaser's use of such data must be strictly circumscribed in light of state law and contractual obligations. In the EU, several steps must be taken before transferring personal data, and, as a general rule, because the disclosure of data is considered more legitimate as the deal progresses and closing becomes more certain, access to data should be tailored to what is necessary for each phase of the deal.*

B. Risks Associated with Transfers at Closing

At closing, the purchaser will expect to receive all of the personal data related to the acquired business. Depending on the nature of the transaction (e.g., a spin-off of a stand-alone subsidiary) the transferred personal data may in fact remain hosted on the target's systems that are sold as part of the transaction.

1. U.S. Law

Under U.S. law, it will again be important to consider both state law and the FTC Act, as well as any contractual commitments made by the target/seller in agreements involving collection of personal data. In a sale out of bankruptcy, the Bankruptcy Code also will be implicated. In all cases, a decisive factor in analyzing the legality of a transfer of personal data will be the promises contained in the target's published privacy policy.

Asset purchases vs. mergers or share purchases. Arguably, whenever a third-party entity gains access to personal data as a result of an M&A transaction, there is a "transfer" of such personal data that could violate privacy laws. In other words, a "transfer" may technically occur even in a share purchase of a target company pursuant to which all of the company's operations remain unchanged (other than its ultimate control) but following which the purchaser and its affiliates have access to such company's data. However, enforcement activity thus far has not focused on "transfers" that occur in mergers or share purchases and instead has focused only on the eventual uses of such data by the purchaser (as discussed in Part III below). By contrast, in the context of asset sales, even the

data transfer itself has been subject to scrutiny by the FTC, state regulators, and (as applicable) bankruptcy courts. The fact pattern of notable cases has involved a company privacy policy that promised not to sell or transfer personal data to third parties (without any exceptions for sales in a restructuring, asset sale, insolvency, or bankruptcy) and a desire by the company to then sell personal data as a stand-alone asset or in the context of a broader asset sale transaction (such as a sale of a business).

FTC vs. state regulators vs. bankruptcy courts. As described below, the FTC, state regulators, and bankruptcy courts have taken slightly different approaches to such asset sales.

- *FTC approach—Either (A) opt-in consent to the data transfer or (B) purchaser must be in the same line of business as target, must comply with target's existing privacy policy, and must obtain opt-in consent to any material policy changes.* The FTC often cites a settlement it reached with internet retailer Toysmart in 2000 which allowed Toysmart, after it ceased operations, to transfer customer personal data to a third party in spite of its privacy policy stating that such personal data would "never be shared with a third party." The FTC had sued to block Toysmart's sale of its customer database, alleging a violation of Section 5 of the FTC Act. Under the Toysmart settlement, Toysmart was able to sell the customer data but: (i) not as a stand-alone asset; (ii) only to a purchaser engaged in substantially the same lines of business as Toysmart; and (iii) only to a purchaser who agreed to be bound by and adhere to the terms of Toysmart's privacy policy and to obtain affirmative (opt-in) consent from consumers for any material changes to the policy that affect information collected under the Toysmart policy (hereinafter, the "Toysmart Principles").[14] As an alternative to the Toysmart Principles, the FTC proposed (in the RadioShack and Borders cases, discussed below) requiring the target to obtain affirmative (opt-in) consent of the data subjects to the transfer of their data to the purchaser and to purge the data of those who did not consent.[15]

- *State regulators approach in RadioShack—Toysmart Principle "iii" plus notice of the data transfer and right to opt out*. In 2015, Attorneys General in 38 states challenged the bankruptcy sale by RadioShack of its personal data (RadioShack's privacy policy stated: "We will not sell or rent your personally identifiable information to anyone at any time."). The states reached a settlement with RadioShack that limited the type of information to be transferred (e.g., only customer e-mail addresses that were active within the two-year period prior to the petition date, and only specific data fields collected in the five-year period preceding the petition, such as store number, price, and SKU number for a transaction). In addition, the settlement required the purchaser to (a) accept clause "iii" of the FTC's Toysmart Principles (being bound by RadioShack's privacy policies and requiring opt-in consent for any material changes that would affect the transferred data) and (b) provide notice and opt-out opportunities to RadioShack customers to enable them to exclude their personal data from the sale.[16]

- *Bankruptcy court—RadioShack (opt in to material policy changes) vs. Borders (opt out of material policy changes*). While in 2015 the bankruptcy court for the District of Delaware endorsed the above settlement reached between the states and RadioShack, four years earlier, in 2011, the bankruptcy court for the Southern District of New York reached a somewhat different conclusion in the *Borders* case.[17] The FTC raised concerns when Borders planned to sell personal data of approximately 45 million customers to Barnes & Noble in a bankruptcy auction. Borders' privacy policy had changed over time, initially stating "we do not rent or sell your information to third parties" and later stating that customer information might be transferred if Borders engaged in an M&A transaction. The bankruptcy court declined to accept the FTC's approach described above and instead required Barnes & Noble to (i) adopt a privacy policy similar to the Borders' policy and provide existing customers an ability to opt out of any material changes to the policy and (ii) provide notice and a data transfer opt-out mechanism, as in *RadioShack*. The court also required Barnes & Noble to honor prior requests by consumers (made to Borders) to opt out of receiving marketing messages (unless such consumers were also Barnes & Noble customers who had not opted out of marketing messages).

In each of the above cases, there was no express provision in the applicable privacy policy allowing for the sale of personal data in the event of a restructuring, asset sale, or bankruptcy (or even in the event of a merger or acquisition). The inclusion of such a provision is advisable, not only in privacy policies but also in contracts containing commitments with respect to treatment of personal data.

- ***Trap**: While "transfers" of personal data in connection with mergers or share purchases have not been criticized by regulators to date, asset sales involving transfer of personal data have been subject to close scrutiny in the United States, and certain steps may be required when planning such transfers in order to prevent exposure to potential liability.*

2. EU Law

In the EU, a transfer of personal data at closing as part of an M&A transaction requires showing that at least one of the grounds for transfer discussed in Part II.A above ("legitimate interest," consent, or necessary for performance of a contract) is found. This should be easier than in the case of a pre-closing disclosure given that once the

transaction has been completed, the purchaser should have a "legitimate interest" in processing the acquired personal data. In addition, the following steps should be considered:

- *The data subjects should be informed of the transfer*. The seller should give the data subjects certain information about the transfer of their data to a third party no later than at the time of the transfer, unless such disclosure would "involve a disproportionate effort." Such information does not necessarily need to be given to each data subject individually (a posting on a website may suffice, depending on the circumstances). A right to opt out of the transfer may need to be granted.[18]

- *Additional steps may have to be taken in the case of transfers of data outside the European Economic Area ("EEA").* EU law imposes stringent regulatory constraints on the transfer of personal data outside the EEA to a country that is not deemed to have an adequate level of data protection,[19] which includes the United States, unless the transfer is to a company that self-certified under the EU-U.S. Privacy Shield.[20] Consent of the data subjects will render the transfer lawful under EU law, but it is often difficult or very burdensome to obtain. In the absence of Privacy Shield certification or individual consent from the data subjects, an M&A-related transfer should be made only after a personal data transfer agreement that incorporates the Model Clauses has been entered into between the parties. The Model Clauses place recipients of personal data under contractual obligations similar to those required in the EU. Note, however, that as discussed below, in certain EU countries (e.g., France) the data transfer agreement (containing the Model Clauses) would need to be approved by the local DPA, which could take up to a few months and could render the Model Clause option inappropriate in some cases.

  • ***Trap****: The decisive factor for determining whether a transfer of personal data outside the EEA occurs (which may require usage of Model Clauses or self-certification under the EU-U.S. Privacy Shield) is not whether the seller/target is an EU corporation while the purchaser is not; it is whether personal data stored within the EEA is transferred (physically or electronically) to locations outside the EEA by an entity that is subject to EU jurisdiction.*

- *Verify whether filings with Data Protection Authorities must be made*. Depending on the national law applicable to the seller, the target, or the purchaser, the transfer of personal data may have to be notified to or authorized by one or several DPAs.[21] Filing requirements vary among Member States and should be reviewed on a case-by-case basis. Planning ahead is important, as a DPA approval, if needed, may take a long time. By preparing for this in advance, a purchaser can ensure minimum disruption to the target's personal data processing activities.

IV. Risks Associated with Post-Acquisition Integration of Personal Data

Immediately after closing, the purchaser must consider how to integrate the target's personal data and the target's IT systems into its own data and systems. Problems arise if either the target's practices do not comply with the purchaser's privacy policies (or contractual obligations) or if the purchaser's practices do not comply with the target's privacy policies (or contractual obligations that survived the sale, including those assumed by the purchaser).

A. Target's Practices and Policies More Robust Than Purchaser's

Even where the consummation of an M&A transaction and the correlating "transfer" of personal data to the purchaser does not violate privacy laws, problems arise when the purchaser's practices are below the standard the target committed to in its pre-acquisition privacy policy. For example, the target's policy may state that certain types of information are not collected or that personal data is used only for certain purposes, shared only with certain third parties, stored only in certain geographic regions, or is de-identified or encrypted. However, the purchaser may have different privacy policies and practices that may conflict with these statements.

Facebook is currently under scrutiny worldwide as it grapples with the aforementioned risks resulting from its acquisition of WhatsApp in 2014. Although at the time of the acquisition WhatsApp's privacy policy contained an express provision stating that it reserved the right to transfer users' personal data to a third party in the event of a merger or acquisition, the FTC took the position that post-acquisition, WhatsApp had to continue to abide by its original privacy policy (which promised not to share personal data with third-party companies for commercial or marketing use, except with users' consent or as part of programs or features, users would be able to opt in or opt out of). At the time the sale was announced, both Facebook and WhatsApp promised consumers that after the acquisition, WhatsApp would continue to operate autonomously and that nothing would change for its users. However, in August 2016, WhatsApp changed its privacy policy to allow it to share customers' personal data (including pre-acquisition data) with Facebook unless customers opted out of such sharing within 30 days. Consumer privacy watchdog groups and other organizations filed a formal complaint with the FTC and urged the FTC to investigate WhatsApp and Facebook.

Guidance on how the FTC views this issue in the context of M&A is found in the FTC's "business blog" published on March 2015, which was prompted at least in part

by Facebook's acquisition of WhatsApp.[22] The FTC blog set forth several important principles:

- The target's pre-acquisition policies continue to govern with respect to personal data collected by the target. As the FTC stated: "One company's purchase of another doesn't nullify the privacy promises made when the data was first collected."
- With respect to data collected by the target prior to the acquisition, the purchaser may either comply with the target's pre-existing policies or allow opt in. The purchaser can simply abide by the target's pre-acquisition promises, i.e., handle the data as promised when the target collected it from consumers. Alternatively, if it wishes to materially change how the data is processed, it must obtain affirmative (opt-in) consent from the individuals to whom the data pertains.
- With respect to data collected by the acquired business or target (if it survives) post-acquisition, the purchaser must provide notice & opt out. If the purchaser desires to change its practices going forward with respect to newly collected personal data, it will need to provide sufficient notice of the change and an opportunity for users to opt out. Per the FTC blog: "Simply revising the language in a privacy policy or user agreement isn't sufficient because existing customers may have viewed the original policy and may reasonably assume it's still in effect. Although it may not be necessary to provide affirmative express consent, the notice and choice must be sufficiently prominent and robust to ensure that existing customers can see the notice and easily exercise their choices."
- With respect to any data of an individual who does not opt in (for pre-acquisition data) or who exercises the right to opt out (for post-acquisition data), the purchaser will have to comply with the applicable pre-acquisition privacy policy of the target.

Thus, where a target's privacy policy and data privacy practices are more robust than the purchaser's, if the purchaser wishes to integrate the target's personal data into its systems or otherwise use the data collected by the target before the acquisition, the purchaser may need to bring its own data privacy practices into compliance with the target's applicable privacy policy. If updating the purchaser's practices and systems is not feasible or desirable, the purchaser will need to segregate the data.

Finally, the target may collect certain personal data that is subject to additional regulation (such as health care data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the personal data of children younger than 13 subject to the Children's Online Privacy Protection Rule). If the purchaser wishes to integrate such personal data and use it, the purchaser will need to ensure compliance with all relevant regulations.

We note that the above discussion relates to U.S. law, where most of the focus is on the target's and purchaser's privacy policies and promises. In the EU, the focus in review of post-acquisition practices (assuming the transfer of the data itself is lawful as discussed in Part II.A above) is on the purposes for which the data initially was collected. The use of the data by the purchaser must be in a manner consistent with the specified (and legitimate) purposes for which it was obtained by the target in the first place. As an illustration, in the case of data obtained for HR-related purposes such as payroll and administrative management, the data should continue being used only for these same purposes by the purchaser.

- ***Trap**: As a purchaser, it is not enough to establish that the target's practices are compliant with your privacy policies. You may be violating the law if your use of data collected by the target does not comply with the target's policy (or, in the EU, if your use of such data is inconsistent with the specified purposes for which it was collected by the target).*

B. Target's Practices and Policies Less Robust Than Purchaser's

Another set of problems arises if a target's data privacy practices are less protective of privacy than the purchaser's and are therefore incompatible with the purchaser's privacy policies (e.g., the personal data collected by the target may contain credit card information or other data fields that the purchaser promises not to collect or store, or the target may use third-party service providers under terms that are inconsistent with statements in the purchaser's privacy policy). While the purchaser's privacy policies may be amended to remove promises that are incompatible with the practices of the target, the amended policy will be effective only for newly-collected personal data (data collected after the date the amended policy is made effective) and, consistent with the FTC blog, customers must receive notice of the change and an opportunity to exercise an opt-out choice. In addition, the purchaser may suffer a reputational hit from lowering the protections in its privacy policy. Furthermore, the purchaser will need opt-in consent for any changes that will affect customers' previously collected data.

The most reasonable approach will likely be for the purchaser to either (1) maintain the target as a separate entity/division that does not use the purchaser's data or (2) bring the target's practices into compliance with the purchaser's previous promises (though this could involve significant costs).

- ***Trap**: Even where the "transfer" of personal data to the purchaser resulting from an M&A transaction is lawful, post-closing processing of personal data, either by the purchaser (of target's data) or the surviving target (of purchaser's data) that conflicts with privacy policies applicable when such data was collected can lead to liability.*

V. Conclusion

We have outlined some of the complex privacy issues that arise at each stage of an M&A transaction. Prior to signing, a purchaser's due diligence will involve multiple areas of inquiry to determine all potential risks associated with the target's existing privacy-related liabilities, and for greatest protection, privacy-specific representations in M&A agreements may be warranted. Between signing and closing, both sellers and purchasers should remain cautious in the disclosure of personal data and should seek counsel both with respect to the content of any disclosures and the disclosure process. After closing of the transaction, the purchaser will need to consider carefully what steps must be taken to enable its use of the acquired data and to ensure such use complies with all applicable laws. Given the rapidly evolving nature of privacy laws, it is advisable to consult with privacy counsel at each stage of a transaction to most effectively mitigate these and other associated risks.

Endnotes

1. Throughout this article, we use the term "privacy" (or "privacy issues" or "privacy laws") broadly as including cybersecurity, data protection and data security as related to personal data (and related issues and laws).
2. This article focuses on U.S. and EU law, but we note that several other jurisdictions have passed or are adopting strict privacy laws. Among those are countries recognized by the European Commission as having an "adequate level" of protection for all or certain types of personal data processing (i.e., as of the date of this article, Andorra, Argentina, Canada (commercial organizations), the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay—please visit http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm) as well as other states such as Brazil, Singapore and South Korea. In any cross-border transaction, the laws of all relevant jurisdictions should be examined.
3. The FTC has also been successful in obtaining monetary awards against companies in actions enforcing its orders. Notably, in 2015, LifeLock agreed to a $100 million settlement with the FTC, after the FTC charged that LifeLock violated the terms of a 2010 federal court order requiring the company to secure consumers' personal information and prohibiting the company from deceptive advertising.
4. For further information on the new GDPR framework, please refer to our May 13, 2016 Alert Memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201650.pdf.
5. In 2014, the FTC filed a complaint against Fandango and Credit Karma charging that the companies had deceived consumers. Both had made representations that they could secure their customers' personal data, but according to the FTC, both had failed to properly implement SSL encryption.
6. The ICO's "*Privacy notices—code of practice*" can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/.
7. Additionally, Member State consumer protection laws should also be considered as these may provide for additional information requirements (see, for example, the German Act Against Unfair Competition, which prohibits unfair commercial practices).
8. *See* https://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917comp0423047.pdf.
9. *See* https://www.ftc.gov/news-events/press-releases/2011/09/ftc-seeks-protection-personal-customer-information-borders.
10. For further information on New York's proposed cybersecurity regulations, please refer to our September 20, 2016 Alert Memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-word-version-201685.pdf.
11. For example, Massachusetts General Law Chapter 93H and its regulations 201 CMR 17.00 impose requirements on all companies who receive, store, maintain, process or otherwise have access to personal data of the state's residents to develop, implement and maintain a comprehensive information security program that contains administrative, technical and physical safeguards to protect the data.
12. While the Directive provides a harmonized regulatory data protection framework that is applicable throughout the EU, there are a few areas where national law differs in each Member State. Starting on May 25, 2018, the Directive and the national laws implementing it will largely be replaced by the GDPR, which will enhance existing legal requirements, create new rules and set out significant fines for organizations failing to comply. For further information on the key changes to be anticipated under the GDPR regime, please refer to our May 13, 2016 Alert Memorandum (https://www.clearygottlieb.com/news-and-insights/publication-listing/general-data-protection-regulation-key-changes-and-implications).
13. Sensitive personal data may be transferred only where the data subject has provided his or her explicit and fully informed consent, or where a legal obligation exists in the context of employment which makes the transfer necessary. The advice of local counsel should be sought before relying on the "legal obligation" ground in connection with the transfer of sensitive employee data.
14. For the Stipulation and Order Establishing Conditions on Sale of Customer Information, *see* https://www.ftc.gov/sites/default/files/documents/cases/toysmarttbankruptcy.1.htm.
15. *See* FTC letter to the court-appointed Consumer Privacy Ombudsman in *RadioShack*, dated May 16, 2015, https://www.ftc.gov/system/files/documents/public_statements/643291/150518radioshackletter.pdf.
16. *See In re RadioShack Corporation, et al.*, No. 15-10197 (BLS) (Bankr. D. Del.).
17. *See In re Borders Group, Inc., et al.*, No. 11-10614 MG, 2011 WL 5520261 (Bankr. S.D.N.Y. Sept. 27, 2011).
18. In 2001, the French DPA declared (in the context of a merger of three companies) that personal data files may only be assigned or made available to a third party on the condition that data subjects be given advance notice as well as the right to object to such transfer. In Germany, it is necessary to provide notice of the transfer in the context of the transaction with a deadline to object where the transferred data goes beyond so-called "list data" (name and postal address). The Bavaria DPA issued fines to a buyer and target in an asset deal in 2015 where customer data was transferred without the parties providing the customers with a deadline to object to the transfer prior to the transaction.
19. *See supra* note 2.
20. Commission Implementing Decision of 12.07.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (the "EU-U.S. Privacy Shield"). For further information on the EU-U.S Privacy Shield and the invalidation of its predecessor (the EU-U.S. Safe Harbor), please refer to our August 2, 2016 Alert Memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201679.pdf).
21. The GDPR provides for a "*one-stop-shop*" mechanism under which data controllers established in the EU will be able to register with one DPA only (in their country of "main establishment").
22. *See* https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.