NYSBA FALL 2013 | Vol. 31 | No. 2

Inside

A publication of the Corporate Counsel Section
of the New York State Bar Association

Message from the Chair

The summer is well under way as I reflect on the first half of the year. Most recently our CLE Committee presented a program on Cyber Liability, Data Loss and Privacy Claims hosted by Brooklyn Law School. The panel included a broad array of professionals including inside and outside counsel and risk management, insurance and technology managers. The program was well attended and a number of our members expressed interest in becoming more involved with the Section. You can read more about the program and data security law inside.

The Kenneth G. Standard Internship Program continues to be a shining star of our Section. Our Section was recognized by the New York State Bar as a Section Diversity Champion for 2013. Many thanks go to David Rothenberg of the Ayco Company L.P., who works tirelessly to ensure the continued success of the program. These internships are supported primarily by your dues and the generous support of our host companies.

As I write this message, planning is going on for our 5th Corporate Counsel Institute, to be held in Manhattan on November 22nd. The full day program will offer CLE on such topics as Employment Law, Alternative Fee Arrangements, Ethics, Social Media, Making Sense of Insurance Policies and Intellectual Property. Please mark your calendars and plan to attend. I look forward to seeing you there.

Howard Shafer

Inside

Inside *Inside* 2
(Janice Handler)

Law and Technology

Negotiating a One-Sided Limitation of Liability 3
(Mark Grossman)

International Trade Regulation of Internet Businesses 5
(William B. Bierce)

Six Things Every In-House Counsel Needs to Know About Employee Privacy Rights 14
(Joel J. Greenwald)

Web Site Checklist: Minding Your Company's Virtual Storefronts 16
(Jessica R. Friedman and Paul S. Ellis)

How (Not) to Make a Contract on YouTube 20
(Clara Flebus)

Being Prepared When the Cloud Rolls In 23
(Natalie Sulimani)

Corporate Counsel Section's Spring CLE Presentation Cyber Liability, Data Loss and Privacy Claims—Preparing, Protecting and Defending 27
(Tara A. Johnson and Elizabeth C. Hersey)

The "Reasonable" Perils of Data Security Law 30
(Yanai Z. Siegel)

Alternative Dispute Resolution (ADR) Law—Why Tech Lawyers Should Care, and What They Should Do About It 32
(David J. Abeshouse)

The Duty to Preserve and the Risks of Spoliation—How Organizations Can Preemptively Limit the Costs of Electronic Discovery 39
(Jamie Weissglass and Rossana Parrotta)

What's New

Inside Books: *Salt Sugar Fat* by Michael Moss 44
(Reviewed by Janice Handler)

Editors: Janice Handler and Allison B. Tomlinson

Inside Inside

I went to law school in a decade when computers were very big rectangles stored in their own computer rooms. (I know I am dating myself but what the heck!) Rutgers Law School—always in front of a trend—offered one of the first courses and clubs in "Computer Law." Many of us, immersed as per the politically correct times in the "big issues," were going to become civil rights lawyers (we didn't) and we rolled our eyes at the computer law thing as an affectation by those who couldn't make Law Review. Know what? The joke was on us. This was the next big thing—and still is.

The development of technologies and their impact on legal substance, processes, and output may be the biggest thing since Henry II brought the common law to England. The General Counsel of a corporation cannot afford to view techno-law as a niche and live as a Luddite. She must get with the program—and *Inside* is here to help.

This Law and Technology special issue is crammed with not only legal analysis but practical pointers. Mark Grossman and Joel Greenwald (two of the most practical and accessible legal writers I know) offer checklists on negotiating liability clauses in tech deals and employee privacy rights respectively. For those of you who prefer lengthier legal analysis (and lots of footnotes), William B. Bierce writes on "International Trade Regulation of Internet Businesses." David Abeshouse, a practitioner in ADR, tailors his comprehensive discussion of ADR options specifically to technology companies.

An issue of growing importance to all of us is cyber security, and we have an excellent article on this topic by Yanai Siegel as well as a summary by Tara Johnson and Elizabeth Hersey of the Section's Spring CLE program on this topic.

More practical advice issues from Clara Flebus on "How (Not) to Make a Contract on YouTube"and Paul Ellis and Jessica Friedman on protecting your company's website. Natalie Sulimani, a tech expert, who has written for us in the past, discusses the ethics of cloud computing (and we are glad to know there are any).

On a more personal note, I am proud to present a piece by my former Fordham Law School student, Jamie Weissglass (with her colleague Rossana Parrotta). Jamie is now Manager of Business Development at HuronLegal, where she deals with litigation readiness amongst other things. She writes on limiting costs of e-discovery, a subject of interest to all of us.

It gives me immense pride and pleasure to see a student bloom like Jamie has—just as it gives me pride and pleasure to offer you an issue of *Inside* which is as expert and user friendly as is this one.

Janice Handler

Janice Handler is co-editor of *Inside*. She is the former General Counsel of Elizabeth Arden Cosmetics Co. and currently teaches Corporate Counseling at Fordham Law School.

Negotiating a One-Sided Limitation of Liability

By Mark Grossman

When clients come to me asking for an evaluation of their remedies because their tech deal has gone sour, the single worst remedy and lawsuit killer I often find in existing tech contracts is that "standard" limitation of liability clause. It never ceases to amaze me how people do not pay attention to these provisions as they blithely sign off on a one-sided agreement. It's just one little clause and yet it can cause so much damage.

Here is an example of the type of a limitation of liability provision that you will find in tech agreements—this one is from a Software as a Service agreement:

> Vendor shall have no liability with respect to Vendor's obligations under this agreement or otherwise for consequential, exemplary, special, incidental, or punitive damages even if Vendor has been advised of the possibility of such damages. In any event, the liability of Vendor to Customer for any reason and upon any cause of action shall be limited to the lesser of the amount paid to Vendor under this Agreement or $_____. This limitation applies to all causes of action in the aggregate, including without limitation to breach of contract, breach of warranty, negligence, strict liability, misrepresentations, and other torts.

No Tricks Up My Sleeve

Now, if your clients signed off on a provision like that because they figured that you would find some technicality to overcome it if necessary, I think they have made a serious mistake. As a generalization, limitation of liability provisions mean what they say and say what they mean. Judges can read, and a judge would more than likely enforce it as written in a contract between two sophisticated parties. I think courts correctly read these provisions as allocation-of-risk provisions that the court should enforce as written.

While the sample provision above was clearly one-sided, courts are not in the business of rewriting deals to make them fairer. Simply put, that is the purpose of the negotiation. If your clients failed to negotiate a more balanced limitation of liability provision, they will almost certainly have to live with the consequences of their failure if there is a dispute down the road.

It's the Norm

When you negotiate your client's agreement and tell the vendor that the limit of liability has to go, you are likely to get a blank look. You know, it is the same one you get from your kids when you remind them that they have not given you your change.

I know what I say because when I represent the seller of tech services I say things like: "Limits of liability are the norm." "Everybody uses them." "We have never done a deal without one." "We would have to increase the price dramatically because of the additional risk we would be assuming."

Ironically, all of this is true. So, we are done, right? Wrong. A skilled and experienced negotiator can make all the difference here. This is where you as the lawyer on the deal can make a meaningful difference. (A difference your clients may not appreciate, but that is a different discussion.)

While it is the norm to see limits of liability in deals like software-as-a-service, cloud computing, licensing, telecom and outsourcing deals it is not necessarily true that they are all as onerous as my example. While getting the other side to remove a limit of liability completely may be like climbing Everest and wholly unrealistic, making it fairer is not necessarily so hard if you ask for the right things.

The Negotiation

If the vendor will not eliminate the limit of liability provision, which no well-represented and solvent tech, telecom, or outsourcing company would, you have to start pecking at the provision to put a chink in its armor. So let us go back to my example where the vendor's liability is "limited to the *lesser of* the amount paid to Vendor under this Agreement or $_____" (emphasis added) and look at some ways to start pecking at it.

Let us say your client has a $5 million deal cooking, which calls for five equal payments over five months as work progresses. Let us say that after the first month it becomes clear that the work the vendor is doing is causing more harm than good, so your client rightly refuses to make the second $1 million payment. Finally, let us say that the vendor has somehow caused your client damages valued at $2 million.

Your client might naïvely think that you could easily obtain a judgment for their two-million dollars. However, you are not likely to achieve what your client might think is the fair result because the limitation of liability provision limited recovery to the amount paid—i.e., a refund. Therefore, as written, no matter what the vendor does and no bad how bad it is, the most your client gets is a refund of the $1 million paid to date. The vendor risked nothing!

My first attempt to chink its armor would be to ask it to agree to a limit of liability of an amount equal to the total value of the contract ($5 million) and not the amount paid to date. Failing that, I might ask for some multiple of the amount paid to date.

As an aside, in the world of service deals like software as a service, a typical limitation of liability is equal to the fees paid by your client to the vendor over some relatively short period. In my experience, vendors typically start with three to six months of fees as their limitation of liability. I can usually get that up to 12 to 18 months, but my goal every time is at least 24 months.

When your contract bases the limitation of liability provision on fees over a certain period, you must be sure to draft the provision to deal with the situation of a breach occurring before the contract has been in place for as long as that certain period.

So for example, if your contract bases the limitation of liability on the fees paid over the last 24 months and the breach occurs in the fifth month, your contract should include the concept that if the breach occurs before the 24th month of the contract term, then the limitation of liability would be the average monthly fee up until the time of the breach times 24 months.

Another approach to chinking vendors' armor is "reciprocity." In fact, I would say that no single word is more important in moving a one-sided agreement toward the middle than reciprocity. What is good for the vendor is good for your client. Do not be embarrassed to ask. They certainly were not embarrassed to make the provision one-sided to their advantage.

The idea is that the most that the vendor could ever recover from your client is equal to the most your client could recover from the vendor. Why should the vendor have a protective limit, but not your client? The vendor will not like that, but it is hard to argue against the proposal's inherent fairness.

Yet another approach would be to carve out an exception if the vendor infringes the intellectual property rights of a third party. In the example as written, if the vendor "created" software for your client and your client is sued for millions for infringing some third party's copyright, your client could end up with millions in liability. Still, your client could only recover up to the amount of the limitation of liability from the vendor as the party who really caused the infringement. Again, the provision is simply not fair nor is it a fair allocation of risk. Therefore, my position is that liability for indemnification arising from the infringement of intellectual property should be excluded from the limitation of liability.

Then, I go farther on all third-party indemnification issues and take the position that vendor should be fully responsible for all third-party damages of every kind and nature including third party's property damage and bodily injury claims. As with the copyright situation, it seems inherently unfair that your client should pay unlimited amounts of money to a third party because of something your vendor did.

A few other items that I want excluded from a limitation of liability include willful or intentional torts, claims arising from the vendor's breach of a confidentiality provision, a claim arising from the vendor's improper use of personal identifiable information, any claim for indemnification other than for IP which we discussed above, claims arising from the vendor's failure to comply with the law, and vendor's intentional breach of contract.

It is almost a waste of time to put effort into negotiating a contract to have it emasculated by a one-sided limitation of liability provision. Do not let that happen to your client. While it may be true that these types of provisions are "normal," do not assume that the one in the vendor's proposed agreement has dropped from the heavens as the only way it can be.

Mark Grossman is a business lawyer who began focusing his practice on technology over 20 years ago. He is also an author and frequent speaker on technology, outsourcing, and the art and science of negotiating deals. Mark is AV-rated by Martindale-Hubbell, the highest level attainable and his peers chose him to appear in the last 11 editions of *The Best Lawyers in America*. Mark's clients range from startups to Fortune 100 companies. Mark authored the book *Technology Law—What Every Business (and Business-Minded Person) Needs to Know*, and released a revised edition in 2009.

International Trade Regulation of Internet Businesses

By William B. Bierce

I. Introduction

A. E-Businesses Go Global

In only 20 years, the Internet has become an ocean for the cross-border transport of information, goods, services and software. New forms of virtual e-business enterprises have rapidly scaled into global enterprises and become a major component of global trade. Nimble, disruptive new virtual enterprises have emerged as software-driven SaaS services, highly scalable and globally uniform,[1] or as IT-enabled remote services.[2] Internet "e-business" models have reshaped the global workforce, decentralized company operations away from headquarters, recentralized employees into shared services and outsourced service centers and created work-at-home industries.

Given their ubiquity and disruption, e-businesses have also become the targets of political power, with potential for becoming victims of censorship or exclusion from local markets for political reasons.[3] E-businesses also face a new political world, dependent upon on global legal protections of intellectual property and constrained by conflicting laws on operations and taxation. They must thread the needle across complex regulation, particularly on privacy, data protection and consumer protection.

The current legal framework of global business and taxation of remotely provided wares was developed in the era before large-scale Internet businesses. Current developments in "international trade regulation" of Internet-enabled businesses are anticipated to change U.S.-EU bilateral "free trade" relations and national rights to regulate "Internet freedoms" under a UN agency.[4] These changes will impact opportunities for startups, equity investments and online or remote business services.

B. Current Trade Regulation of E-Businesses

Trade regulation reflects national treatment of imports. Abuses by exporting countries are typically resolved by the imposition of countervailing duties to offset foreign export subsidies, anti-dumping duties to prevent import sales at "less than fair value," and other forms of politically inspired economic retaliation against the "abusive" foreign country's exports. In the context of international e-business, "trade regulation" and "free trade" relate to market access and non-tariff barriers, where traditional anti-abuse rules are unlikely to be needed.

International trade regulation involving free trade agreements (FTAs) represent a partial relinquishment of sovereignty in order to gain economic benefits.

1. WTO Multilateral "Free Trade" Framework

The World Trade Organization adopted the Uruguay Round trade agreements in 1994. The WTO Trade Agreements on Intellectual Property ("TRIPs"), Trade in Services and Trade-Related Investment Measures ("TRIMs")[5] require member countries to provide non-discriminatory treatment, to make trade concessions available to all others under the "most favored nation" principle, and maintain transparency in regulation of trade. As a result, the global service economy expanded through outsourcing and offshoring of IT-enabled services.

2. UN's ITU Multilateral "Regulatory" Framework

Until December 2012, there was no multilateral regulation of "Internet freedoms." In a surprise move, in December 2012, 89 countries adhered to International Telecommunications Regulations (ITRs) of the International Telecommunications Union, a UN body consisting of countries as the only members. The ITRs claim to be a "binding global" treaty "designed to facilitate international interconnection and interoperability of information and communication services, as well as ensuring their efficiency and widespread public usefulness and availability." The treaty sets out general principles for "assuring the free flow of information around the world, promoting affordable and equitable access for all and laying the foundation for ongoing innovation and market growth."[6]

However, the treaty also assures the rights of governments to regulate the uses of the Internet locally. Hence, it was not accepted by the U.S., India or major European countries because it has the capacity to limit Web freedoms by giving to the ITU jurisdiction over the Internet's operations and content, including the right to censor, reduce telecommunications speeds and limit access to the Internet.[7] As a result, non-signatories to the ITRs have an incentive to develop their own form of Internet freedoms by separate trade negotiations.

II. EU-U.S. Free Trade Negotiations Under TTIP

In response to a global economic slowdown and perceived abuses (such as by "free-riders" and state-owned enterprises, or SOEs) under the WTO agreements, the EU and the U.S. have begun bilateral free trade negotiations in July 2013. Called the Transatlantic Trade and Investment Partnership (TTIP), such trade negotiations seek to promote transatlantic economic growth, not only in e-business, but also in aviation, automobiles, financial services and other important consumer sectors. At France's insistence, it might exclude "cultural" wares such as en-

tertainment delivered in any form (including online) and arts.[8]

III. Conflicts of Law as Barriers to EU-U.S. Trade in E-Business

U.S. IT- and e-businesses have a lot at stake in TTIP. Current non-tariff barriers limit U.S.-EU trade in IP, IT and e-businesses. Currently, more than 13 million American and EU jobs are already supported by transatlantic trade and investment.[9]

A. EU Restrictions

American e-businesses must comply with European Union internal rules when they sell online to European residents. Such European rules include the Directive on Distance Selling,[10] the Data Protection Directive[11] and EU norms on environmental, health and safety of consumer products. Given relatively low tariffs, the comparatively high compliance costs of non-tariff trade barriers in IP, IT, e-businesses and other sectors have become a target for transatlantic trade liberalization.[12]

B. U.S. Restrictions

European sellers face the same problems with a fragmented federal regime of federal, state and local regulation of Internet-based sellers in privacy, data breach notification, value-added taxation and consumer protections such as safety norms[13] and warranties for consumer products.[14]

IV. Harmonizing the Conflicts: The TTIP Agenda

Negotiations between the EU and the United States were scheduled to begin in early July 2013 to boost economic growth in the United States and the EU. As announced by the White House, TTIP aims to:

- Further open EU markets, increasing the $458 billion in goods and private services the United States exported in 2012 to the EU, our largest export market.
- Strengthen rules-based investment to grow the world's largest investment relationship. The United States and the EU already maintain a total of nearly $3.7 trillion in investment in each other's economies (as of 2011).
- Eliminate all tariffs on trade.
- Tackle costly "behind the border" non-tariff barriers that impede the flow of goods, including agricultural goods.
- Obtain improved market access on trade in services.
- Significantly reduce the cost of differences in regulations and standards by promoting greater [regulatory] compatibility, transparency, and cooperation, while maintaining our high levels of health, safety, and environmental protection.
- Develop rules, principles, and new modes of cooperation on issues of global concern, including intellectual property and market-based disciplines addressing state-owned enterprises and discriminatory localization barriers to trade.
- Promote the global competitiveness of small- and medium-sized enterprises.[15]

Arbitration, tariff elimination, non-tariff barriers (especially privacy and data protection rules) are of most concern to e-businesses.

A. Arbitration of Trade-Related Investment Disputes

Under TTIP, U.S. companies investing in European Union would be entitled to a special arbitration under well-established principles for disputes between foreign investors and host governments. Such disputes involve involuntary "taking" (or "indirect appropriation") of private property for governmental purposes. While the European Commission asserts that there have been no such disputes involving intellectual property or other property,[16] there is an increasingly fine line between "police power" and "public order" rights of governments and the "taking" of private property.

For example, a "taking" of an Internet service provider's business might occur when a government shuts down access in order to reduce public debate on social networks. Google's experience in facing interruptions in access and then exiting from mainland China to Hong Kong and then entirely out of China is instructive on the risks of ISPs and e-businesses. A "taking" may also occur when "extortionate" regulatory conditions to market access are imposed that exceed a reasonable state police power.[17]

Use of an arbitral forum in international investment disputes is a voluntary erosion of state sovereignty. As included in bilateral investment treaties (BITs) that the U.S.[18] and the EU[19] each have with less developed countries, such arbitrations have been effective in keeping host governments from adopting unusual regulations that stifle commerce and deplete the value of foreign investment. By yielding such sovereignty across the Atlantic, the negotiators hope to inspire others (e.g., India and China) to follow the model.

B. Elimination of U.S.-EU Tariffs

1. *Low Tariffs.* By definition, a tariff is the customs duty payable upon importation, before goods (or ser-

vices, investments or intellectual property rights and goods and services incorporating such rights) can enter the local market. Since current tariff levels between the U.S. and the EU are approximately 4%, the elimination of tariffs will not be so important as a trade goal.

2. *Brazil's Tariffs on Importation of Foreign Services.* As a goal for liberalization of trade, "elimination of tariffs" should also apply to import taxes on foreign-sourced services. Brazil has adopted a regime of tariffs on imported services. Dubbed the ISS, the tax applies to foreign services delivered remotely via the Internet or from a foreign source. Foreign services subject to the ISS tax include Software as a Service (SaaS), remote IT assistance (help desk), outsourced software application development and maintenance (ADM) and online training and educational courses.[20] By targeting such practices of the Brazilians, TTIP could open markets for U.S. and EU service providers to provide such online or remote services to Brazilian customers, assuming Brazil were to join on a multilateral basis later.

C. Cutting "Behind the Border" Non-Tariff Barriers

1. *Why NTBs Are So Difficult to Free Trade.* The TTIP negotiations target "barriers that lie behind the customs border—such as differences in technical regulations, standards and certification."[21] By definition, a non-tariff barrier (NTB) impedes the free flow of goods, services, investment and/or intellectual property without imposing any tariff on importation. NTBs are not necessarily "technical barriers to trade' (TBTs).[22] NTB's reflect a country's regulatory framework for protection of consumers, safety, environment and health. For example, the EU and the U.S. each impose consumer product safety standards, but the particular norms are different. As a result, there is little possibility for selling automobiles across the Atlantic.

NTBs are politically sensitive just because they reflect local legislation and administrative rulemaking that are supposedly "neutral" and "technical." However, where technical standards are equivalent, they can be used for protectionism.

The 1994 WTO agreement on the elimination of TBTs barriers opened the door to further negotiations to eliminate NTBs.[23] In Internet businesses, the primary NTBs are those that protect consumers from fraud, invasion of privacy (or one's "private life"), child pornography, civil rights abuses and unfair trade practices. Both the EU and the U.S. have elaborate regimes for consumer protection.

2. *TTIP Agenda on NTBs.* The impact of any TTIP agreement would be felt mostly in non-tariff barriers such as consumer safety, privacy, data protection and other compliance requirements for e-businesses:

- The objectives of the [NTB] chapter would be to yield greater openness, transparency, and convergence in regulatory approaches and requirements and related standards-development processes, as well as, inter alia, to reduce redundant and burdensome testing and certification requirements, promote confidence in our respective conformity assessment bodies, and enhance cooperation on conformity assessment and standardization issues globally.
- Cross-cutting disciplines on regulatory coherence and transparency for the development and implementation of efficient, cost-effective, and more compatible regulations for goods and services, including early consultations on significant regulations, use of impact assessments, periodic review of existing regulatory measures, and application of good regulatory practices.
- Provisions or annexes containing additional commitments or steps aimed at promoting regulatory compatibility in specific, mutually agreed goods and services sectors, with the objective of reducing costs stemming from regulatory differences in specific sectors, including consideration of approaches relating to regulatory harmonization, equivalence, or mutual recognition, where appropriate.
- A framework for identifying opportunities for and guiding future regulatory cooperation, including provisions that provide an institutional basis for future progress.[24]

3. *"Harmonization, Equivalence and Mutual Recognition" for NTBs.* Current differences in regulatory standards cost businesses substantial compliance costs and delay new product introduction. The TTIP negotiators would pursue the reduction of such non-tariff barriers in three possible ways.

a. *Mutual Recognition.* First, each side could agree to mutually recognize foreign regulations as "legally adequate" to meet its own regulatory purposes, without having to change its own internal regulations. Akin to comity, this solution seems the most likely in areas where the consumer (and the voter) is seen as accepting reciprocity, such as in a "globally compliant" automobile, aircraft, airline service or online business or entertainment service.

b. *Harmonization.* Second, the two sides could change internal regulations by adopting a trade agreement that defines harmonized standards to supersede the existing differences. In such a "lowest common denominator" approach, consumer protections might not be the same, but they could be substantially equivalent, thereby promoting trade. How far the EU and the U.S. might go towards

simplification and harmonization of regulating Internet businesses depends on economics (the number of jobs likely to be created) balanced against public order concerns (consumer protection in each economy).

c. *Equivalence or New Standards.* Third, trade negotiators could liberalize trade by adopting "new" "global" standards for particular industries, or simply declare that their respective standards conform to a new, higher-order standard. In essence, governments would look to experts in non-profit organizations who have already developed, and continue to improve, "best practices" and international "standards" for quality, consumer protection, safety and minimal environmental impact.

4. *The Disciplines of Standards*. Adoption of a "standards-based" legal framework would change regulation from one of government-defined rules to process-driven standards that change. Businesses would have to follow processes and procedures for continuous improvement, not merely adhering slavishly to bureaucratic standards adopted in a political process. Moreover, to be politically acceptable, "standards" must be neutral, mature, administered by globally accepted legitimate standards-defining organizations[25] and not controlled by special interests. Finally, any standards-based method for mutual recognition and enforcement of "minimally acceptable" regulations depends on the maturity of the industry. Automobiles and aircraft have a track record over 100 years. Internet-based service industries are younger but maturing.

a. *Consumer Protection Through Quality Standards.* The International Organization for Standardization (ISO) adopted a general "quality" standard, ISO 9000 that demands fulfillment of eight principles for quality in the design and management of goods or services. The revised ISO 9000:2008 series of standards is based on eight quality management principles that senior management can apply for organizational improvement:

1. Customer focus
2. Leadership
3. Involvement of people
4. A "process" approach
5. System approach to management
6. Continual improvement
7. Factual approach to decision-making
8. Mutually beneficial supplier relationships.[26]

Adopting technocratic regulation in lieu of politically driven regulation would be a novel approach and would support harmonization only if the political goals are shared.

b. *Environmental Protection Through "Green" Standards.* When it announced the TTIP trade talks, the EU Commission acknowledged consumers' fears of losing existing EU consumer protection. The Commission announced that TTIP will not eliminate the right of either side to regulate "environmental, safety or health" issues or result in compromises on consumer protection or the environment.[27] In the environmental arena, adoption of international standards would be highly political and dependent on harmonizing potentially conflicting political objectives. Thus, in environmental protection, for example, ISO Standards in the ISO 14000 series specify requirements for establishing an environmental policy, determining environmental impacts of products or services, planning environmental objectives, implementation of programs to meet objectives, corrective action and management review.

D. "Harmonizing" Privacy Rules as an NTB

1. *The EU's "Adequate Protection" and "Opt-In" Consent Standards.* Based on the stated NTB and "harmonization" principles, in theory a TTIP agreement could result in harmonized privacy rules. This could occur if the EU merely declared that the U.S. legal regime of data protection is "adequate protection" for the specific rights of EU data subjects under that directive. Harmonization of privacy laws might be feasible by giving American consumers data privacy rights roughly similar to the rights of European residents, though enforcement procedures would have to be developed, and differences in enforcement (such as regulatory versus civil rights litigation) would have to be developed.

Currently, the core of the EU's privacy protections requires organizations collecting personally identifiable information (PII) to (i) identify the purposes (or to be very specific about the purposes), (ii) limit the collection of PII to collecting only those data needed for such purposes, (iii) limit the use and disclosure to what is needed for such purposes and (iv) delete the PII when no longer needed for such purposes. The EU enforces these rules.

The EU adopts an opt-in approach to personal consent, while the U.S. permits an opt-out approach (but does prohibit spam).[28]

The European Commission has recognized that some non-EU countries (even the U.S. in some cases) provide "adequate protection."[29] Canada's privacy law sets forth ten basic principles akin to the EU's eight principles.[30] California's legislature is considering a draft law that would broadly define personal data (to include geolocation, IP address information and many other categories) and give data subjects information about how their personal information is being used.[31]

2. *Possible New EU "Right to Be Forgotten."* Harmonization means that new policies on privacy would need to be adopted only after dialogue. For the controversial proposed European "right to be forgotten,"[32] the U.S. constitutional freedom of speech would need to protect the right to comment on someone's behavior.[33] One U.S. diplomat warned that adoption of "the right to be forgotten" would elicit a trade war.[34] Since then, the EU has recognized the vital importance of mutuality in adopting new "fundamental rights" like privacy.

3. *U.S.'s "Inadequate" Protection by "Opt-Out" or Vague "Opt In."* Current U.S. privacy rules allow voracious collection of PII with minimal disclosure of uses or aggregation resulting in pinpointing of individuals. U.S. Internet businesses can collect and track sensitive PII such as geolocation, which, when aggregated with other data collected by different services and linked by "cookie" identifiers, can be used commercially. Geolocational data might be disclosed actively (by the individual "signing in" to a geolocational website) or inactively (by GPS tracking). In either case, such data can be used to push an advertising message or discount coupon. Pending U.S. legislation would adopt EU-style disclosure and consent requirements, and would differentiate between "ordinary" PII and "sensitive" PII,[35] and would prohibit employers from obtaining from job applicants or employees "a user name, password, or any other means for accessing a private email account" for any social networking website, or taking employment disciplinary action in case of refusal.[36]

4. *Conflicting Regimes on Remedies for Privacy Breaches.* Any TTIP negotiation would require resolution of differences in legal enforcement against breaches of privacy rights. The U.S. approach depends on regulatory enforcement of "unfair trade practices" by the FTC (which can order injunctions and payment of fines) and on private rights of "victims" (and "whistleblowers" protecting victims) for damages under defamation and civil rights laws and, in California, a state data security breach law. The EU approach depends on regulatory enforcement by Data Protection Agencies (DPAs) which levy fines and issue injunctions. EU laws do not generally allow American-style "class actions."

5. *Possible Convergence*

a. *HIPAA Standards in the U.S.* For certain PII, public policy is identical on both sides of the Atlantic. Under the Data Protection Directive, governments must assure "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[37] That directive includes rules on the electronic exchange, privacy and security of health information. Similarly, under HIPAA and its regulations,[38] the federal government adopts standards for the electronic exchange, privacy and security of health information, including on accountability of organizations and designated agents, obtaining consent, limited uses, limited disclosures, limited retention, accuracy and updates, security safeguards, transparency about privacy practices, individual access and to health matters, limited disclosures and enforcement procedures.[39]

A HIPAA-compliant solution for all PII would be costly to business and would stunt the growth of many e-businesses. So businesses need to understand the costs and risks of an enforcement action under any harmonized privacy protocols under any TTIP FTA.

b. *Mutual Safe Harbor.* The agenda for "market access" invites speculation on possible outcomes based on comity, with reciprocity in respecting each other's regulations as reasonably sufficient to achieve each other's public policy within existing laws. In Internet and e-businesses, liberalization of market access rules might result in making the unilateral adoption by U.S. businesses of the EU data protection and privacy rules (adopted by diplomatic framework in 2000) into a bilateral, reciprocal "Safe Harbor" agreement. European ISPs and e-businesses might be able to adhere to U.S. privacy, data protection and data breach notification rules by some similar bilateral agreement.

Such a reciprocal "Safe Harbor" regime could have significant internal impact on U.S. state and local regulations of e-businesses. While the U.S. Constitution bars the federal government from regulating many "local" state businesses, any e-business uses means of interstate commerce and thus may be used as a jurisdictional basis for U.S. federal governmental harmonization of state and local rules on data protection, privacy and data breach notification on networks that access the Internet.[40]

c. *Prior Approval vs. Self-Governance.* Under French law, the sales of a company's client list requires prior notification to France's DPA.[41] Assuming the EU and the U.S. can agree on substantive equivalency of rights, they must also agree on the mutual recognition of administrative procedures, such as prior approval instead of self-governance and later audit.

6. *Benefits of Mutual Consultation and Decision-making.* TTIP raises a fundamental question as to how to best promote trade while protecting a sacred cow (NTB) of the "fundamental rights" of one's citizens. In an ideal world, all nations would adopt basic rights as their own legislation, and trade agreements only achieve a "lowest common denominator" because local legislative processes reflect different cultural and constitutional frameworks. Harmonization requires continuing consultations, and a trade agreement might not be politically acceptable for legislatures or their voters, since a trade agreement is fun-

damentally non-democratic except for the technicality of ratification.

V. Impact of Bilateral FTA on Multilateral Trade

The WTO Doha Round has stalled, if not failed. One purpose of bilateral trade agreements in this context is to set standards for WTO participants that could be adopted by other countries in a new WTO multilateral agreement.[42] TTIP might be used to deny access to the privileged bilateral relationship to "free-rider" countries that sign multilateral trade agreements but practice protectionism. Such protectionism might arise from the state's refusal to arbitrate its own international responsibility for illegal and unfair trade subsidies for export markets, preferring instead to unilaterally impose countervailing duties against another state that adjudicated such subsidies.[43] Or it might arise from the use of SOEs that receive government financial support and dump products in foreign markets at less than fair value[44] or that are "national champions" whose government refuses to permit management to sell their e-business subsidiaries to foreigners.[45] Or it might arise from restrictions on market access to the free-rider's economy. The multilateral liberalization of international trade in services, intellectual property and investment from the Uruguay Round has failed to address the free-rider problem.

The impact would be felt most by China, where protectionist laws and/or SOEs enable it to be free-riders on the MFN and non-discriminatory rules under current WTO agreements. The negotiations could counter "any trade-related issues or disputes that arise due to government censorship or disruption of the Internet among United States trade partners."

VI. Conclusions

Cost-Effective Regulations. TTIP faces the risk of failure if it cannot reduce levels of regulation, reduce compliance costs, and preserve "fundamental rights" and "civil rights." This tightrope will take a few years, but could yield significant benefits.

Consumer Protections. Depending on implementing legislation, consumers or businesses could face a reduction in their current legal rights under U.S. federal and state laws.[46] Any meaningful trade liberalization under a TTIP agreement could be difficult to achieve because policymakers might decide that key consumer protections should not be sacrificed for the sake of improving trade. Consumer groups may oppose any Internet-focused TTIP "harmonization" or reduction in consumer protections as a "back door" tool to defeat existing consumer protections.[47] This argument neglects that each side has strong, and strengthening, policies for consumer protection.

Data Processing Services After Privacy Harmonization. Is privacy harmonization necessary for increased trade and investment? Existing avenues already yield similar results, except that U.S. data centers cannot process EU PII without a Safe Harbor commitment. With a declaration that U.S. privacy rules are "adequate protection" for EU PII, American data centers, software developers and business process outsourcers could have a greater market and might even compete effectively with India and other low-wage countries based on economies of scale.

Employment. TTIP has been promoted as a tool for creating jobs in the EU and the U.S.. But the TTIP agenda omits tech visas. For e-businesses, the jobs that count require technical skills in software design, databases, analytics, business process management and cybersecurity. TTIP could promote employment by including special FTA-approved tech visas,[48] just as the North American Free Trade Agreement does, particularly to support more transatlantic tech services.

Taxation. TTIP's agenda does not include harmonization of sales or VAT taxes on digital goods. Pending U.S. federal legislation might, if enacted, open the debate to administrative simplification of cross-border collection of sales and VAT taxes from e-businesses.[49] Such simplification could be separate from the current OECD, U.S. and EU core principle, under income tax treaties, to impose local income tax only if a foreign enterprise has a "permanent establishment" in the taxing jurisdiction.

Cross-Border Startups. Many EU countries promote startups through R&D tax credits, tax holidays,[50] hiring credits and other incentives. Liberalized trade and investment under a TTIP agreement would heighten the value of comparative incentives in each direction.

Cross-Border Investments. A TTIP agreement alone might not increase investment, but it could increase M&A or joint ventures. The TTIP agenda omits specific attention to how to "simplify" governmental review of cross-border mergers and acquisitions.

Business Participation in the TTIP Process. As a a new process for innovation in regulatory and administrative procedures, TTIP raises expectations but could result in surprises for e-businesses. While businesses do not participate in trade negotiations, they have an interest in identifying the particular foreign NTBs that limit or bar their entry into foreign markets or impose unreasonable burdens. Businesses like automobiles, aviation and data processing need to identify such NTBs and press their governments for reduction of regulatory burdens.

Endnotes

1. E-businesses have adopted new business models across the full spectrum of research and development (e.g., pharmaceuticals),

design (e.g., architecture), marketing and sales, logistics, customer service and assemblages of funding (crowd-funding), professionals (e.g., "hoteling" and virtual professional services organizations).

New businesses have grown from e-discovery and electronic document review and data extraction, mobile gaming, gamification of marketing, health care informatics and distance learning. The "Internet of Things" collects massive data from multiple sensors, interprets data flows and enables high-velocity stock market trading, rapid police response and complex risk management for "smart" businesses. Virtual law firms and virtual global consulting companies relying on shared collective knowledge databases and legal process outsourcing support services are competing for talent and clients.

2. The Internet has spawned "ancillary services" (outsourcing) industries to enable outsourcing of virtually any information technology (ITO) or business process (BPO). E-businesses extend beyond back-office "voice-based" services (such as call centers and help desks) and "non-voice services" (such as the application and development of software, managed network security and data centers, database creation and administration for any kind of non-digital business). Outsourcing services have progressed from nearshore to offshore or some blend, from functional to multi-functional and multi-jurisdictional, and from domestic to global shared service centers for multinationals.

3. Pending U.S. legislation would require the Federal government to identify "any trade-related issues or disputes that arise due to government censorship or disruption of the Internet among United States trade partners." U.S. publicly traded companies would be required to disclose company "policies applicable to the company's internal operations that address human rights due diligence through a statement of policy that is consistent with applicable provisions of the Guidelines for Multinational Enterprises issued by the Organization for Economic Co-operation and Development." Proposed "Global Online Freedom Act of 2013," H.R. 491, §§ 105, 201 (113th Cong.) (introduced Feb. 4, 2013). *See* existing U.S. and foreign export control regulations as well.

4. This article does not address "trade regulation" under the rubric of national security, counterterrorism or state-sponsored espionage or counter-espionage.

5. World Trade Organization, *WTO Legal Texts, The Uruguay Round Agreements*, http://www.wto.org/english/docs_e/legal_e/legal_e.htm.

6. International Telecommunications Union, "Final Acts of the World Conference on International Telecommunications (WCIT-12)," available at http://www.itu.int/pub/S-CONF-WCIT-2012/en (Dec. 2012).

7. Violet Blue, ZD Net, "FCC to Congress: U.N.'s ITU Internet plans 'must be stopped,'" http://www.zdnet.com/fcc-to-congress-u-n-s-itu-internet-plans-must-be-stopped-7000010835/ (Feb. 5, 2013); Stephen Kaufman, "International Treaty Puts Free Internet in Jeopardy," http://iipdigital.usembassy.gov/st/english/article/2013/02/20130205142109.html#axzz2YI8mjXRG (Feb. 5, 2013).

8. Angela Diffley, "France will veto EU-U.S. trade talks if culture is included," http://www.english.rfi.fr/americas/20130613-france-will-veto-eu-us-trade-talks-if-culture-inclded (June 13, 2013); Jean-Pierre Frodon, "*Pourquoi l'Exception Culturelle est un combat légitime*," http://www.slate.fr/story/74443/excection-culturelle-legitime (June 26, 2013).

9. Office of the Press Secretary, U.S. White House, "Fact Sheet: Transatlantic Trade and Investment Partnership," http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-transatlantic-trade-and-investment-partnership-t-tip (June 17, 2013) ["White House TTIP Fact Sheet"].

10. The EU Directive on Distance Selling protects consumer across borders by mandating certain disclosures by online merchants and giving a 14-day period for the consumer to rescind "off-premises" and "distance" (telephone, fax or Internet only) transactions. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:en:NOT.

11. 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, *Official Journal L 281, 23/11/1995 P. 0031 – 0050*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML ["Data Protection Directive"].

12. U.S.-EU High Level Working Group, Final Report, *High Level Working Group on Jobs and Growth*, trade.ec.europa.eu/doclib/html/150519.htm> (Feb 11, 2013) ["HLWG Report"].

13. *See, e.g.*, Consumer Product Safety Act of 1972, Pub. L. 92-573, 88 Stat. 1207 (Oct. 27, 1972), *available at* http://www.cpsc.gov/en/Regulations-Laws--Standards/Statutes/.

14. *See, e.g.*, the minimum federal standards for consumer product warranties under the Magnuson-Moss Consumer Product Warranty Act, 15 U.S.C §§ 2301 *et seq.*, http://uscode.house.gov/download/pls/15C50.txt; implied warranties under Article 2 of the Uniform Commercial Code; and the consumer's rights to rescind unconscionable transactions, if the court determines that "the contract or any clause of the contract to have been unconscionable at the time it was made," under Section 2-302 of the Uniform Commercial Code. See., e.g., NY UCC § 2-302, http://public.leginfo.state.ny.us.

15. White House TTIP Fact Sheet; *see also* Office of the U.S Trade Representative, "Fact Sheet: United States to Negotiate Transatlantic Trade and Investment Partnership with the European Union," http://www.ustr.gov/about-us/press-office/fact-sheets/2013/february/U.S.-EU-TTIP (Feb. 13, 2013).

16. Eur. Comm'n, "FAQ on the EU-U.S. Transatlantic Trade and Investment Partnership ('TTIP')," p. 6, http://trade.ec.europa.eu/doclib/docs/2013/may/tradoc_151351.pdf (June 17, 2013).

17. *Koontz. v. St. John's River Water Mgt. District*, 570 U.S. ___, slip op. at p. 7 (June 25, 2013), http://www.supremecourt.gov/opinions/12pdf/11-1447_4e46.pdf (invalidating a local water district's "extortionate" demands imposed as a condition for granting a permit for construction of improvements on land owned by a builder).

18. U.S. Department of State, "*Bilateral Investment Treaties in Force*," http://www.state.gov/e/eb/ifd/bit/117402.htm. This list includes the Czech Republic, Croatia and Poland, all members of the EU.

19. See generally Nathalie Berlosconi-Osteralder, "*Analysis of the European Commission's Draft Text on Investor-State Dispute Settlement for EU Agreements*," Investment Treaty News, http://www.iisd.org/itn/2012/07/19/analysis-of-the-european-commissions-draft-text-on-investor-state-dispute-settlement-for-eu-agreements/ (June 19, 2012).

20. Egil Fujikawa Nes, "*The Cost of Importing Services into Brazil*," http://thebrazilbusiness.com/article/cost-of-importing-services-to-brazil (Apr. 13, 2011). This tax on imported services is structured like a tariff because it is exonerated and refunded when the imported services are used as a component of another service or product resold in Brazil. *Id.*

21. Eur. Comm'n, "Transatlantic Trade and Investment Partnership (TTIP)," http://ec.europa.eu/trade/policy/in-focus/ttip/ (June 23, 2013).

22. See WTO Agreement on Technical Barriers to Trade, available at World Trade Organization, WTO Legal Texts, The Uruguay Round Agreements, http://www.wto.org/english/docs_e/legal_e/legal_e.htm.

23. World Trade Organization, "*WTO Legal Texts," listing all of Uruguay Round agreements including Agreement on "Technical Barriers to Trade,*" http://www.wto.org/english/docs_e/legal_e/legal_e.htm.

24. HLWG Report, at p. 6.

25. The International Organization for Standardization is a network of national standards organizations that has adopted over 19,500 standards in business and commerce since its inception in 1947. http://www.iso.org/iso/home/about.htm. For automobiles, "SAE International is a global body of scientists, engineers, and practitioners that advances self-propelled vehicle and system knowledge in a neutral forum for the benefit of society." http://www.sae.org/about/board/vision.htm.

26. American Society for Quality, ISO 9000 and Other Quality Standards, http://asq.org/learn-about-quality/iso-9000/overview/overview.html.

27. "The negotiations will not be about lowering standards: they are about getting rid of tariffs and useless red-tape while keeping high standards in place. There will be no compromise whatsoever on safety, consumer protection or the environment. But there will be a willingness to look pragmatically on whether we can do things better and in a more coordinated fashion. Obviously, each side will keep the right to regulate environmental, safety and health issues at the level each side considers appropriate." Eur. Comm'n, "FAQ on the EU-U.S. Transatlantic Trade and Investment Partnership ('TTIP')," p. 6, http://trade.ec.europa.eu/doclib/docs/2013/may/tradoc_151351.pdf (June 17, 2013).

28. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2013, or "CAN-SPAM Act of 2013," Pub. L 108-187, 117 Stat. 2699, *available at* http://www.ftc.gov/os/caselist/0723041/canspam.pdf.

29. *Id.* Art. 28. Article 25(2) defines what is "adequate protection" for a transfer of EU-sourced personal information to a third country like the U.S.: "2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country." The process for determining "adequate protection" is described at Eur. Comm'n, "Commission Decisions on the Adequacy of Protection of Transfers of Personal Data to Another Country," *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm. Qualifying countries are Andorra, Argentina, Australia, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, as to Air Passenger Name Records for airlines reporting to the Department of Homeland Security, and as to voluntary adoption by American companies of EU data privacy rules, the "Safe Harbor" administered by the U.S. Department of Commerce.

30. Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"); Industry Canada, "Electronic Commerce in Canada," http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00466.html.

31. See California's draft "Right to Know Act of 2013" (Assembly Bill 1291), amending Cal. Civil Code § 1798.83, *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1291.

32. See proposal by Viviane Reding, Vice President, Eur. Comm'n, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age," 5 (Jan. 22, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF.

33. For analysis, see Jeffrey Rosen, "The Right to Be Forgotten Online," 64 Stanford U. L. Rev. Online 88 (Feb. 13, 2012), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten. This debate has been put on the back burner for now.

34. OUT-LAW.com, "U.S. diplomat: If EU allows 'right to be forgotten'…it might spark TRADE WAR, 'Things could really explode' warns U.S. Foreign Service man," (Feb. 5, 2013), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

35. The "Do Not Track Me Online Act of 2011," 112th Cong., H.R. 504 (2011), was never enacted. It would have required the Federal Trade Commission to impose a privacy rule requiring the user's consent to the harvesting, use or disclosure of a PII, on the online activity of the individual, including "(i) the web sites and content from such web sites accessed; (ii) the date and hour of online access; (iii) the computer and geolocation from which online information was accessed; and (iv) the means by which online information was accessed, such as a device, browser, or application," as well as any "unique or substantially unique identifier, such as a customer number or Internet protocol address," name, postal address or other location or email address or the user's "screen" name. *Id.*, § 2(3). "Sensitive" PII would include "precise geolocation information and any information about the individual's activities and relationships associated with such geolocation." A new proposal is pending: "Do Not Track Online Act of 2013," S. 418, 113th Cong., 1st Sess. (Feb. 2, 2013), *available at* http://thomas.loc.gov/cgi-bin/query/z?c113:S.418.

36. See pending "Social Networking Online Protection Act," H.R. 537, 113th Cong., 1st Sess. (Feb. 6, 2013), *available at* http://thomas.loc.gov/cgi-bin/query/z?c113:H.R.537.

37. Data Protection Directive, *supra*, Preamble #68 and Art. 1.

38. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, 100 Stat. 2548 (1996) and 45 CFR Pts. 160 (privacy rule), 162 (data security rule) and 164 (breach notification rule), *available at* http://www.law.cornell.edu/cfr/text/45/160 *et seq*. For U.S. Code citations, see U.S. Govt. Printing Office summary at http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html.

39. See Dept. of Health and Human Services, "Summary of the HIPAA Privacy Rule," *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/.

40. The Racketeer-Influenced and Corrupt Organizations Act, 42 U.S.C §§ 1961 *et seq*., adopts "regulation of interstate commerce" as the federal jurisdictional basis for federalizing offenses that would otherwise not be federal offenses.

41. Metro News, «Virgin : «Pouvoir sortir d'un fichier clients est un droit absolu,» quoting French attorney Gérard Haas, *available at* http://www.metronews.fr/high-tech/virgin-pouvoir-sortir-d-un-fichier-clients-est-un-droit-absolu/mmgc!STiH8CObEcoLo/; *X v. Société Bout-Chard*, Arrêt n° 685 du 25 juin 2013 (12-17.037), *available at* http://www.courdecassation.fr/jurisprudence_2/chambre_commerciale_financiere_economique_574/685_25_26909.html (French Cour de Cassation, Chambre commerciale, financière et économique, Docket ECLI:FR:CCASS:2013:CO00685, June 25, 2013).

42. "Furthermore, if the EU and U.S. are able to harmonise many of their regulations and standards, this could act as a basis for creating global rules with all the cost savings and economic benefits that would bring." *Id.*, at p. 9.

43. After the U.S. imposed sanctions on Chinese state-subsidized solar panels in 2011, China did not retaliate. After the EU imposed similar sanctions in 2012, China imposed countervailing duties on wines from France and Spain before any international dispute resolution.

44. In the Cold War era, Communist Poland was found to have "dumped" golf carts at less than fair value, and the U.S. used Spain as a reference "free market" economy for measuring the amount of dumping.

45. In 2013, France refused to permit the sale to Google of Dailymotion, a French subsidiary of a French government-controlled telecom company. This "national pride" exception to free investment rules highlights the hurdles that TTIP negotiators face in providing market access and open investment opportunities.

46. American Presidents have long used international agreements to promote and regulate trade, and American rules can be protected (and changed) when implementing multilateral conventions. In the Berne Convention Implementation Act of 1998, H.R.4262 (100th Cong., 2nd Sess.), 102 Stat. 2853-2861, P.L. 100-568, http://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg2853.pdf (1988), the U.S. did not enact any "moral rights"(which the Berne Convention protects to prevent any post-assignment use (or alteration) of a work of authorship that impugns the author's moral character or reputation during the author's lifetime The U.S. changed its own copyright law by removing the requirement of registration as a prerequisite to instituting an action for copyright infringement, but the remedy for such an action would be limited to injunctive relief (unless the foreign author registered with the U.S. Copyright Office). The enabling law also eliminated the previous requirement that the author put the copyright notice on all copies. See generally, World Intellectual Property Organization (WIPO), "Berne Convention on the Protection of Literary and Artistic Works" of Sept. 9, 1886, as amended; http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html; Reference for Business, "Berne Convention," http://www.referenceforbusiness.com/encyclopedia/Assem-Braz/Berne-Convention.html.

47. Doug Palmer, "Consumer groups worry U.S.-EU trade pact will weaken health, privacy regulations," http://www.reuters.com/article/2013/05/29/us-usa-eu-trade-idU.S.BRE94S0XP20130529 (May 29, 2013).

48. Current L-1 visas permit "intracompany transferees" of foreign managerial or specialized knowledge workers, but they must have a one-year employment record abroad. An FTA could open the doors without this requirement. Pending U.S. immigration reform bills would increase the quota of H1-B visas, but a TTIP FTA could be exempt from such visa quotas.

49. "Marketplace Fairness Act of 2013," S. 743 (113rd Cong., 1st Sess.), approved by Senate on June 14, 2013, referred to House, *available at* http://thomas.loc.gov/cgi-bin/query/D?c113:2:./temp/~c1134gVtAv::. If enacted, it would establish a federal regime of mandatory collection by Internet-based businesses of U.S. sales taxes imposed currently by over 9,600 domestic taxing jurisdictions. Online retailers grossing more than $1 million per year would be forced to compute and collect taxes in thousands of localities, identify exemptions and tax holidays, submit monthly or quarterly tax returns to the 46 states that have sales taxes, and collect taxes from 565 federally recognized Indian tribes. New state-level "one-stop" collections services and software would soften the burdens.

50. For young innovative companies under eight years old, for example, France grants (i) 100% exoneration of taxes on profits for the first three fiscal years and a 50% abatement for the next two fiscal years, but this ends in 2013; (ii) 100% exemption from annual minimum tax (imposition forfaitaire annuelle) for the entire period of special status; (iii) upon local governmental approval, exemption for seven years on real property taxes (contribution foncière d'entreprises) and (iv) under certain conditions, 100% exemption from capital gains tax upon the sale of shares held by individuals. French Direction Générale des Finances Publiques, FAQ's on «Jeunes Entreprises Innovantes,» *available at* http://www.impots.gouv.fr/portal/dgi/public/popup;jsessionid=PMELAKP3XRPNZQFIEIPSFFA?espId=2&typePage=cpr02&docOid=documentstandard_1656; Direction d'Informations Légales et Administratives, «Jeune Entreprise Innovante ou Universitaire,» http://vosdroits.service-public.fr/professionnels-entreprises/F31188.xhtml.

William B. Bierce advises entrepreneurs, investors and multinational enterprises in corporate, commercial, technology, privacy and cyber law, licensing, strategic alliances, sourcing and cross-border growth. He practices law with Bierce & Kenerson, P.C., in New York City.

Six Things Every In-House Counsel Needs to Know About Employee Privacy Rights

By Joel J. Greenwald

Employers need to monitor their businesses and their workplaces to protect against employee data theft, employee time abuse, and other actions. Employers also have certain obligations to respect their employees' workplace privacy rights. Here are six things every in-house counsel needs to know in order to help their clients do both.

1. Company computer and phone systems are (almost) never private for employees

Under federal and state law, employers can monitor employee activity on company computers and phone systems, but should destroy any expectations of privacy by having clear monitoring policies with signed employee acknowledgements. Even so, employers do not have carte blanche to monitor employees' personal e-mail and phone calls made through company equipment. Once an employer determines that a call or email is personal, then monitoring must generally stop.

2. Employers can look to video surveillance as a method of monitoring employees

Generally, employers can monitor the workplace with video surveillance in public places without employee consent or notice (unless your workplace is unionized, in which case certain bargaining issues arise). New York labor law, however, prevents employers from using video surveillance to monitor employees in restrooms, locker rooms, changing rooms, fitting rooms, or other "room[s] designated by an employer for employees to change their clothes" unless the employer has a court order.[1] Sound recording is prohibited, however, and governed by complex wiretap laws.

3. Employees' public social media activity is not off limits to employers

Information that is freely accessible through the Internet is public information so there is generally no privacy limitation to employers' monitoring of their employees' publicly available activity (e.g., blogging, posting, commenting, "Like"-ing, "Tweet"-ing, etc.). However, employment discrimination laws may come into play and govern how information obtained online can be used (and should be stored).

Additionally, employers should not take actions to circumvent employee password protections on their private social media accounts. New York is poised to join other states in prohibiting employers from asking employees and job applicants for password information.[2]

4. It's a-OK to track employees using GPS

Knowing your employees' locations can be important to track productivity and employee efficiency. To that end, employers may legally use GPS systems to track employees who carry company phones or drive company-provided vehicles—even without notice (although, again, union bargaining rights may trump). Using GPS offers real-time tracking of assets and employees, but tracking during non-work hours is potentially prohibited.

5. Employee images, likenesses, and voice recordings are protected by statute

Sections 50 and 51 of the New York Civil Rights Law protect a person's "name," "portrait," "picture," and—in the case of section 51 only—"voice" from being used for trade or advertising purposes without the person's "written consent."[3] Employers should thus obtain their employees written permission in writing before, for example, shooting pictures or video for a company website or marketing brochure. Under section 50, any "person, firm or corporation" who does otherwise is guilty of a misdemeanor, so prudence is warranted. Section 51 imposes civil liability and authorizes any victim to seek an injunction. Providing employees with a consent form to be signed on hire is a good way to avoid running afoul of these rules.

6. Employee Social Security numbers require enhanced privacy protections

Social Security numbers (SSNs) have enhanced privacy protections under New York law and may only be obtained by employers for taxation and benefits purposes.[4] But, once obtained, employers must handle SSNs with care, including "encrypt[ion]" if necessary.[5] Accordingly, employers generally may not print SSNs on employee IDs and must take other precautions to protect this information.[6] These rules apply not only to full nine-digit SSNs, but also to "any number derived from such number," including the last four digits.[7] Employers enjoy a safe harbor for unintentional violations of these rules resulting from a "bona fide error made notwithstanding the maintenance of procedures reasonably adopted to avoid such error."[8] But access to such information should be restricted to those with a business need to know.[9]

By being mindful of the New York and federal employee privacy protections, employers can navigate these requirements to balance their interests in employee productivity and honesty, against their privacy obligations to their employees.

DISCLAIMER: The foregoing is a summary of the laws discussed above for the purpose of providing a general overview of these laws. These materials are not meant, nor should they be construed, to provide information that is specific to any law(s). The above is not legal advice and you should consult with counsel concerning the applicability of any law to your particular situation.

Endnotes

1. N.Y. Labor Law § 203-c.
2. Senate Bill S02434B, which was introduced on January 17, 2013, proposes to add New York Labor Law s 201-g expressly prohibiting employers from requiring employees or applicants for employment to "disclose any user name, password or other means for accessing a personal account or service through an electronic communications device."
3. N.Y. Civ. Rights Law ss 50-51.
4. N.Y. Gen. Bus. Law s 399-ddd(g), 2012 Sess. Law News N.Y. Ch. 372, s 1.
5. N.Y. Gen. Bus. Law s 399-ddd(1)(a), 2012 Sess. Law News N.Y. Ch. 371, s 1.
6. S 399-ddd(2), 2012 Sess. Law News N.Y. Ch. 371, s 1.
7. S 399-ddd(1)(a), 2012 Sess. Law News N.Y. Ch. 371, s 1; s 399-ddd(1), 2012 Sess. Law News N.Y. Ch. 372, s 1.
8. S 399-ddd(7), 2012 Sess. Law News N.Y. Ch. 371, s 1; s 399-ddd(5), 2012 Sess. Law News N.Y. Ch. 372, s 1.
9. N.Y. Labor Law s 203-d(1)(c).

Joel J. Greenwald, Esq., is the managing partner of Greenwald Doherty, LLP, an employment and labor law firm, representing exclusively management, and can be reached at (212) 644-1310 or jg@greenwaldllp.com.

Web Site Checklist: Minding Your Company's Virtual Storefronts

By Jessica R. Friedman and Paul S. Ellis

Any Web site that your company operates has the potential to be both a blessing and a curse. An attractive Web site can be a significant boost to your company's bottom line. But the same features that make a company's Web sites attractive can also spark a variety of legal claims if they have not been properly vetted. Many of those claims are not unique to the online environment. Defamation or false advertising, for example, can occur in any medium, and counsel should be reviewing all content in any format that might pose a risk of either claim. But Web sites present some unique problems.

First, because it is so easy to post new material online, and because there is such pressure to keep content fresh, people tend to post content without subjecting it to the same legal review to which they would subject print content. Second, user-generated content occurs only on Web sites (and social media pages, which carry some of the same risks). Finally, only Web sites have terms of use and privacy policies, and although the average consumer will probably never read either of them on any Web site, those legal provisions are the first place a sharp plaintiff's lawyer will look when analyzing a potential claim against your company arising from a user's interaction with one of your company's sites.

Many in-house attorneys would be hard-pressed to find the time to review their companies' Web sites on any type of periodic basis, let alone to conduct the daily or even weekly review that would really be required to eliminate all the possible risks. But based on our experience, if you can find the time, checking for the following potential problems will significantly reduce your company's exposure.

1. Trademark Infringement

Even if your company has a policy that requires that the legal department clear each and every trademark before it is used, unless everyone in the company is aware of and adheres to that policy, even a cursory review is likely to reveal trademarks and service marks for your company's products and services that you have never seen before. If this happens, you have to decide whether the mark needs to be removed (is it very clearly likely to be confused with another company's mark? How important is that mark to that other company?), and if so, how fast (immediately, or can it wait until you clear the rights?) and for how long (temporarily while you clear the rights, or permanently?). Not every company, and certainly not every start-up, can afford to conduct complete clearance on each and every mark that some marketing staffer thinks the company should use. Even if you bring a mark that has not been cleared to the attention of the head of the relevant business division, he or she may decide to take a risk and just continue to use the mark. But by at least keeping an eye out for those potentially problematic marks on the Web sites, you will be significantly reducing the company's risk.

Also, every company likes to showcase its existing client list, especially if that list includes heavy hitters or "household names." But not all companies like their names to be used that way. Many companies actually have provisions in their vendor agreements that expressly prohibit clients' use of their names and logos as endorsements without their consent. You should check all of your companies' sites periodically for third-party names and logos. When you find one, you need to check that your company is authorized to display it, or, at least, that your company is not prohibited from displaying it.

2. Copyright Infringement

Many people, and especially the younger people who run many companies' online operations, think that if content can be reproduced, it's perfectly legal to reproduce and display it on another site, either because it's somehow not subject to copyright, or because doing so is "fair use." Both of these assumptions are unfounded.

Under U.S. copyright law, any content that meets a very minimal originality requirement is automatically subject to copyright protection, and only the owner of the copyright in that content has the right to reproduce that content, modify it, create adaptations of it, distribute copies of it (which includes transmit it electronically), display it publicly, and perform it publicly. If anyone other than the owner does any of those things, it is copyright infringement. Since your company's Web sites are accessible all over the world, if your editorial and marketing people are cutting and pasting in articles, photos or other content from other sites, the company is vulnerable to a claim of copyright infringement both in the U.S. and abroad.

Moreover, despite popular misunderstanding, "fair use" is not a magic wand that automatically converts infringing use into non-infringing use, and there are no "bright line" standards that apply to all situations. Fair use is a specific defense to a charge of copyright infringement, pursuant to which a court may excuse certain copying that otherwise would be infringement, after it considers four factors set out in the Copyright Act, together with

whatever else the court considers relevant, as applied to the specific facts at hand.

Even if your company's sites comply with all the requirements of U.S. law, it may still be infringing copyright laws or related laws of other jurisdictions, which could result in the company's being sued in another country. In 2007, a French court held that Viewfinder, the owner of a Web site based in the United States that posts photographs from fashion shows, was liable for copyright infringement under French law for displaying photos from two French fashion houses on its Web site, because while U.S. copyright law does not recognize a copyright in fashion designs, French law does.[1] Viewfinder defaulted, and the French court not only found Viewfinder liable, but awarded the plaintiffs one million francs in compensatory damages in a judgment that the plaintiffs then sought to enforce in court in New York. (That is not the end of the story, but suffice it to say that Viewfinder ended up having to spend a good deal on legal fees just to try to avoid enforcement of that judgment.)

The takeaway here is that you need to check for third-party articles, photos, graphics, and any other content on the company's sites. If you are told that particular content is licensed, you should review the license to make sure it covers Internet usage and has not expired.

Learning that a particular image has been licensed from a stock photo house should not end your inquiry. If your company uses a stock image on a Web site under a license that does not cover Internet use, or if it had a license for Internet use that has expired, sooner or later you can expect a letter from the stock house that demands that the company pay not only a license fee but a penalty fee that your company "agreed" to pay when the license was signed, or else face a copyright infringement suit. Often, these kinds of demands can be settled for less than $5,000, but if your company is small, is a start-up, or is just not doing well in this economy, even that amount can be more than you want to spend. The best way to avoid this is to tell your marketing department (or whoever is responsible for what appears on the Web sites) exactly which versions of the major stock licenses are acceptable.

If you spot any material that turns out not to be licensed at all, try to find out where it came from, or at least try to make sure that it is not the result of "scraping" other sites, which is especially common on real-estate industry sites and other listing sites.

3. Right of Publicity Violations

Displaying a person's name or photo, or using a recording of someone's voice, to advertise your company's products or services without that person's permission may violate that person's so-called "right of publicity." Not every state recognizes the right of publicity, and of the states that do, some have specific statutes and some only enforce it through judicial decisions, and the penalties vary from state to state. But as a general rule, even if Madonna is using your company's products, the company may not say so on its site or social media pages without Madonna's permission. So check for anything that looks like a celebrity endorsement—even a "candid" photo of a celebrity using your product. The fact that a celebrity was actually wearing your company's sunglasses does not mean that the celebrity consents to the use of her image to advertise those same sunglasses. In some states, one's right of publicity survives death, so that even using the name or photo of a deceased celebrity can result in a legal challenge. So if you happen to see a photo of Rosa Parks as part of a branding campaign designed to indicate that your company is "revolutionary," take it down immediately.

Just looking for celebrity names and photos is not enough, though, because one doesn't have to be famous to bring a right of publicity claim. In 2011, a group of users brought a class action against Facebook in which they alleged that Facebook was violating their rights of publicity by displaying the fact that they had "liked" certain products.[2] Facebook moved to dismiss the claim, but the court denied the motion because Facebook itself had admitted that an advertisement with that kind of testimonial attached to it was twice as valuable as an ad without one. (The case eventually settled.) So if any consumer-facing page includes a testimonial of a real person, even if that person is not famous, check whether the company has permission to use that person's name for that purpose.

4. Outdated Privacy Policies

Your consumer-facing privacy policies should be customized for the businesses that they represent. There is no one-size-fits-all. The online policy for each company Web site has to say what personal information *your* company collects on that site, what *your* company does with that information, and with whom *your* company shares that information. The language in which you articulate these policies should be clear and the graphic presentation should make them conspicuous.

But even if you are sure that each of your online privacy policies was drafted specifically for the business it reflects, you need to revisit them every couple of months to make sure that they are still accurate. If the company has actually changed its privacy practices in some material way—for example, if it has decided to sell its e-mail lists even though it initially did not do that—it may not be enough to simply rewrite the online policies. The company will need to notify users of the changes *separately from* its company's terms of use and privacy policy, and

preferably *before* it starts to sell the information, so that users who do not want their information handled according to the new policy have a chance to opt out. One effective way to notify users is to send out an e-mail to all your users that contains a link to the impending new policy. Needless to say, if you propose this, you are likely to get some serious pushback from the head of your marketing department. But one good antidote to that pushback would be to describe the burdensome FTC consent decree that Google was forced to enter into in 2011 after it violated its own privacy promises when it rolled out its "Google Buzz" service.[3]

Although many privacy policies don't have it, your policy should include a provision that is required by California law that says that if a California resident asks to be told with whom your company is sharing his or her personal information, you will provide that information within thirty days.

Finally, even if the facts stated in your consumer-facing privacy policies have not changed, the laws that govern what those policies have to say may have changed. It is beyond the scope of this article to talk about worldwide privacy law developments, but you should either have outside privacy counsel or a few good sources you can turn to for the latest developments.

5. Out-of-Date and/or Unenforceable Terms of Use

Like consumer-facing privacy policies, your terms of use need to be written specifically for your company. But even if your company was smart enough to start out with terms of use that were drafted specifically to fit its operations, if the company has changed the way that it does business, those terms of use may no longer be accurate. Maybe the company has changed its refund policy or the way its auctions work or its rules concerning the posting of user-generated content.

Equally important, if up to now your company has not been requiring users to agree to its terms of use, consider changing that policy by making them actually click on an "I agree" icon, either when they enter the site or at some crucial point, such as when they buy an item or click on an article (even if it's free). Just displaying a statement somewhere on the site that by browsing the site, a user is bound to the site's terms of use—which is sometimes inaccurately called a "browsewrap" agreement—has been held to be ineffective in many cases. If your company has been lucky enough not to experience any serious user disputes, the difference between a browsewrap agreement and a clickthrough agreement may not be immediately obvious. For example, if your user agreement says that the company will only give refunds within the first 30 days after a purchase, and someone seeks a refund six months later, not being able to enforce the 30-day limitation may not be a big deal (and unless the product was very expensive, the chances of anyone's actually initiating legal action are very low to start with). But if your company is unable to enforce a disclaimer of warranty, or a limitation on the company's liability for an expensive defective product to the price that the user paid for it, or a requirement that any claims against the company be subject to arbitration in Miami, the costs may be very high, especially if you are trying to fend off multiple lawsuits or a class-action suit by disgruntled users.

Zappos learned this the hard way in 2012 when it sought to enforce a clause in its terms of use that required users to submit all disputes to arbitration in Las Vegas.[4] Although a link to the terms of use appeared on every page of the Zappos site, the court found that those links were "inconspicuous, buried in the middle to bottom of every Zappos.com webpage among many other links, and the website never direct[ed] a user to the Terms of Use." Because the plaintiffs had never assented to the terms, no contract existed, so they could not be compelled to arbitrate. This past May, a court held that Yahoo! could not enforce a requirement that any litigation be brought in California.[5] On the other hand, in a 2011 case, the court held that Zynga's terms of use were enforceable even though users were not actually required to click "I agree" before accessing the application at issue, because "the terms were presented right underneath the button which allowed [the plaintiff] to access the application."[6] It's okay if your terms of use are in a "scrollbox," which a user would have to scroll through to read, as long as assent to them is mandatory.[7]

Another reason that the court held that Zappos could not enforce its terms of use is that those terms provided that Zappos had the right to change them at any time. Many terms of use include such unilateral amendment provisions, but well before the Zappos decision, courts had held that such a provision converts any agreement that otherwise might be formed into an "illusory" contract, which is not enforceable. If your company's terms of use include such provisions, consider removing them.

Last but not least, make sure that the information about your DMCA agent—your agent for receiving claims of online copyright infringement under the Digital Millennium Copyright Act—is up to date. If you never appointed an agent in the first place, you should do so at http://www.copyright.gov/onlinesp/agent.pdf, or else the company will not be eligible for the safe-harbor protections of Section 512 of the DMCA.

6. "Creation and Development" of Offensive User-Generated Content

If your company's sites allow the posting of user-generated content, you are probably aware of Section 230 of the Communications Decency Act.[8] Section 230

immunizes an "interactive service provider," which includes a Web site operator, from most federal and state liability[9] arising out of user-generated content (and other third-party content) as long as the Web site operator is not "responsible in whole or in part for the creation or development of the offending content."

Unfortunately, despite one court's statement that "[i]f you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune,"[10] Section 230 is not self-enforcing. There seems to be no shortage of creative plaintiffs' lawyers—and even plaintiffs who themselves are lawyers—who will allege that just by making it technologically possible to post content, a Web site operator is responsible for the creation of that content.[11] Plaintiffs also continue to bring cases that allege that newspapers are responsible for reader comments on account of their having moderated those comments to make sure that they were not abusive, obscene, profane or otherwise in violation of the newspaper site's own terms of use, even though it is well-established that this is not the case.[12] And despite the seemingly clear protection that Section 230 literally provides, once in a while, a court will refuse to dismiss a claim that clearly should be dismissed under Section 230.[13] Moreover, ever since the Ninth Circuit held in *Fair Housing Council v. Roommates.com* that by requiring subscribers to include certain information in their profiles, Roommates.com in effect became the developer "at least in part" of that information,[14] many plaintiffs make sure to include allegations to the effect that the defendants have created or developed the allegedly offensive content "in part," which is sometimes enough for the court to permit discovery on the issue of how the offending content was created.[15]

Although there is no way to completely insulate your company against lawsuits over user-generated content, you still may be able to reduce your company's risk of liability by making sure that whoever runs your company's forums or message boards is not doing any more than "moderating" user comments and that the interactive features of your company's sites are not structured so as to somehow solicit content that is illegal or that reasonably can be anticipated to be harmful or offensive.

Endnotes

1. *Sarl Louis Feraud Int'l v. Viewfinder, Inc*. 489 F.3d 474 (2nd Cir. 2007).
2. *Fraley v. Facebook, Inc., et al.*, no. 111-CV-196193 (Cal. Super. Ct.).
3. The settlement (i) bars Google from misrepresenting the privacy or confidentiality of individuals' information or misrepresenting compliance with the U.S.-EU Safe Harbor or other privacy, security, or compliance programs, (ii) requires Google to obtain users' consent before sharing its information with third parties if it changes its products or services in a way that results in information sharing that is contrary to any privacy promises made when the user's information was collected, (iii) requires Google to establish and maintain a comprehensive privacy program, and (iv) requires that for the next 20 years, the company have audits conducted by independent third parties every two years to assess its privacy and data protection practices. See http://www.ftc.gov/opa/2011/03/google.shtm for a summary and http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf for the actual consent decree.
4. *Id*.
5. *Ajemian v. Yahoo!*, 12-P-178 (Mass. Ct. App. 2013).
6. *Swift v. Zynga*, 2011 WL 3419499 (N.D. Cal. 2011).
7. *Scherillo v. Dun & Bradstreet, Inc*., 2010 WL 537805 (E.D.N.Y. 2010).
8. 47 U.S.C. § 230.
9. Section 230 does not apply to liability arising out of the use (or misuse) of intellectual property, federal criminal prosecutions, or liability arising under the Electronic Communications Privacy Act or analogous state laws.
10. *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 2008 WL 879293 (9th Cir. 2008).
11. *See, e.g., Barnes v. Yahoo!*, 2005 WL 3005602 (D. Or. 2005), in which the plaintiff claimed that Yahoo! was responsible for profiles posted by her ex-boyfriend that included nude photos of her and her contact information, because Yahoo! provided the tools to create the offending profiles.
12. *See, e.g., Gains v. Romkey*, 2012 IL App (3d) 110594-U (Ill. App. Ct. 2012); *Delle v. Worcester Telegram & Gazette Corp*., 2011 WL 7090709 (Mass. Super. Ct. 2011).
13. *See, e.g., Jones v. Dirty World Entertainment Recordings, LLC*, 2012 WL 70426 (E.D. Ky. 2012).
14. *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 2008 WL 879293 (9th Cir. 2008). The inclusion of information such as user gender and sexual preference was held to violate the federal Fair Housing Act and California housing discrimination laws by making it possible for potential roommates to discriminate against people based on the contents of their profiles.
15. *Chang v. Wozo LLC*, 2012 WL 1067643 (D. Mass. 2012).

Jessica R. Friedman has practiced copyright, trademark, e-commerce and publishing law in New York City for over 20 years. Her clients include technology, publishing, and entertainment companies. In addition to conducting her own private practice (www.literarypropertylaw.com), she serves as counsel to the Paul Ellis Law Group.

Paul Ellis is the principal of the Paul Ellis Law Group LLC (www.pelglaw.com), a 6-lawyer firm that represents small and midsize companies in corporate, intellectual property and general operational matters. Paul is a founding board member of the New York Technology Council, a trade association dedicated to supporting and promoting the technology industry, and is a frequent speaker on legal issues for technology companies.

How (Not) to Make a Contract on YouTube

By Clara Flebus

It is often said that "it pays to advertise." But as social media becomes the lingua franca of business today, lawyers should educate their clients on how to avoid paying *because* they have advertised. In the brave new electronic world, statements posted on the Internet for the purpose of reaching a multitude of people across boundaries with only few clicks can create unintended binding contracts. The recent decision of *Augstein v. Leslie*[1] is instructive on this point.

In *Augstein*, the Southern District of New York addressed the question of whether an online offer of a reward for the return of a stolen laptop computer containing valuable intellectual property constituted a unilateral contract, which became binding upon plaintiff's finding and delivering the computer, or whether the offer was merely an innocuous advertisement, or invitation to negotiate. Another interesting aspect of the decision is a ruling on sanctions for defendant's negligent failure to preserve electronically stored evidence in anticipation of litigation.

The defendant, Ryan Leslie, is a singer-songwriter and musician whose laptop computer, external hard drive, passport, and other personal belongings were stolen from the back seat of a car during a concert tour appearance in Germany in October 2010. The laptop contained music and videos related to his records and performances. Immediately after the theft, Leslie posted a video on YouTube offering a $20,000 reward for the return of the laptop. Few days later, Leslie posted another YouTube video at the conclusion of which a written message appeared stating:

> In the interest of retrieving the invaluable intellectual property contained on his laptop & hard drive, Mr. Leslie has increased the reward offer from $20,000 to $1,000,000 U.S.D.[2]

Leslie publicized the increased reward also on Facebook and Twitter, including a post on Twitter which read, "I'm absolutely continuing my Euro tour plus raised the reward for my intellectual property to $1mm."[3] The reward was reported internationally on various newspapers and Internet postings. Finally, Leslie appeared on MTV, where he reiterated his $1,000,000 offer by saying, "I got a million-dollar reward for anybody that can return all my intellectual property to me."[4]

In November 2010, the plaintiff, Armin Augstein, found a bag in Germany containing Leslie's laptop, hard drive, and passport, and brought it to the local police, who returned it to Leslie in New York.[5] Knowing about the $1,000,000 reward, Augstein made a demand for payment, but Leslie refused to honor his promise. Subsequently, Augstein retained a law firm in New York and brought suit to enforce the reward. In response to Augstein's claim, Leslie stated that the intellectual property, which made the laptop valuable to him, was not present on the hard drive when Augstein returned it.[6] According to Leslie, he tried to access the information on the hard drive, but was unable to do so.[7] He then sent the hard drive to the manufacturer, which allegedly deleted any material on it prior to issuing a replacement.[8] For his part, Augstein claimed that Leslie caused the information on the hard drive to be erased in the United States, after receiving correspondence from Augstein asking for the reward.[9] Eventually, Augstein moved for summary judgment on the issue of the validity of the offer, reward, and acceptance by Augstein in returning the laptop, and for sanctions due to Leslie's alleged spoliation of evidence on the hard drive.

I. Was the YouTube Reward Video a Valid Offer?

The crux of Leslie's argument was that the video was merely an advertisement, and, as such, could not result in a binding contract through unilateral action of Augstein.

First, Leslie relied on *Leonard v. Pepsico*,[10] where a teenager attempted to redeem a Harrier Jet featured in a television commercial run in the Nineties by Pepsico, the producer and distributor of soft drinks, which invited customers to collect "Pepsi Points" found on its products and then redeem the points for "Pepsi Stuff" contained in a catalog.[11] The Pepsico commercial started with a teenager on his way to school wearing some Pepsi merchandise, such as a t-shirt, a leather jacket, and a pair of sunglasses, with subtitles listing the number of points necessary for each item, and concluded with the teen boy landing in a Harrier Jet by the side of the school building with a final subtitle: "Harrier Fighter 7,000,000 Pepsi Points."[12] After watching that commercial, an enterprising teenager obtained a Pepsi Points catalog. Despite noticing that the catalog did not list the military plane, the teenager set out to raise the money necessary to purchase the 7,000,000 points required to claim the jet; he then submitted an order form with a check to Pepsico, which, in turn, rejected the claim and returned the check, explaining that the jet could not be redeemed because it was not included in the catalog.[13]

In *Pepsico*, the court relied on the general rule that an advertisement does not constitute an offer, but an invitation to enter into negotiations, or a solicitation for offers.[14] As such, an advertisement requires a further manifestation of assent by the advertising party to become a binding contract, and an offeree's willingness to accept the offer by filling out an order form is not enough. The court went on to explain that, by contrast, public offers of a reward for performance of a specific act are a special type of unilateral offers that become binding upon performance, without requiring a reciprocal promise.[15]

The rationale of *Pepsico* was derived from the leading British case of *Carlill v. Carbolic Smoke Ball Co.*,[16] in which the purchaser and user of a mysterious "smoke ball" remedy against influenza was stricken with that illness. The purchaser was awarded a £100 reward pursuant to the company's advertisement that it would pay such a sum to any person who contracted influenza after having used the ball according to the instructions.[17] *Carbolic Smoke Ball* held that an advertisement may be construed as an offer for a reward where it seeks to induce performance, rather than calling for a reciprocal promise.[18]

Applying these principles to the statements made in the YouTube video, the court in *Augstein* laptop case distinguished *Pepsico* explaining that, unlike the Pepsi commercial, the video was intended to induce performance, i.e., the actual return of the stolen laptop, and not just a promise from someone to deliver, or help him find, his property.[19] Thus, returning the laptop constituted an acceptance of the reward offer resulting in an enforceable contract.

Next, Leslie contended that, in any event, the offer was not legitimate because it was conveyed through YouTube, a social media site generally used to broadcast advertisements and promotional videos, along with several other kinds of videos. The court found this argument unpersuasive and noted that several courts have held that an offer was legitimate even if made via television or the radio.[20] In this regard, the court specifically stated:

> The forum for conveying the offer is not determinative, but rather, the question is whether a reasonable person would have understood that Leslie made an offer of a reward.[21]

The reasonable person standard was also used in *Pepsico*, where the court stated that when evaluating the Pepsi commercial it "must not consider defendant's subjective intent in making the commercial, or plaintiff's subjective view of what the commercial offered, but what an objective, reasonable person would have understood the commercial to convey."[22] Thus, if an offer is "evidently in jest," or done without intent to create a legal relationship, there may not be a valid contract.[23] In *Pepsico*, the court concluded that the idea of flying to school in a Harrier Jet represented an "exaggerated adolescent fantasy," and could not be understood as a serious offer by any reasonable person.[24]

Conversely, in the laptop case the court implicitly held that the offer of a $1,000,000 reward by Leslie, a popular musician, could objectively be construed as a serious one considering the potential commercial value of the intellectual property allegedly stored on the hard drive, despite the fact that it was conveyed through social media and amplified over the Internet.

II. Were Sanctions Warranted for Failure to Preserve the Data?

The court stated that a party seeking imposition of sanctions for spoliation of evidence must show that: (1) the party with control over the evidence had an obligation to preserve it when it was destroyed; (2) the evidence was destroyed with a culpable state of mind; and (3) the evidence destroyed was relevant to the party's claim or defense.[25] An obligation to preserve evidence arises when "the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."[26] Here, the court readily found that Leslie was on notice that information on the hard drive may be relevant to future litigation because he was contacted by Augstein about the reward before sending the hard drive to the manufacturer.[27] He thus had an obligation to preserve that evidence, which, undoubtedly, was relevant to the reward claim.[28]

A more complex question was determining the level of Leslie's culpability, and, consequently, the severity of the sanctions. The court noted that:

> The law is not clear in [the Second Circuit] on what state of mind a party must have when destroying [the evidence]. In *Reilly v. Natwest Markets Group Inc.*, we noted that at times we have required a party to have intentionally destroyed evidence; at other times we have required action in bad faith; and at still other times we have allowed an adverse inference based on gross negligence. In light of this, we concluded a case by case approach was appropriate.[29]

The court went on to cite precedent from the Second Circuit holding that ordinary negligence, and not only gross negligence or bad faith, may constitute a culpable state of mind warranting an adverse inference as a sanction,

based on the rationale that each party should bear the risk of its own negligence.[30]

Here, several disputed facts emerged at deposition as to the extent of Leslie's efforts to retrieve and preserve the data from the hard drive. Leslie himself stated that he never talked with his team about hiring an outside vendor or computer company to attempt to recover the information, while one of his assistants stated that he consulted a technician who examined the hard drive and concluded it could not be repaired.[31] That assistant also stated that he contacted the manufacturer and requested data retrieval, but was later told the information could not be recovered.[32]

However, the manufacturer, subpoenaed by Augstein, produced an employee, and records, indicating that a request for data recovery was never made by Leslie or his team.[33] In light of this contradictory proof, the court concluded that Leslie was at least negligent in his handling of the hard drive.[34] It further held that Augstein was entitled to an adverse inference jury instruction, i.e., the jury can infer that the intellectual property was present on the hard drive when the plaintiff returned it to the police.[35]

Augstein v. Leslie was tried at the end of November 2012. At the conclusion of the trial, the jury rendered a verdict in favor of Augstein in the amount of $1,000,000 for the return of Leslie's laptop.[36] A lesson to be learned from this case is to be careful about what you say on the Internet. The old adage "buyer beware" (*caveat emptor*) might be expanded to include "beware of the buyer." If a client uses social media and makes an extravagant reward offer, he or she may be bound by it if a reasonable person would have deemed the offer to be a real one. In all events, clients should be advised not to worsen a problematic situation by negligently handling evidence relevant to the claim for a reward; a court may instruct the jury to infer that the prized property was actually delivered.

Endnotes

1. 2012 WL 4928914 (S.D.N.Y. Oct. 17, 2012).
2. *Id.* at *2. This video is available at: http://www.youtube.com/watch?v=F8Jf0huEyNU.
3. *Id.* at *2.
4. *Id.*
5. *See Augstein v. Leslie*, 2012 WL 77880 at *1 (S.D.N.Y. Jan. 10, 2012).
6. *See id.*
7. *See Augstein v. Leslie*, 2012 WL 4928914 at *1.
8. *See id.*
9. *See id.*
10. 88 F. Supp. 2d 116 (S.D.N.Y. 1999).
11. *See id.* at 118.
12. *Id.* at 118-119. The Pepsico commercial is available at: http://www.youtube.com/watch?v=ZdackF2H7Qc.
13. *See id.* at 119-120.
14. *See id.* at 122-123.
15. *See id.* at 125.
16. *See id.* (citing *Carlill v. Carbolic Smoke Ball Co.*, 1 Q.B. 256 [Court of Appeal 1892]).
17. *See id.* (citing *Carlill v. Carbolic Smoke Ball*, 1 Q.B. at 256-57).
18. *See id.* (citing *Carlill v. Carbolic Smoke Ball*, 1 Q.B. at 262).
19. *See Augstein v. Leslie*, 2012 WL 4928914 at *3.
20. *See id.* n.2 (citing *Newman v. Shiff*, 778 F.2d 460, 466 [8th Cir. 1985]; *James v. Turilli*, 473 S.W.2d 757, 760 [Mo. Ct. App. 1971]).
21. *Id.* at *3.
22. *Leonard v. Pepsico*, 88 F. Supp. 2d at 127.
23. *Id.*
24. *Id.* at 129.
25. *See Augstein v. Leslie*, 2012 WL 4928914 at *3.
26. *Id.*
27. *See id.*
28. *See id.*
29. *Id.* at *4 (internal citations omitted).
30. *See id.* (citing *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108 (2d Cir. 2002); *see also Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 220 [S.D.N.Y. 2003] ["Once the duty to preserve attaches, any destruction of documents is, at a minimum, negligent"]).
31. *See id.* at *5.
32. *See id.*
33. *See id.*
34. *See id.* at *6.
35. *See id.*
36. *See Augstein v. Leslie*, 2012 WL 7008147 (S.D.N.Y. Dec. 28, 2012).

Clara Flebus is an appellate court attorney in New York State Supreme Court. She has clerked in the Commercial Division of the court and holds an LL.M. degree in International Business Regulation, Litigation and Arbitration from NYU School of Law.

Being Prepared When the Cloud Rolls In

By Natalie Sulimani

With each new technological advance comes at least one new term, if not a whole new language. It seems as if once you get a handle on one term there is yet another one to learn—crowdfunding and crowdsourcing, to name a few. And then there is social media, which should not be confused with social networks, of course. All of this in the spirit of and service to technology and innovation. But none strike more fear in the heart of attorneys lately than the ubiquitous term, cloud computing. What is the cause of the shudder you may have just felt run through the legal profession? Maybe the discomfort comes from the natural desire in the field of law to control as much of our client's situation as possible, and cloud computing is an environment that we, as attorneys, cannot ultimately control. It is, by its very nature, in the hands of someone else. Hopefully, you have found a trusted IT vendor to manage your part of the Cloud.

But, while with technology, the players and the terminology may change, what does not and will never change is an attorney's ethical obligations. We have a duty to maintain confidences, a duty to remain conflict free in our representations and, of particular interest to me lately, a duty to preserve.

The lesson has been taught, and sorely learned, that files must be backed up. Hard drive failures are, unfortunately, a reality. So, you backup to an external hard drive, except the unwritten rule of the cyberverse is, hard drives always fail. **Always**. Recently, the onslaught of natural disasters, the latest being Hurricane Sandy on the East Coast, has taught some lawyers a very harsh lesson. Redundancy is important. Maintaining files in multiple locations is a must. How many files were lost due to flooding or a server going underwater? How many attorneys were unable to access their files because of these or other similar catastrophes? If it was even one, then it was too many. And worse yet, there is no reason for such things to happen.

Early in my solo career, I had a breakfast networking meeting with an attorney from a mid-size firm and the discussion turned to the topic of working from home. Now, technically, I do not have a virtual law firm, but I do consider myself mobile as an attorney. I think most of us do. Technology allows us to do so. Moreover, the amount of work necessitates that we work remotely. Clients expect you to be available on their schedule, and worse yet, clients or opposing counsel may live in a different time zone. Not everyone exists on Eastern Standard Time. So, I casually asked, how do you manage your work from home? The answer was, "I email my files to myself." I followed up with, "Okay, to your firm address?" The response that mentally gave me pause was, "No, personal email address." There seemed something wrong about this, but more on that later.

Opinions regarding maintaining confidentiality are numerous and frequent and as we move forward, technologically, the subject keeps returning like a bad penny. We all know that we need to maintain confidentiality, but the challenge as we progress may be understanding new technology so that we are able to use it to be more efficient while at the same time being confident that we are maintaining client confidentiality.

History and the Ethics Trail to Cloud Computing

If you have attended seminars on cloud computing then you may know that the first iteration of the Cloud was voicemail. Answering machines were replaced with voicemail, which meant that your messages were stored on a remote server that required you to use a code to retrieve them. Although this was a shift in where personal and official information was stored, I cannot remember anyone wondering whether this would be an issue, confidentiality or otherwise, and kept answering machines over voicemail and the convenience of listening to messages anywhere.

The next step in cloud computing came in the form of third party email providers like Gmail, Yahoo, MSN, Hotmail, AOL, etc. These services stored our communications on remote servers in any number of locations, but most importantly, all this information resided in the Cloud. Again, almost everyone is happy to access his or her email from anywhere without fretting over the fact that all our words and thoughts are floating out there in the Cloud.

So how do the courts view this use of the Cloud? The opinion rendered in 1998 in New York State was that a lawyer may use ***unencrypted*** email to transmit confidential information since it is considered as private as any other form of communication. Unencrypted means that from point to point, the email could be intercepted and read. The reasoning was that "there is a reasonable expectation that e-mail will be as private as other forms of telecommunication…." However, the attorney must assess whether there may be a chance that any confidential information could be intercepted. For example, if your client is divorcing his/her spouse, an email that both spouses share, or even an email to which the non-client spouse has

access, should not be the method of communication. The attorney must seek alternate methods of communicating.

Gmail did add an extra twist which other email service providers quickly copied. As a "service" to you, email service providers started to scan emails in order to provide you with relevant ad content. They would scan keywords in your email and provide relevant advertising. For instance, if you were discussing shoes in an email, the email service provider would tailor ads when you were in the email inbox and you would now be receiving advertisements for Zappos or any other shoe vendor. After all, nothing is better than a captured audience.

So, the question now becomes whether a lawyer can use an email service that scans emails to provide computer generated advertisements. The New York State Bar Association opined in Opinion 820 (2/8/08 (32-07)) that, yes, it was okay since the emails were scanned by machine and not by human eyes. If the emails were read by someone other than sender and recipient, the opinion would have certainly been different.

And now to the topic at hand, storing client files in the Cloud. Through services like DropBox, Box.com, Rackspace, Google Docs, etc., an attorney can add to his or her mobility and efficiency by storing client files online. Although I know there is a lot of debate surrounding this practice, I do not see how it is very different from storing client files offsite in a warehouse. In the cyberworld, electronic files are held by a third party in a secure remote server with a guarantee that they will be safe and only authorized persons will have access. In the brick and mortar world, paper files are held by a third party in a warehouse with the same guarantees. Both are equally secure and equally liable to be broken into by nefarious agents bent on getting to the diligently hidden confidential information. Again, the technology might change but the principles are the same. One should not be more or less afraid of one method of storage over the other.

A number of state bar associations have been grappling with the issue of cloud computing and the ethical issues it raises, including North Carolina, Massachusetts, Oregon, Florida, as well as our esteemed New York State Bar Association. However, surprisingly to date, only 14 of the 50 States have opined regarding use of cloud computing in the legal profession. One would think more would have joined the fray in giving its lawyers some guidance.

The American Bar Association amended its model rules last year perhaps as a beacon to other bar associations, but certainly as a guide for other states.

Model Rule 1.6 holds:

> A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Across the board, opinion is cautious about using cloud computing in the practice of law but there is nothing about it that could be called unethical. The ethical standard of confidentiality is *reasonable efforts to prevent disclosure*. The question, therefore, lies in what is considered reasonable efforts.

Rule 1.6(a) of the New York Rules of Professional Conduct states:

> A lawyer shall not knowingly reveal confidential information…[and goes on to say that] [a] lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose service is utilized by the lawyer from disclosing or using confidential information of a client….

It is safe to assume that Rule 1.6(c) imposes the obligation for lawyers to use reasonable care in choosing their cloud computing and/or IT vendors, but indeed those lawyers may take advantage of the Cloud and employ those who provide and manage those services in good conscience.

In fact, in September 2010, the New York State Bar Association issued Ethics Opinion 842 regarding the question of using an outside storage provider to store client information. The question that was asked of the New York State Bar Association was whether a lawyer can use an online storage provider to store confidential material without violating the duty of confidentiality.

So What Exactly Is the Cloud?

To understand what the issue is and why it may pose a problem, it is best to understand what it means to store in the Cloud. A Cloud, in its simplest terms, is a third party server. The server in which the information is stored is neither on the law firm's premises nor owned by the law firm. The law firm's IT person or department does not maintain where the database is stored in any way. It is in the hands of a third party offering a service.

So an internal storage is a closed circuit, meaning there is a direct line from your desktop to the firm's server. Absent hacking, the information is controlled internally. Once removed from this closed system and stored in the Cloud, your information may be more vulnerable because you have now created access points in which oth-

ers may gain access to that data. To illustrate, data will now flow out on the Internet and beyond your control to get to the remote server where it is housed. However, encrypt the data, and you have limited the exposure. As stated above, once encrypted it would take a nefarious and willful mind to be able to read what you are sending into the Cloud.

Why Should You Move Your Data to the Cloud?

There are many reasons why you would want to move to the Cloud and many reasons why it is prudent to move your storage to the Cloud. To begin with, properly using cloud computing in the storage of client information reduces the possibility of human error. Emailing yourself files, transferring to a thumb drive, storing client files in offsite warehouses, to name a few, are all steps that introduce and increase the chance for human error. Email to your personal email account runs the risk that your family would access your email at home, thumb drives get lost, people break into warehouses and natural disasters happen that can destroy files. Cloud computing, by contrast, puts your files in the hands of competent IT professionals who will secure your information and provide the necessary redundancy so that if a server goes down, your files will live on and be available when you need them from another server. Their major, if not sole, purpose (and the reason you pay them) is to safeguard your files and ensure that you will always have access to them when necessary, so they are highly motivated to do it well and properly.

In December 2010, the FTC issued a report regarding consumer privacy "in an era of rapid change." While attorneys may be subject to higher standards in keeping client confidences, I think this is a good guide in understanding the technology and best practices associated with it.

The FTC report recognized that businesses are moving to the Cloud because it improves efficiency and is cost effective. However, the overarching concern is privacy. The FTC recommended overall guidelines for technology and consumer data. In particular, there are four recommendations that businesses should follow:

1. Scope: Define what information is stored;
2. Privacy by Design: Companies should promote privacy in their organizations;
3. Simplified Choice: Simplify choice so that the customer is able to choose how information is collected and used in cases where it is not routine, such as order fulfillment;
4. Greater Transparency: Companies should be transparent in their data practices.

Using these guidelines, what are best practices for attorneys?

- Consider what client information you will store in the cloud.
- Privacy is easy to ensure, attorney-client privilege should be maintained.
- Determine what information you will share with your clients. For example, will you share their case files with them? You can pick and choose what you share with your clients in the Cloud for greater collaboration and reduction of emails going back and forth with attachments. They can upload their data in a secure environment and you can share information in a secure, password protected environment where you can ensure that only a specific client or clients have access.
- Choice and transparency go hand and hand. While it is the attorney's best judgment in deciding how to reasonably protect client information, you should make your client aware that you are using these services. Build it into your retainer. If, for any reason, your client objects, you will know and can deal with the reasons why right there at the beginning. It may just take a short conversation about the confidentiality, reliability and ease of the Cloud to assuage any fears or concerns.
- Finally, have a breach notification policy in place. This is not just for your corporate clients; any client whose information is in the Cloud should be notified of and subject to this policy.

Now that I have you on board with moving your files to the Cloud, consider that you need to exercise "reasonable care" in choosing a Cloud provider. Opinion 842 offers some guidance:

1. Ensure that the online storage has an enforceable obligation to preserve confidentiality and will notify you of a subpoena;
2. Investigate the online storage's security measures, policies, recoverability methods and other procedures;
3. Ensure that the online storage provider has available technology to guard against breaches;
4. Investigate storage provider's ability to wipe data and transfer data to the attorney should you decide to sever the relationship.

Read the Terms of Service and, when you can, negotiate with the Cloud vendor. Cloud vendors update their policies and may be willing to change their practices to the needs of their (and your) clients. If you have concerns and/or specific needs, contact them, and if they are unwilling to change their practices, go somewhere else. Frankly, there are too many online storage providers to not be discerning when it comes to client data.

While utilizing an online storage provider consider its encryption practices. Will your data be stored encrypted? Will you encrypt the data en route to the online storage and who has access while it is being stored? Also, if the online storage provides access on mobile devices, just as you would your computer, laptop, tablet and mobile phone, add security by password protecting the online storage's mobile app. After all, just as in the non-cyber world, a big threat to effective storage is human error. Therefore, it is of utmost importance that you know how to remotely wipe the data if your device is lost or stolen. One aspect of mobile storage to be aware of is that when you download client data to your mobile device, it may be downloaded to your SD card unencrypted. Whether you want this situation is something to consider, and take steps to avoid it if desired. This aspect is an example of the importance of understanding how the technology works, understanding where problems, such as interception, may occur, and ultimately how to take steps to avoid them. Education here is key.

In short, the advantages of cloud computing as outlined in this article make it a perfect complement to an effective and successful law practice. There is little difference in the potential ethical issues or any other such problems that exist in the Cloud and in the brick and mortar world of physical offsite storage of clients' files. Rather than running away from this new technology, it would be better to embrace it by learning more and making wise decisions that will minimize potential pitfalls down the road, while at the same time increasing the ease and usefulness of client communication and interaction.

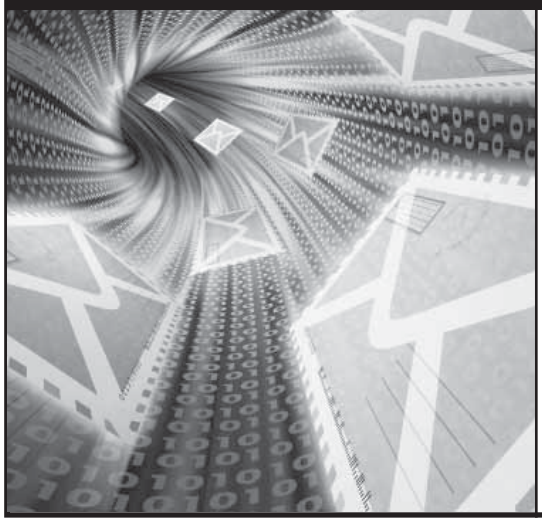
Natalie Sulimani is the founder and partner of Sulimani & Nahoum, PC since 2004. She is engaged in a wide variety of corporate, employment, intellectual property, technology, Internet, arbitration and litigation matters. She counsels both domestic and international clients in an array of industries, including Internet and new media, information technology, entertainment, jewelry, consulting and the arts.

Natalie is an Executive Committee member of the Corporate Counsel Section of the New York State Bar Association, where she is actively involved in the Technology and New Media Subcommittee as Co-Chair. She also serves on the Electronic Communications Committee of the New York State Bar Association.

Natalie is a frequent speaker and panelist on intellectual property and startup matters, especially as it pertains to technology and emerging media.

Natalie graduated from the University of Manchester at Kiryat Ono, Israel with an LLB. She lives in New Jersey with her husband and sons.

Request for Articles



If you have written an article and would like to have it considered for publication in *Inside*, please send it to either of its editors:

Allison B. Tomlinson
Gensler
1230 Avenue of the Americas
Ste. 1500
New York, NY 10020
allison_tomlinson@gensler.com

Janice Handler
handlerj@aol.com

Articles should be submittted in electronic document format (pdfs are NOT acceptable), and include biographical information.

Corporate Counsel Section's Spring CLE Presentation

Cyber Liability, Data Loss and Privacy Claims—Preparing, Protecting and Defending

By Tara A. Johnson and Elizabeth C. Hersey

The information in this article is adapted from the Corporate Counsel Section's Spring CLE presentation, *Cyber Liability, Data Loss and Privacy Claims—Preparing, Protecting and Defending*, dated June 11, 2013. This event was organized by Howard S. Shafer, Esq., Section and Program Chair of the Corporate Counsel Section. Program speakers included: Rachelle Stern, Esq. (Senior Counsel, Macy's Inc.), Joshua M. Ladeau (Assistant Vice President, Allied World Insurance Company), Bruce H. Raymond, Esq. (Partner, Raymond Law Group, LLC), Greg Osinoff, Esq. (Managing Director, Navigant), Yanai Z. Siegel, Esq. (Counsel, Shafer Glazer LLP), and Bob Bowman (Vice President, Risk Management, Macy's, Inc.). The views expressed by the panelists were their own and did not necessarily represent the views of their organizations.

Cyber Liability, Data Loss and Privacy Claims

The majority of data breaches are caused by employee errors or negligence, rather than malicious cyber-attack or spyware, and most organizations are ill-equipped to prevent such breaches. Moreover, the average organization takes 90 days to detect a data breach before it can even begin to implement remedial measures. There are various forms of encryption software that can be installed on laptops and devices that can produce immediate results in a cost effective manner. However, organizations should also be investing in the creation of comprehensive internal prevention and remediation plans. This can make it easier to obtain a thorough insurance policy, which will protect a company against losses relating to first- and third-party claims.

Preparing for a Data Breach

Bob Bowman, Vice President of Risk Management for Macy's Inc., recommends that organizations develop internal sensors for detecting potential data security breaches. To do this, an organization should first develop a common vocabulary regarding the various types of data it uses, in order to develop a comprehensive plan. The organization should strive to develop an organizational understanding of the vocabulary, consistent with the relevant industry, regulatory, and statutory vocabulary. Second, the organization must classify its data according to the agreed upon vocabulary, by categorization (for example, customer versus employee data), and according to statutory and regulatory obligations, and data sensitivity (from highly sensitive to protected data). Third, the organization must inventory the data to understand both the quantity and form of data that is susceptible to breach. For example, data may be stored in various databases, on hardware, in physical form, virtually in a cloud, on the internet or a website, or it may be in transit. Fourth, an organization should create a data map to understand the movement of its data both within and without the organization. And fifth, the organization should determine how to control its data, through systemic and cultural controls.

In addition to developing internal sensors, Greg Osinoff recommends conducting information systems risk assessments to identify vulnerabilities and procedural gaps. This can include hiring outside specialists to conduct tests, reviewing internal policies and compliance procedures, conducting physical monitoring, and obtaining a cyber-security readiness assessment report and gap analysis. While doing this, an organization should document every step taken to be used as a defense in case the organization's procedures are later called into question. These auditing procedures should then be followed by an enforcement component, in the form of an incident response plan, to be deployed after the discovery of a data breach. In developing an incident response plan, an organization should consider where the data is and how to stop access or use of the data, compile a list of contracts or obligations that may be implicated, consider possible effects on business and insurance coverage, and obtain possible legal representation. An organization should create a team of lawyers, compliance, and risk management professionals to collaborate with on the plan. The goal of this enforcement component is to have a documented account of all precautions the organization took, including comprehensive accessible instructions to employees, who can easily report potential violations.

Managing a Data Breach

There are several considerations for an organization faced with a potential data security incident. On average, such an incident costs approximately $200, and the top contributors to that amount are loss of customer business, legal services, and forensic analysis. Larger public compa-

nies may be more seriously harmed by the negative effect on their reputations, and companies that are forced to suspend operations entirely may lose valuable business during that time period.

Immediately following a data breach, organizations are often concerned and uncertain about whether a breach has in fact occurred, what risks are posed, the scope of the breach, and the extent of the organization's obligation to investigate or remedy the situation. The most important initial determinations are how the breach occurred, which data sources or physical information are involved, and who was involved. Organizations should try to control the scope of the investigation, and determine the need to notify clients, employees, or business partners.

According to Osinoff, an organization's key responses to a data breach should include quarantining the environment, preserving electronic and physical evidence, interviewing key personnel, performing forensic analysis to determine the root cause, evaluating access to data sources and physical information, and remediation. Other common incident-related tasks that companies deploy following a breach include consultation or interpretation services, forensic imaging and preservation, forensic analysis, network or application data collection, documentation or report writing, and other out-of-pocket expenses.

Bob Bowman recommends that organizations have in place an organizational compliance plan, an electronic code of conduct, and an event management process consisting of a defined decision tree or process map. The first component of the event management process is reporting, which should facilitate and encourage communication among employees immediately following a potential breach. A second component is event intake, which allows an organization to identify the symptoms of the breach, including the date of occurrence, the area affected, and a summary of the event. Following intake, an organization should conduct analysis and triage of the event, to determine the scope and extent of the breach, and any additional mitigation factors. After analyzing the breach, an organization can begin to respond to it by deploying an incident response plan, which should be in place before the breach. Following resolution of a breach, an organization should review its processes to improve upon them as a guide for future potential breaches. Bowman stresses that throughout the event management process, an organization should encourage communication—both internally among staff members, and externally with vendors or customers, where appropriate.

Legal and Insurance Considerations

In the United States, data protection has become increasingly regulated, yet as of May 2013, there is no comprehensive federal legislation. There are at least 19 federal laws related to privacy protection, and there are approximately 46 distinct state security breach laws. In addition, the Securities and Exchange Commission currently has a recommendation that publicly traded companies must disclose significant data breaches. By contrast, other countries have national privacy law standards, which may be useful in predicting the future content of U.S. data laws. In addition, the United States is behind several other countries in developing and using technologies, and therefore also behind in the litigation and resolution of disputes relating to data breaches. Bruce Raymond notes that because the Massachusetts privacy statute (940 CMR 27.00) is currently the most rigorous one in the country, organizations may seek to comply with its requirements in order to protect themselves. Moreover, there is a distinction between corporate information and personal information: personal information is treated as a consumer protection issue, and is therefore subject to more regulation and oversight as compared to corporate information.

The proposed legal standard for data loss is typically strict liability, with the requirement that a duty to protect exists. However, it is currently unclear whether there exists a private cause of action. If an organization has no evidence of planning or contingency for data breach, negligence is implied, or there may be an adverse inference spoliation charge. It is therefore imperative that organizations document all of their preparation and planning activities.

There are multiple issues that may arise in litigation defending against privacy breach and data loss claims. The first issue that arises for counsel is to understand the nature of the breach and the resulting potential criminal liability. Second, during litigation an organization has multiple reporting obligations to take into account. Therefore, counsel should consider the possibility that an organization be required not to report a breach, or delay reporting, which is seen in some criminal and human resources contexts.

A third issue that commonly arises in litigation relates to insurance, including when coverage applies and what triggers the outside counsel defense obligation. Counsel should distinguish between first party claims and third party claims. When resolving third party claims specifically, an organization must seek to contain potential losses, evaluate and develop protective third-party contract language, consider spoliation and preservation issues, and retain knowledgeable expert witnesses. This process can

be facilitated by obtaining, prior to a data breach, a favorable insurance policy. Josh Ladeau notes that underwriters are particularly looking for prevention and mitigation as a part of an organization's culture, evidenced by the procedures described above, called "defense in depth." By adopting a "defense in depth" culture, an organization can obtain broader insurance coverage with lower premiums. Ladeau also recommends that organizations fully utilize the resources offered by insurance companies, including not only money, but also templates for policies, documents, consultation time, access to vendors, white papers, and other relevant information.

Finally, document productions during litigation may lead to potential breaches within themselves because some databases hold data indefinitely and are not subject to any data destruction policy. Therefore, organizations and counsel should implement procedures to safeguard data throughout the litigation process.

Although there is little uniform statutory guidance relating to data protection, organizations can begin to prepare themselves for potential breaches in several ways. By developing a culture of prevention, communication, and compliance, organizations can be prepared to detect breaches quickly. In addition, having internal sensors, conducting information systems risk assessments, and implementing an event management process prior to a breach can accelerate response time and allow companies to mitigate losses effectively. Organizations can build on these internal efforts by obtaining a favorable insurance policy, which may help streamline any resulting litigation.

Tara A. Johnson and Elizabeth C. Hersey are students at Brooklyn Law School and summer interns at Shafer Glazer, LLP.

The "Reasonable" Perils of Data Security Law

By Yanai Z. Siegel

NEGLIGENCE. "The omission to do something which a reasonable man, guided by those ordinary considerations which ordinarily regulate human affairs, would do, or the doing of something which a reasonable and prudent man would not do."[1]

"*When we think about data breaches, we often worry about malicious minded computer hackers exploiting software flaws, or perhaps Internet criminals seeking to enrich themselves at our expense. But the truth is that errors and negligence within the workplace are a significant cause of data breaches that compromise sensitive personal information.*"[2]

According to a recent privacy institute study by the Ponemon Institute, only 8% of the surveyed data breach incidents were due to external cyber attack, while 22% could be attributed in part to malicious employees or other insiders. Loss of laptops or other mobile devices containing sensitive data topped the survey, while mishandling of data "at rest" or "in motion" were also major contributors.[3] A later study showed that 39% of surveyed organizations identified negligence as the root cause of their data breaches, while 37% were attributed to malicious or criminal attack.[4]

Negligent document disposal is a clear source of preventable negligence. On December 7, 2012, at least eight garbage bags were left unattended on a dirt road in Hudson, Florida, containing credit applications to Rock Bottom Auto Sales, with names, driver's license information, and Social Security numbers. Three days later, in Pittsburgh, Pennsylvania, job placement documents were found in a dumpster from the West Pittsburgh Partnership, all containing names and SSNs.[5] For that matter, the Internal Revenue Service in 2008 was found to have disposed of taxpayer documents in regular waste containers and dumpsters, and that a follow-up investigation revealed that IRS officials failed to consistently verify whether contract employees who have access to taxpayer documents had passed background checks.[6]

Convincing users to back up their laptops has been difficult enough in practice; getting them to encrypt them voluntarily is much more daunting a task. A 2010 Ponemon Institute study, admittedly biased towards large corporations, concluded that of those surveyed typically 46% of the laptops held confidential data, while only 30% had their contents encrypted. A startlingly low 29% of the laptops had backup / imaging software installed, which implies that more than two-thirds of all laptops if lost or stolen would leave no backup of work in progress.[7]

Even though more devices are coming to market with built-in encryption capabilities, these features may simply be left switched off by their users despite the fact that lost laptops, tablets, smartphones, U.S.B "thumb" drives and other portable devices with unencrypted contents continue to provide a wealth of information to identity thieves.

On March 22, 2013, a laptop used by clinicians at the University of Mississippi Medical Center was discovered to be missing. It contained patient names, Social Security numbers, addresses, diagnoses, birthdates and other personal information, protected only by a password.[8] On January 8, 2013, an unencrypted flash drive was stolen from a Hephzibah, Georgia middle school teacher's car, containing student SSNs and other information.[9] TD Bank had two unencrypted backup tapes with customers' and their dependents' names, SSNs, addresses, account, credit and debit card numbers go missing while being transported between two TD Bank offices in March 2012, but public notice was not made until March 4, 2013.[10]

An examination of reported data security incidents with potential or actual data privacy breaches reveals that the scope of what is deemed "reasonable" ranges from ordinary care in the disposal of documents containing personally identifiable information ("PII") and personal health information ("PHI"), to sophisticated data encryption, access authentication and other highly technical data security practices "reasonably prudent" persons, companies and governmental agencies are now expected to employ to protect the personal data that they have collected.

On October 10, 2012, the South Carolina Department of Revenue was informed of a potential cyber attack involving the personal information of taxpayers.[11] The origin of the attack was traced to a state Department of Revenue employee who clicked on an embedded link in a "salacious" email and compromised his computer.[12] The subsequent investigation revealed that "outdated computers and security flaws at the state's Department of Revenue allowed international hackers to steal 3.8 million tax records," according to Governor Nikki R. Haley. Apparently South Carolina did not encrypt Social Security numbers, and once the outer perimeter security was compromised the hackers were able to log in as tax officials and read the data.[13]

Users of online services will routinely provide personal information as a matter of course to shop or obtain other services, all of which gets recorded and tracked. Data privacy laws are intended to promote and enforce a number of fair information practices to give individuals the ability to find out what personal information is being kept and by whom, opportunities to correct or remove

such information, assurances that reasonable measures will be undertaken to protect such information from disclosure and to properly dispose of such information when appropriate, and may include remedial measures to be undertaken in the event of a data breach.

In the United States, there is no single comprehensive statute for data privacy laws.[14] Instead, a number of sector-specific federal laws have been enacted to address the particular sensitivity of information generally recorded by companies in that market sector, and forty six states have enacted data breach notification statutes. If there is a data breach, you may be liable under state law to provide notice to those affected.[15] In some jurisdictions, you may be required to provide notice to all consumer credit reporting agencies as well.[16]

The financial exposure to a data breach by a company may be insurable to some degree using various forms of "cyber liability" insurance, which expand and supplement many forms of more standard insurance coverages underwritten today. Premiums for such policies, however, are dependent upon the extent of data security practices implemented.

Conducting a data security risk assessment before encountering a data breach should identify measures that can be taken at the corporate level to provide additional protection not only to sensitive data, but also mitigate the consequences of a security incident where company data is disclosed, lost or stolen. Encrypted data in many cases may not be considered "exposed" for purposes of mandated notice to affected individuals.

In the event of a data security incident, consider obtaining a data forensic team to not only identify the source and extent of the breach, but to preserve evidence in the event that a potential prosecution may be possible.

Endnotes

1. BLACK'S LAW DICTIONARY 1184 (4th ed. 1968).
2. Privacy Rights Clearinghouse, Are the Businesses You Frequent or Work For Exposing You to an Identity Thief? (Mar. 6, 2012), https://www.privacyrights.org/workplace-identity-theft-quiz-alert-2012.
3. *The Human Factor in Data Protection*, 3 PONEMON INSTITUTE LLC (January 2012), available at http://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf.
4. *2011 Cost of Data Breach Study: United States*, 7 PONEMON INSTITUTE LLC (March 2012), available at http://www.ponemon.org/local/upload/file/2011_U.S._CODB_FINAL_5.pdf.
5. http://www.privacyrights.org/data-breach/new (check Breach Type "PHYS," Organization Type "BSR" and Year "2012").
6. *Increased Management Oversight of the Sensitive but Unclassified Waste Disposal Process Is Needed to Prevent Inadvertent Disclosure of Personally Identifiable Information*, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION (May 8, 2009), http://www.treas.gov/tigta/auditreports/2009reports/200930059fr.pdf.
7. *The Billion Dollar Lost Laptop Problem* 6 PONEMON INSTITUTE LLC (Sept. 30, 2010), available at http://newsroom.intel.com/servlet/JiveServlet/download/1544-8-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf.
8. http://www.privacyrights.org/data-breach/new (check Breach Type "PORT," Organization Type "EDU" and Year "2013").
9. http://www.privacyrights.org/data-breach/new (check Breach Type "PORT," Organization Type "EDU" and Year "2013").
10. http://www.privacyrights.org/data-breach/new (check Breach Type "PORT," Organization Type "BSF" and Year "2013").
11. Kara Durrette, *SC Department of Revenue hacked; millions of SC residents affected*, http://www.midlandsconnect.com/sports/story.aspx?id=817902#.UVyOdheYu7w (posted Oct. 26, 2012, updated Oct. 27, 2012).
12. Matthew J. Schwartz, *How South Carolina Failed To Spot Hack Attack*, INFORMATIONWEEK, Nov. 26, 2012, http://www.informationweek.com/security/attacks/how-south-carolina-failed-to-spot-hack-a/240142543.
13. Robbie Brown, *South Carolina Offers Details of Data Theft and Warns It Could Happen Elsewhere*, N.Y. TIMES, Nov. 20, 2012, available at http://www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hacking-episode.html?_r=0.
14. PETER P. SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION 41 (International Association of Privacy Professionals) (2012).
15. NYC Administrative Code § 20-117(c) (2013); NY CLS State Technology Law § 208(2) (NY state residents only); 73 Pa. Stat. § 2303 (PA residents).
16. 73 Pa. Stat. § 2305; NY CLS State Technology Law §208(7)(b).

Yanai Z. Siegel serves as Of Counsel at Shafer Glazer, LLP with more than twenty years' experience as both corporate counsel and as an information technology and management professional in the retail, wholesale, and distribution logistics sectors. His background in business operations facilitates developing response plans with corporate management for computer-related contingencies, such as data protection failures.

Yanai has previously served at Appliance Dealers Cooperative, first as Assistant Comptroller, then Director of Computer Services, and later as Corporate Counsel in conjunction with a variety of senior management roles. The company provides goods and services to major home appliance retailers across nine states, including New York.

Yanai received his Bachelor of Science in Business Administration from Georgetown University with concentrations in accounting and finance, then an MBA from Rutgers University Graduate School of Management in marketing and management, and then a JD from Rutgers-Camden School of Law. Yanai is admitted to practice in New York, New Jersey and Pennsylvania, and is a member of the Association of Information Privacy Professionals as well as the New York State Bar Association Corporate Counsel Section.

Alternative Dispute Resolution (ADR) Law—Why Tech Lawyers Should Care, and What They Should Do About It

By David J. Abeshouse

Unfortunately, most clients—as well as their lawyers—do not know enough about Alternative Dispute Resolution (ADR—principally arbitration and mediation) to serve themselves and/or their clients well, and too much of what they believe they know is based at least in part on myth and historical misconception. Recent formal and informal surveys reflect that many corporate counsel are less inclined to employ hardball litigation at least initially, and tend to favor using mediation to manage conflict. Many corporations and law firms have signed the CPR Institute's 21st Century ADR Pledge, committing to resolve disputes through ADR processes when appropriate.[1] And arbitration—while controversial for some—can be highly beneficial and preferable to litigation, if initiated and managed properly. So it seems appropriate to address some of the principal benefits (and detriments) of using ADR in technology and similar business disputes, comparing and contrasting it with court litigation, so clients and counsel will have the tools to decide when it likely will be better for them to be in court, arbitration, or mediation, and how best to implement the decision.

ADR Is a Creature of Contract

It all starts with the contract. Better customized contractual dispute resolution clauses lead to better ADR proceedings. Succinctly put: Bad clause, bad process, unhappy client, unhappy lawyer; good clause, good process, happier party, happier counsel. Business transactional counsel and their clients need to focus more and better attention on this seminal issue, because if they give it short shrift, it can and likely will return to "bite" them when a dispute arises.

The honeymoon phase of a business relationship—when the parties are amicably getting together contractually—is precisely the best time to arrange for a business "prenup" in the form of a well-crafted ADR clause in the initial business agreement among the parties, whether an internal document such as a corporate shareholders agreement or LLC operating agreement, or an external agreement between companies entering into a joint venture, vendor-vendee relationship, or other arrangement. ADR is not one-size-fits-all; rather, strategic customization, based on dispute resolution experience of counsel targeted to the specific contractual relationship at hand, carries the day. "Clause-building" software available online may afford a starting point; actual expertise of counsel makes the difference between a deficient and an appropriate clause.

Unfortunately, it is clear, based on extensive review of many hundreds of executed business agreements, that most contract-drafting lawyers squander that opportunity either by not knowing when to include a dispute resolution clause providing for arbitration and/or mediation instead of court resolution of disputes, or by using an old, tired, "standard" dispute resolution clause (a/k/a the "sub-standard clause"), which in its two-or-three-sentence simplicity does nothing to assist the parties achieve the fast, fair, expert, economical, private, customized resolution of their business dispute for which ADR is suited.

Defining What We Are Talking About—Contrasting Processes

The state and federal courts generally favor arbitration, as reflected in numerous decisions, including at the United States Supreme Court level, upholding broad interpretations of arbitrability of disputes and encompassing substantial deference—under the applicable federal (e.g., Federal Arbitration Act) and state (e.g., NY CPLR Article 75) statutory standards—in sustaining arbitral awards. As an added bonus: The better the private ADR systems work, the better it will be for the courts, because the cases resolved through arbitration and mediation will be off the court dockets, allowing the court systems to do a better job when less burdened with an excessive caseload.

Arbitration:

- is essentially a streamlined version of litigation, culminating in an evidentiary hearing (trial) before a panel of one or three arbitrators (typically neutral), who will render an award that is enforceable as a court judgment
- employs a flexible selection process encompassing neutrality, allowing for parties and counsel to choose from a list of arbitrators provided by the forum or independently, and to delineate qualifications of the neutral arbitrator(s)
- is flexible in many other respects, as it is governed by the parties' contract which can be customized in advance according to the needs of the particular situation

- generally is private and may be rendered confidential by agreement (unlike public record court actions)
- results in a binding award akin to a court judgment
- offers "finality" in that it is difficult to vacate (appeal) an arbitral award—judicial review usually is limited to serious defects in the process, predicated on statutory standards, rather than on the nature of the resulting award
- provides subject matter expertise of the neutral hearing the case, in contrast to many judges who are "generalists" or expert in other areas, and juries that are unpredictable at best
- usually strips away many of the unnecessary yet time- and money-consuming elements of litigation such as exhaustive discovery and endless motion practice, yielding considerable savings of time and expense, as statistically demonstrated by independent studies (cost savings naturally are greater when a sole arbitrator is used, rather than a panel of three)
- does not set legal precedent, which may benefit some parties but not others
- hearings are scheduled at times and places convenient to the parties and counsel rather than at courthouses and based on the judge's schedule; moreover, whereas trial days in court are short and often interrupted, arbitration evidentiary hearings are more efficient, often yielding more than double or even triple the actual number of hours of hearing per day, resulting in shorter proceedings
- is managed actively by the arbitrator and, if a forum (such as the American Arbitration Association [AAA], JAMS, NAM, and the like) is involved, then also by a case administrator, to keep the process on track[2]
- often is preferable for situations involving international parties, as arbitration usually is more effective than litigation in any country for obtaining an enforceable judgment, and also may be perceived by one or more parties as more fair than the courts of a particular foreign nation.

Mediation:

- is a settlement negotiation facilitated by a neutral whose presence and activity changes the settlement dynamic, and assists the parties through a variety of techniques to achieve a more effective, efficient, rapid, beneficial, and permanent settlement of the dispute
- lets parties and counsel select the mediator, independently or through a forum
- is not binding unless and until the parties sign a written settlement agreement, so the parties control the resolution of the dispute
- allows parties and counsel to manage outcomes; the mediator does not force a decision on the parties
- usually is undertaken with the assistance of counsel, but may encompass elements where counsel steps back, if counsel and party consent
- empowers the parties to meet collectively or separately in caucus with the mediator, to suit the situation
- permits creative solutions that a judge or arbitrator could not create
- avoids adverse determinations that a judge or arbitrator might have to impose
- is flexible in style, ranging from transformative to facilitative to evaluative
- is private and typically confidential (and mediators enjoy general immunity from subpoena if there is a subsequent court or arbitral proceeding)
- focuses on the parties' interests rather than merely on their positions
- affords parties the opportunity to be heard (and even "vent"), unrestricted by the rules of evidence that apply in court
- fosters and facilitates communication, identification of issues, and generation of options for settlement
- allows for all parties to benefit rather than having winners and losers
- permits the parties to improve communication and preserve relationships, even to the point of enabling them to work together in future
- provides considerable savings of time expenditure both in overall hours, and duration from start to conclusion
- is highly cost-effective, as it takes relatively little time
- is extremely successful, with approximately 85% of mediated business and technology cases resulting in settlement agreements

– encourages parties' compliance because they retain considerable control over the process and result

– capitalizes on the experience and creativity of the mediator, who may help the parties to reach creative solutions that they might not have achieved otherwise

– may be used before or instead of litigation or arbitration; or may occur during the course of a litigated or arbitrated matter

– often is less stressful for the parties than a court trial or arbitral evidentiary hearing

– is appropriate for both simple and complex matters.

The "DR Continuum" graphically reflects the principal categorical distinctions among four main categories of dispute resolution: negotiation, mediation, arbitration, and court litigation:

Dispute Resolution Continuum

More control by parties — Less control by parties

More informal process — More formal process

<---------->

Consensual: Parties Decide Outcome — Adversarial: Neutral Decides Outcome

| | | — | | |

| | | — | | |

Negotiation (parties / counsel) — ***Mediation*** (adds mediator) — ***Arbitration*** (adds arbitrator) — ***Litigation*** (adds judge)

<---------->

More private process — More public process (less privacy)

Lower cost of procedures overall — Higher cost of procedures overall

Less assistance / intervention of others — More assistance / intervention of others

Myths and Misconceptions About ADR

Misunderstandings about ADR persist, notwithstanding substantial evidence to the contrary; a few examples follow.

– *Some believe that arbitration is more expensive than court.* This assumption results from several sources. First, occasionally an arbitration proceeding indeed may become protracted and expensive, but this is statistically rare, both based on independent studies as well as empirical observation of experienced practitioners. It is more prone to occur with a three-arbitrator panel, but even then, is far less likely to become protracted than had it been in court. Second, arbitration requires payment of the arbitrator's fees, often up-front; however, this relatively modest add-on (the arbitrator expends a small fraction of the time on a case relative to counsel in the case) is far outweighed by the substantial reduction in overall costs because the timespan of the case in arbitration is considerably shorter than in court, costly segments of the proceedings—such as discovery and motion practice—are eliminated or reduced, and the matter proceeds more efficiently through hearing than would a similar matter consigned to court.

– *Some believe that arbitrators merely "split the baby" and do not focus on the merits.* Closer consideration reveals that this simply cannot be accurate in any respect. Arbitration arose and proliferated precisely because it was intended to address many of the perceived defects in the court system; if arbitration merely resulted in a midpoint compromise ruling in any appreciable percentage of cases, there would be no reason for anyone to use arbitration. To the contrary, independent studies demonstrate that there actually is a statistical dearth of arbitration awards falling within the 40 to 60% range of monetary claims—the opposite of splitting the baby. The myth likely results in part from people—including

lawyers—confusing arbitration and mediation. Compromise is an element of the latter; modern arbitrator training incorporates many techniques for avoiding the natural human tendency to find middle ground.

– *Some believe that mediators are not necessary.* Parties and their counsel may think that they have the tools to reach resolution on their own, but that often is not the case. Indeed, were that so, they might not have become embroiled in the dispute in the first place. Moreover, the presence of a neutral favorably alters the settlement dynamic in ways that some have described as "magical," as parties and counsel tend to behave more collaboratively when a mediator is involved. Mediators can dig into matters and ascertain what really underlies the dispute, as it often is not what it superficially appears to be about, and can find out what it will take to satisfy all parties and let them get back to business. Not only does the mediator use techniques geared to enhance likelihood of resolution (including the potentially game-changing opportunity for caucusing, which is not possible absent a mediator), but the mediator's experience in prior cases and his or her creativity in the realm of crafting settlements makes that eventuality far more likely than it would be absent the neutral facilitator.

– *Some believe that arbitrators are arbitrary.* Arbitrator qualification and training are quite rigorous and continuing, and the scope of the arbitrator's authority over a given matter is predetermined by the arbitration clause and the rules it invokes. Indeed, one of the limited grounds for judicial vacatur of an arbitrator's award is if an arbitrator is found to have exceeded the scope of arbitral authority under the contract. Because very few arbitration awards are the subject of motions to vacate, and very few of those motions are granted, this obviously does not happen regularly, thus underscoring the concrete nature of arbitral awards. For particularly complex or high-dollar disputes, the parties can provide for a three-arbitrator panel as an additional safeguard.

– *Some outside counsel fear diminished legal fees.* These lawyers may be short-sighted. Clients who have been through ADR proceedings generally are more satisfied with and refer more business to their ADR lawyer than do those who go through court litigation, all else being equal. They understand that their ADR lawyer is united in interest with them to a greater degree than in litigation representation. It is preferable from a practice management perspective for outside counsel to have multiple efficient ADR matters on the docket rather than one large litigation: The lawyer is more in control of scheduling, better able to deliver what has been promised to clients, and is not left wondering where the next case will come from once the large litigation ends.

When Might One Prefer Court Over ADR? Some Examples:

– The more moneyed party, if willing to expend the time and resources, may be able to use the less streamlined court system to its advantage, applying that leverage to "bury" its less solvent adversary.

– The party wishing to delay the initial result (judgment or award) and the ultimate result (on appeal) will achieve that aim better in court than in arbitration.

– The party wanting to create judicial precedent and a public record only can do so in court (some "repeat players" may prefer creating precedent, whereas others may abhor it).

– The party expecting to be able to prevail in the case on an early motion may prefer court because arbitral panels tend to be less prone to summary adjudication than are the courts.

– The party anticipating the need for a temporary restraining order (TRO) and preliminary injunctive relief (PIR) likely will be more secure obtaining the TRO and PIR from a court rather than an arbitration tribunal, for purposes of enforcement; however, as a general rule, parties to an arbitration clause retain the right to seek immediate injunctions such as a TRO and/or PIR in court to maintain the *status quo* pending adjudication by the arbitration panel. In this context, the two forums peacefully co-exist. A similar situation exists for enforcing certain subpoenas.

– ADR is less appropriate when you need to ensure the ability to conduct significant and far-reaching discovery.

– ADR may be disadvantageous when one "inherits" a poorly conceived and/or poorly drafted contractual dispute resolution clause; the parties may be bound to governing language that may be ambiguous, logistically impractical, difficult to enforce, or otherwise problematic, or ironically may have to litigate over the interpretation of the clause (the better route is to try to renegotiate the clause—after the fact—for the greater good of all parties).

Application of ADR to Technology Cases—Selected Issues

Cases involving technology (e.g., intellectual property [IP] including copyright, trademark, and patent; licensing and Software as a Service [SaaS] agreements; trade secrets; NDAs; R&D agreements; computer and Internet law; and similar matters) that otherwise would reside in federal or state court may be handled in a variety of ADR forums or privately.

When parties litigate technology matters in federal or state court, the statutory procedural rules (e.g., FRCP, FRE, FRAP, CPLR) are set; but when they decide to arbitrate, they have a menu of prospective forums—and even sets of rules within forums—from which to choose, and even these rules can be contractually modified by the parties, in advance. For example, within the AAA alone, at least five sets of rules and procedures are available for technology disputes: (i) The Commercial Arbitration Rules and Mediation Procedures; (ii) The Large Complex Commercial Disputes Procedures; (iii) The Supplementary Procedures for International Commercial Arbitration; (iv) The Supplementary Rules for the Resolution of Patent Disputes; and (v) The International Dispute Resolution Procedures. They are distinct yet complementary, and may be used singly or together, as the contract prescribes. The patent rules, for example, automatically apply to patent cases (unless the parties have opted out); ensure the expertise of the neutral; in contrast to the parsimonious international rules, grant considerable discretion to the arbitrator regarding the nature and extent of discovery; and provide expressly for the availability of temporary and preliminary injunctive relief to maintain the *status quo* during the pendency of the matter (again, resort to court for injunctive relief often may be more efficacious). Not surprisingly, familiarity with the various ADR rules when in arbitration or mediation is as essential as knowing the FRCP or CPLR when in court.

After the United States Supreme Court decided *eBay Inc. v. MercExchange, L.L.C.*,[3] judicial injunctive relief has been less available in patent infringement cases. It may be more readily obtained, however, in some arbitral forums. This can play a critical role in facilitating resolution of patent disputes. Because patent adversaries often are strangers with whom there is no preexisting contractual relationship, mutual submission to arbitration would have to be negotiated. Incentive exists, as it may be better for both sides than federal litigation (which often also encompasses a judicially mandated "mediation" phase, or a process nominally resembling mediation). The extensive discovery often conducted in patent cases is largely unnecessary; the subject invention itself can be analyzed without examining the minutiae of every e-mail and memorandum. Infringement and validity are not necessarily discovery-intensive issues, and the extent of discovery relating to damages will vary from case to case. Patent cases indeed can be arbitrated. Patent litigators would need to break out of the court litigation mindset to consider the potential advantages of arbitration, and would need to become conversant in ADR processes, but this might prove beneficial to their clients, and hence themselves, in the medium-run, if not immediately. Corporate in-house counsel can influence outside counsel to encourage steps in this direction.

Federal and state judges—with some exceptions—generally are not technology experts, and only a handful of jurisdictions have technology-oriented courts. The specialized panels of several national and international arbitral forums stand in stark contrast, with entire panels of technology law, science, and business experts as neutrals. This disparity contributes to technology cases often languishing in court (while outside advisors may be used to review the parties' submissions) whereas these cases can receive more expeditious treatment via ADR.

ADR also can be useful in adjudicating claims of theft of confidential information, where breach of an NDA is asserted. The extent of use of confidential information often is unclear; this provides ideal fodder for counsel and parties to have an open and frank discussion about the evidence, in the context of a confidential mediation. The presence of the mediator changes the settlement dynamic, and helps both sides gain perspective and fashion creative resolution of the dispute. With earlier resolution, there remains more of the "pie" with which to work, as resources have not been squandered on unnecessary legal fees. Similarly, trademark cases can be mediated—parties can work out whether existing inventory can be sold off, whether a disclaimer is sufficient, who retains the website, and whether a limited license can be created (e.g., a co-existence agreement or consent to use agreement).

International ADR Technology Cases

Many technology cases are international in scope. Because national court systems are diverse, ADR provides an appropriate means for resolving cross-border claims. The Arbitration and Mediation Center of WIPO—the World Intellectual Property Organization—offers ADR options for resolution of international commercial disputes between private parties.[4] The International Chamber of Commerce (ICC) likewise provides ADR services for a wide range of international business disputes, including technology cases.[5] And the International Centre for Dispute Resolution (ICDR), a division of the AAA, similarly handles international technology matters.[6] The ICDR often applies the United Nations Commission on

International Trade Law (UNCITRAL) rules. The ICDR also was selected by the Internet Corporation for Assigned Names and Numbers (ICANN) as the dispute resolution provider for two programs relating to domain names.

A recent international survey on dispute resolution in technology transactions conducted by the WIPO revealed several interesting trends:

- Survey respondents were asked to estimate what percentage of the technology-related agreements led to disputes, among NDAs, R&D agreements, licenses, settlement agreements, M&A agreements and assignments. Among technology-related agreements, licenses most frequently give rise to disputes (25% of survey respondents), R&D agreements rank second (18% of respondents), followed by NDAs (16%), settlement agreements (15%), assignments (13%), and M&A agreements (13%).
- 94% of survey respondents indicated that negotiating dispute resolution clauses forms part of their contract negotiations.
- Court litigation was the most common stand-alone dispute resolution clause (32%), followed by (expedited) arbitration (30%) and mediation (12%). Mediation is also included where parties use multi-tier clauses (17% of all clauses) prior to court litigation, arbitration, or expert determination.
- Survey respondents generally perceived an increasing trend toward out-of-court dispute resolution mechanisms.
- Cost and time are the principal considerations for survey respondents when negotiating dispute resolution clauses, both in domestic and international agreements.
- For international agreements, survey respondents placed a higher value on enforceability and forum neutrality than they did for domestic transactions.
- Enforceability also ranked as a motivating factor among survey respondents using court litigation and arbitration clauses. Finding a business solution was an important factor for respondents choosing mediation.[7]

Some forums have specialized panels relating to technology; for example, CPR's roster includes:

- Technology / IP—This panel is composed of neutrals with experience in all aspects of scientific and technological disputes. Most have backgrounds in patent and other intellectual property disputes.
- Trademark—This panel includes practitioners who are highly experienced in resolving trademark, copyright, unfair competition, design patent, and trade dress disputes between corporations.[8]

Focus on the Contractual Clause

Armed with basic knowledge about the ADR alternatives, the contract-drafter has a better idea about what might be best to incorporate into the dispute resolution clause, including, depending on the situation:

- whether the clause will be of "broad" all-encompassing scope or limited in some fashion (note: broad-form clauses limit the need to resort to court for interpretation)
- whether the clause will specify only mediation (allowing the case to go to court if not settled) or med-arb (allowing the case to go to arbitration, preferably before a different neutral, if not settled through mediation by a certain milestone) or only arbitration (rendering pre-arbitration mediation less likely, and precluding court litigation except in limited circumstances)
- which forum (e.g., AAA, ICDR, JAMS, NAM, CPR, ICC, or an independent) to invoke, and in some circumstances whether to include a back-up forum
- which set of rules should govern (e.g., Commercial Rules)
- whether one or three arbitrators will constitute the panel (and whether all will be neutral), and whether the number of arbitrators will differ depending on the size or complexity of the case
- setting the locale or venue of the proceeding, and governing state or federal law
- provision that any arbitration award rendered may be entered as a judgment and enforced through courts having jurisdiction
- setting any limitations on the types or amount of damages that may be awarded
- specifying the language in which the proceeding will be conducted
- whether the arbitrator(s) will have jurisdiction to rule on challenges to the validity of the arbitration agreement
- any experience or credentialing requirements of the neutral mediator or arbitrator(s) (e.g., for a three-arbitrator panel, the clause could specify that the panel will consist of one lawyer with at least 15

years of IP law experience; one CPA with technology valuation experience and credentialing; and one industry expert focusing on the particular IP niche at issue)

- requiring basic scheduling availability commitments of prospective arbitration panelists, in an effort to promote expeditious proceedings
- any exceptions from the set of governing rules (such as differing discovery guidelines or specific mandates for the timing of the proceedings, taking care not to turn the proceeding into the equivalent of court litigation)
- any optional rules (e.g., emergency measures of protection) to be invoked
- any additional confidentiality provisions desired
- the repercussions of a party's failure to pay its required share of deposits for arbitrator compensation and/or forum administrative charges
- use of "baseball arbitration" (used for MLB salary determinations)
- permission for exercise of discretion by the arbitrator in determining the extent of discovery and prehearing motion practice, and whether there will be a single expert rather than one for each side
- whether the arbitrator has discretion to award attorneys' fees to the prevailing party
- allowing low-dollar claims to be heard in small claims court
- a severability provision to maintain any provisions not ruled invalid
- excluding judicial review (but perhaps allowing arbitral review through the forum)
- whether the award should be in bare/standard form, or a reasoned opinion
- and a nearly unlimited variety of other prospective provisions suited to the particular situation.

A contractual ADR clause should: be clear and unequivocal, be strategically designed to maximize advantage to the client and/or all parties in as many respects as possible, include all essential elements, refrain from overspecificity that might make it impossible to fulfill, avoid converting the proceeding into the non-court equivalent of litigation (if the parties want litigation, they should go to court), and be equitable and enforceable.

With a bit of advance strategic thought, business owners and their counsel can include a dispute resolution clause tailored to their particular circumstances. Opposing counsel often accedes to the proffered terms, unaware of the alternatives. Unfortunately, in practice, all too often negotiating dispute resolution clauses is an afterthought, if it is considered at all. Parties tend to negotiate them minimally after the rest of the contract has been negotiated, ignoring that a dispute resolution clause becomes a key provision when a dispute later arises.

Conclusion

Business owners and their counsel need to know more about ADR, to protect themselves against the vagaries inherent when inadvertently defaulting to court litigation. Rather, a dispute resolution clause is an essential element of any business agreement, as it can be uniquely customized to enhance the likelihood of appropriate resolution of any dispute that might arise out of that agreement. To do so, counsel must have substantial dispute resolution experience or obtain guidance from one who does, and apply that knowledge to the circumstances at hand. This is particularly essential in any technology agreement, where a dispute about the subject matter might otherwise result in bet-the-company litigation.

Endnotes

1. *See* http://www.cpradr.org.
2. *See* http://www.adr.org ; http://www.jamsadr.com ; http://www.namadr.com.
3. 547 U.S. 388 (2006).
4. *See* http://www.wipo.int.
5. *See* http://www.iccwbo.org.
6. *See* <http://www.adr.org/aaa/faces/aoe/icdr?_afrLoop=534489613884016&_afrWindowMode=0&_afrWindowId=vceitldh3_39#%40%3F_afrWindowId%3Dvceitldh3_39%26_afrLoop%3D534489613884016%26_afrWindowMode%3D0%26_adf.ctrl-state%3D1dns7rthjz_4>.
7. For further results, *see*: http://www.wipo.int/amc/en/center/survey/results.html.
8. *See* <http://www.cpradr.org/FileaCase/CPRsNeutrals/SpecialtyPanelsofNeutrals.aspx>.

David J. Abeshouse is a solo business litigator, arbitrator, mediator, writer, speaker, and past adjunct professor of ADR Law at St. John's University Law School. He is a Fellow of the College of Commercial Arbitrators (CCA), and a member of the National Academy of Distinguished Neutrals (NADN). He represents clients in B2B dispute resolution, and serves on the Commercial Panels of Neutrals of the American Arbitration Association and several other national and international ADR forums. He can be reached at his Uniondale, NY office through his website, at www.BizLawNY.com.

The Duty to Preserve and the Risks of Spoliation—How Organizations Can Preemptively Limit the Costs of Electronic Discovery

By Jamie Weissglass and Rossana Parrotta

I. Introduction

The best defense against spoliation sanctions is preserving evidence. However, in the era of Big Data, organizations often face a Goldilocks dilemma: preserve too much electronically stored information (ESI) and discovery becomes unwieldy and expensive; preserve too little and face sanctions, which can range from shifting the costs of discovery to adverse inference instructions to dismissal.[1] Moreover, the more data an organization has, the more difficult it is to find needed information; delays in response can lead to noncompliance with court and government agency rules and result in penalties. Consequently, saving everything is risky and not economically feasible. On the other hand, it is clear that failing to retain the right information is equally, if not more, risky. Fortunately, there is a solution that is "just right": developing an information governance and management program that provides for routine, defensible destruction of data pursuant to well-researched and documented retention schedules. Under Rule 37(e) of the Federal Rules of Civil Procedure, federal courts cannot impose sanctions for data lost "as a result of the routine, good-faith operation of an electronic information system." In other words, routine, automatic deletions of electronic records that have met their retention requirements and are not subject to a duty to preserve should not be penalized. The best defense against discovery sanctions therefore starts with comprehensive information governance and litigation readiness programs—that begin well before litigation is on the horizon.

II. Litigation Readiness

Litigation readiness begins with an organization focusing on managing information responsibly. The core of this responsibility is consistently following an information governance and management program that addresses the entire lifecycle of information, from creation or receipt to disposition.

A. Establish a Litigation Readiness Team

First, the organization should establish a team to create and oversee its litigation readiness program. In implementing the program, the team will be responsible for working with the records and information group (RIM) to confirm that there is a defensible records retention policy, establishing procedures relating to preservation of information when there is a duty to preserve, creating and monitoring litigation holds to ensure preservation, and training employees on the program. The team should consist of representatives from the Legal, RIM, IT, and Compliance departments, as well as representation from the business units. The team may also include outside partners, such as e-discovery specialists and third-party vendors that the organization will rely upon in the event of litigation.

B. Assess the Information Landscape

The next task is to identify likely locations of information typically sought in litigation. Many organizations find it helpful to create a data map that memorializes the locations and types of the organization's most commonly requested forms of ESI. In creating the map, the team should not overlook legacy data or emerging forms of information, such as voicemail, social media, and text messages. It should also account for any data stored in the cloud or on mobile devices. If the team cannot determine what is stored in a particular repository, sometimes sampling or cataloging the data may be of some help. As important as creating the data map is maintaining it in what is a very dynamic and constantly changing information management landscape. Data maps can quickly become stale without this vigilance.

C. Create a Defensible Disposal Program

The organization's information governance program should define records retention periods and provide for routine destruction of records, including ESI, whose retention requirements have expired and are not subject to a preservation hold order. The records and information management team typically develops the retention schedule by working with the business unit representatives to identify their information and related systems, as well as the business needs for the records—their purposes and useful life. The records and information management team will then conduct the legal research into the applicable recordkeeping regulations, validated and approved by the team's legal experts. The legal and operational needs for the records are then used to determine the appropriate retention period, and the sensitivity classification of the information determines the method of disposal. It is particularly important to work with IT to understand the

disposal of ESI, because often those processes can be automatic. (For example, many organizations have systems that automatically delete emails after a certain period.)

A key procedure to develop is one that addresses records and information of departing employees to ensure responsibilities for on-going retention are defined, and to ensure information is available and accessible. Otherwise, the information may be lost. For example, data can be lost if the former employee's computer is wiped and given to another employee, if a mailbox or the exchange server is shut down, or if a file share that belonged to the former employee is deleted.

Note that the information governance program and records retention policy is regarded as "best practice" and is not something to institute in anticipation of litigation. Instituting a program or changing its rules after learning of a potential dispute may give rise to an inference that the party enacted its policy to facilitate the destruction of evidence.[2]

D. Determine When the Duty to Preserve May Be Triggered

Once the information governance program is in place, it can be helpful for the team to anticipate scenarios when the duty to preserve will be triggered. Pre-planning can mitigate the risk of *ad hoc* decisions that could prove inefficient and inconsistent.

Unfortunately, there is no bright-line test to determine when the duty is triggered. Under New York federal and state law, the duty to preserve arises when litigation is "reasonably anticipated."[3] Obviously, initiating litigation, retaining counsel, or receiving a complaint, subpoena, or notice of government inquiry puts a party on notice. But New York courts have established that the duty to preserve can arise well before a party receives notice of a claim.[4] Consider the following common, thought-provoking scenarios:

Does a triggering dispute exist? The "mere existence of a dispute between two parties does not necessarily mean that a party should reasonably have anticipated litigation and taken steps to preserve evidence."[5] Some courts have excused parties from the duty to preserve where they show that claims similar to those in the lawsuit usually do not lead to litigation;[6] other courts disagree.[7]

Who knows about the dispute? Key personnel must be aware that litigation is likely.[8] If only a few employees in a firm or municipality are aware that litigation may be imminent, it will not necessarily trigger the duty. However, if a lawyer receives notice, a higher standard may apply: in one case, receiving a letter terminating an attorney's representation "for some reasons not yet fully defined" established the duty.[9]

Is litigation foreseeable for other purposes? At least one court has found that designating documents as protected work product prepared "in anticipation of litigation" triggers the duty to preserve.[10] The court ruled that if "litigation was reasonably foreseeable for one purpose…it was reasonably foreseeable for all purposes."[11]

What is the regulatory environment? New York courts have found regulations requiring the retention of records sufficient to warn an organization to preserve documents, even if litigation involving those records is not reasonably foreseeable.[12] Similarly, a duty to preserve can arise as early as the inception of a relationship between regulated parties.[13] For example, one court relied on the rules of professional responsibility and ethics opinions in finding the obligation to preserve documents arose when lawyers began to represent a party.[14]

When does the duty end? At some point, the duty to preserve will end and organizations can resume programmatic destruction. Settlement talks do not "vitiate the duty to preserve"; such a standard "ignores the practical reality that parties often engage in settlement discussions before and during litigation…[A contrary] argument would allow parties to freely shred documents and purge e-mails, simply by faking a willingness to engage in settlement negotiations."[15]

Given the range of circumstances that can create reasonable anticipation, when in doubt, parties should err on the side of presuming the duty exists.

E. Determine the Scope of the Litigation Hold

Once the duty to preserve is triggered, the next step is to figure out what data to save. A party must preserve "what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request."[16] This does not mean parties must preserve "every shred of paper, every e-mail or electronic document, and every backup tape."[17] Instead, they must preserve ESI that is relevant and unique; it is unnecessary to retain multiple copies.

The NYSBA's E-Discovery Committee suggests using the following criteria to determine what to preserve: "the facts upon which the triggering event is based and the subject matter of the triggering event; whether the ESI is relevant to that event; the expense and burden incurred in preserving the ESI; and whether the loss of the ESI would be prejudicial to an opposing party."[18]

Some courts outside New York have directed parties to *The Sedona Conference Commentary on Proportionality*, which suggests weighing the burden of preservation against the data's potential value and uniqueness, in setting the scope.[19] Some federal courts also tend toward considerations of proportionality, and a proposed amendment to Fed. R. Civ. P. 26(b) would limit the scope of discovery to information "proportional to the needs of the case." However, New York courts have not been receptive to this concept. One judge explained that the proportionality "standard may prove too amorphous to provide much comfort to a party deciding what files it may delete or backup tapes it may recycle."[20]

As with other aspects of preservation, a conservative approach is best. In consultation with key stakeholders counsel can identify issues likely to arise; they can then pinpoint the types of documents likely to be relevant and the probable key custodians. Before deeming ESI inaccessible because of undue burden, counsel should consider whether the data is available elsewhere; if it is not, courts can override considerations of undue burden where the "requesting party shows good cause."[21]

One of the best ways to limit the scope of preservation and manage costs is to reach an agreement with opposing counsel regarding the scope of discovery. For example, agreement can be reached on issues such as the identity of key custodians, types of information sought, etc. The "meet and confer" process in federal court and in New York Commercial Division cases provides structured venues for discussions with opposing counsel, but counsel can also reach agreements without formally required meetings.

F. Stop the Destruction of Data to Be Preserved

Satisfying the duty to preserve requires organizations to suspend their routine destruction mechanisms.[22] A litigation hold is the communication mechanism typically used to document and inform employees of the need to suspend destruction. It has been held that the "utter failure to establish any form of litigation hold at the outset of litigation is grossly negligent."[23] However, the proper form of litigation holds is an open question: must they be in writing, or will oral holds suffice? There is arguably a mix of opinions on the subject.

While at least one federal court held that the failure to issue a written litigation hold constituted gross negligence,[24] the Second Circuit rejected that position.[25] New York state courts have also declined to follow that stance. For example, one court found "the functional equivalent of a litigation hold" where a company's policy was "to retain all information relevant to the claims and litigation."[26] Furthermore, it ruled "a directive to refrain from purging documents is unnecessary and unwarranted… [and] would risk confusion regarding the policy and practice to preserve all documents in all formats for all files."[27]

At least one New York court has supported tailoring a litigation hold's form to the organization's size.[28] The court noted that in smaller organizations, "issuing a written litigation hold may not only be unnecessary, but it could be counterproductive, since such a hold would likely be more general and less tailored to individual records custodians than oral directives could be."[29]

Even so, the best practice is to issue a clearly written litigation hold, to provide tangible evidence of a party's good-faith attempt to meet its discovery obligations.[30] Litigation holds should describe the subject matter and relevant date ranges, instruct recipients to preserve ESI until notified otherwise, and provide a contact person in case of questions.[31]

In preserving ESI, it is important for the legal department to collaborate with IT in stopping automatic destruction and in issuing the legal hold. Discussions should cover the types of data that may be implicated and the names of key custodians. If any of these types of data are subject to automatic destruction, IT should halt that process for those categories of data. Some organizations find it useful to adopt a "triage" approach—immediately addressing data for the most critical custodians while continuing to identify additional relevant information. In addition to stopping automatic destruction and issuing a legal hold, counsel can consider whether there is the need for IT to collect any data immediately; for example, if certain employees may not follow the directive to preserve data.

Identifying the sources of data early can also help determine whether collecting that data may place an undue burden on the organization, necessitating discussions with opposing counsel or motions to the court for protection.

G. Ensure Compliance With the Litigation Hold

Issuing a litigation hold is not the final word in meeting the duty to preserve. Organizations should take affirmative steps to ensure compliance throughout the organization; leaving preservation up to lay employees without adequate guidance is asking for trouble. Counsel too, should work to ensure compliance.[32]

Some organizations require employees to sign an acknowledgment that they have read, understood, and agree to the terms of the litigation hold. Tracking the distribution of the holds as well as any employee acknowledgements is important in demonstrating the organization's efforts to ensure preservation.

In addition, organizations should reissue and update litigation holds periodically to ensure their effectiveness.[33] It is also counsel's responsibility to remind custodians of their duty to preserve, communicating directly with key players.[34] Again, keep in mind that documentation of these reminders may be important in establishing the company's good faith effort to preserve evidence.

In fact, it is a best practice to record every step of the litigation hold process to ensure defensibility, including the reasoning for determining when the duty to preserve was triggered and decisions for what data to preserve. If the scope of the litigation shifts, not only should the litigation hold be updated to reflect new claims, date ranges, and custodians, but the reasoning for doing so should be memorialized. It is also important to record critical dates, including when the initial hold and reminders are issued. Although litigation holds are typically privileged, courts have required their production when spoliation has occurred.[35]

To help ensure consistency in following litigation hold procedures, the team may want to consider litigation hold software, which can build in rules consistent with a retention policy and document employees' receipt and acknowledgement of the hold and reminders.

H. Educate Employees and Monitor Compliance

A litigation readiness program is only as good as the degree to which its policies and processes are adhered to. Because employees are on the front lines, they may be the first to become aware of circumstances giving rise to potential litigation. Therefore, they should be coached to approach management or legal counsel as soon as they learn of any risk. The litigation readiness team can establish a training program that simply explains the company's discovery process, legal hold policies, and document retention protocol. To reinforce the training, the team may want to share examples of the negative ramifications of failing to follow policy.

III. Conclusion

A proactive litigation readiness program can move an organization from a reactive to a proactive stance. When controlled in a systematic, consistent fashion, the disposal of ESI in compliance with the organization's retention policy can enhance defensibility, reduce the likelihood of spoliation claims and sanctions, and save significant expense. Furthermore, better information management leads to more efficient searches for information, faster decision making, and better compliance with recordkeeping rules. In sum, litigation readiness programs that incorporate strong information governance will lead to controlled discovery costs and minimize the risks of unwelcome budget surprises.

Endnotes

1. *Fitzpatrick v. Am. Int'l Grp., Inc.*, 10 Civ. 142 (MHD) (S.D.N.Y. May 29, 2013) (footnotes and citation omitted); *QK Healthcare, Inc. v. Forest Labs., Inc.*, No. 117407/09 (Sup. Ct., N.Y. Co. May 13, 2013).
2. *See*, for example, *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 642 (S.D.Tex. 2010) (where one former employee claimed emails were destroyed pursuant to an email destruction policy at the new competing entity, the court held that, even if that was true, because any such policy was selectively implemented, the Rule 37 safe harbor would not apply).
3. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) ("*Zubulake IV*"); *Voom HD Holdings LLC v. EchoStar Satellite L.L.C.*, 93 A.D.3d 33, 36, 939 N.Y.S.2d 321, 324 (1st Dep't 2012).
4. *Voom HD Holdings*, 93 A.D.3d at 40 (citation omitted).
5. *Treppel v. Biovail Corp.*, 233 F.R.D. 363, 371 (S.D.N.Y. 2006).
6. *See, e.g., Star Direct Telecom, Inc. v. Global Crossing Bandwidth, Inc.*, No. 05-CV-6734T (W.D.N.Y. Mar. 22, 2012) (finding it unreasonable to anticipate litigation where data showed that "out of approximately 3,800 billing disputes filed during 2005 and 2006, only three customers (including the plaintiffs) commenced litigation").
7. *Field Day, LLC v. County of Suffolk*, No. 04-2202 (S.D.N.Y. Mar. 25, 2010) (rejecting the argument that a defendant's duty to preserve was triggered only when it received notice of a claim because "it receives thousands of claims a year while the percentage of notices that result in actual lawsuits is small").
8. *Toussie v. County of Suffolk*, No. CV 01-6716 (JS) (ARL) (E.D.N.Y. Dec. 21, 2007) (citing *Zubulake IV*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003)).
9. *DiStefano v. Law Offices of Barbara H. Katsos, PC*, CV 11-2893 (JS) (AKT) (E.D.N.Y. Mar. 29, 2013) (citation omitted).
10. *Siani v. State Univ. of N.Y. at Farmingdale*, No. CV09-407 (JFB) (WDW) (E.D.N.Y. Aug. 10, 2010).
11. *Id.*
12. *Byrnie v. Town of Cromwell*, 243 F.3d 93, 109 (2d Cir. 2001).
13. *FDIC v. Malik*, 09-CV-4805 (KAM) (JMA) (E.D.N.Y. Mar. 26, 2012).
14. *Id.* (noting that the defendants failed to contest this assertion).
15. *Voom HD Holdings LLC v. EchoStar Satellite L.L.C.*, 93 A.D.3d 33, 40, 939 N.Y.S.2d 321, 327 (1st Dep't 2012).
16. *Zubulake IV*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003).
17. *Id.*
18. NYSBA E-Discovery Comm., *Best Practices in E-Discovery in New York State and Federal Courts* (2011), http://www.nysba.org/AM/Template.cfm?Section=Home&Template=/CM/ContentDisplay.cfm&ContentID=58331 (hereinafter "NYSBA Best Practices").
19. The Sedona Conference, *The Sedona Conference Commentary on Proportionality* (2013), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Proportionality.
20. *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 271 F.R.D. 429, 436 (S.D.N.Y. 2010) (citation omitted).
21. Fed. R. Civ. P. 26(b)(2)(B).
22. *915 Broadway Assocs. LLC v. Paul, Hastings, Janofsky & Walker, LLP*, No. 403124/08 (Sup. Ct., N.Y. Co. Feb. 16, 2012); *see also Kravtsov v. Town of Greenburgh*, No. 10-CV-3142 (CS) (S.D.N.Y. July 9, 2012) (finding the failure to suspend the automatic deletion of video recordings at least grossly negligent).

23. *Heng Chan v. Triple 8 Palace, Inc.*, No. 03 Civ. 6048 (GEL) (JCF) (S.D.N.Y. Aug. 11, 2005); *Einstein v. 357 LLC*, No. 604199/07 (Sup. Ct., N.Y. Co. Nov. 12, 2009).
24. *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Secs.*, 685 F. Supp. 2d 456, 471, 476-77 (S.D.N.Y. 2010).
25. *Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135, 162 (2d Cir. 2012).
26. *Estee Lauder Inc. v. One Beacon Ins. Grp., LLC*, No. 602379/05 (Sup. Ct., N.Y. Co. Apr. 15, 2013).
27. *Id.*
28. *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 271 F.R.D. 429, 441 (S.D.N.Y. 2010).
29. *Id.*; *see also Steuben Foods, Inc. v. Country Gourmet Foods, LLC*, No. 08-CV-561S(F) (W.D.N.Y. Apr. 21, 2011) (finding "series of oral communications" from counsel to senior staff in a company of 400 employees sufficient to avoid sanctions).
30. NYSBA Best Practices.
31. *Id.*
32. *915 Broadway Assocs. LLC v. Paul, Hastings, Janofsky & Walker, LLP*, No. 403124/08 (Sup. Ct., N.Y. Co. Feb. 16, 2012) ("Counsel must oversee compliance with the litigation hold.").
33. *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 433-34 (S.D.N.Y. 2004).
34. *Id.*
35. *See, e.g., Tracy v. NVR, Inc.*, No. 04-CV-6541L (W.D.N.Y. Mar. 26, 2012).

Jamie Weissglass has a B.A. and M.S. from the University of Pennsylvania and received her J.D. from Fordham University School of Law. Jamie currently works as a Manager of Business Development at Huron Legal. In this capacity, she works with many Fortune 500 corporations and AmLaw 200 firms to create customized legal solutions for a variety of complex needs including litigation readiness protocols, eDiscovery and managed review services, operational restructuring, and cost-efficiency modeling.

Rossana Parrotta is a head of Strategic Sales, East Coast, at Huron Legal and she is based in New York City. She has ten years of experience in litigation discovery, managed review, database and repository management, and trial support. Her expertise is in helping clients navigate the entire electronic discovery process related to complex litigation and developing cost-saving approaches for their document review matters, which include incorporating analytical and predictive coding techniques. At Huron Legal, she provides strategic direction to law firms and corporate legal departments to support them with their legal matters. She focuses on growing Huron Legal's services across all of our offerings, helping build the Northeast market as well as the financial services and pharmaceuticals industries. She has a B.A. from Fordham University and a J.D. from CUNY School of Law.

Inside Books

Salt Sugar Fat

By Michael Moss

(Random House, 2013, 122 pages)

Reviewed by Janice Handler

This is a book about—Salt! Sugar! Fat! And if you don't believe these mundane and ubiquitous substances can be a riveting read, you don't know what a great investigative reporter Michael Moss is. Moss, a Pulitzer Prize winning *New York Times* journalist, sets out to tell us how the food companies have hooked us on three satisfying, addictive, and not-so-good-for-you ingredients. Yet he doesn't make the companies sound all that evil (unlike their tobacco counterparts). He makes us all—the consumer, the companies, the regulators—out to be victims of a vicious cycle that we have been trapped in**. Disclaimer**: I worked many years for Unilever, one of the companies discussed in this book.

Moss begins by documenting a meeting that took place amongst food company honchos in April, 1999, where a vice president of Kraft argued that the food industry should get ahead of the obesity epidemic—and the regulators and trial lawyers—by acknowledging the role played by packaged food and drinks in over consumption, and then pull back on their use of salt, sugar and fat. He was immediately up against a wall—these ingredients, after all, are those that create the greatest allure for the industry's products. The 114 slides presented by the Kraft executive were of little value when the head of General Foods took the stage and said, "Don't talk to me about nutrition. Talk to me about taste, and if this stuff tastes better, don't run around selling stuff that doesn't taste good." End of meeting, end of initiative! Said another industry participant "(W)e're not going to screw around with the company jewels here and change the formulations because a bunch of guys in white coats are worried about obesity."

According to Moss the guys in white coats have a lot to worry about. Every year Americans eat over 33 pounds of cheese (triple the consumption in 1970) and 70 pounds of sugar. We ingest 8500 mgs of salt, most of it coming from processed foods. One in three adults and one in five children are clinically obese. Twenty-six million Americans have diabetes. Combining hard facts, industry history, and fascinating anecdotes and "people" stories, Moss tells us how we got here.

He tells us about the food chemists who spend untold hours calculating the "bliss points" (optimum concentration of sugar or fat at which sensory pleasure is maximal) of foods.

He tells us about the marketing campaigns developed from the ruthless competition of the Coke-Pepsi wars and drawing on the take-no-prisoners tactics of the tobacco marketers (at least one of which, Philip Morris, got into the food business with its takeover of Kraft / General Foods).

He tells compelling personal stories of industry executives, past and present, who developed the products and marketing campaigns we grew up with. He tells of Jeffrey Dunn, a Coca Cola executive, whose father had worked at Coke and who had always wanted to work there. After arriving at the upper ranks of management, Dunn left the company after observing its marketing efforts in impoverished areas of Brazil. "These people need a lot of things, but they don't need a Coke," he thought. Dunn now works for a company that markets carrots. Dean Southworth was the food scientist at Kraft who invented Cheez Whiz. After retirement, he sampled the latest version of the product, which seemed devoid of cheese. "You are putting out a goddamn axle grease," he complained to Kraft.

Moss reveals secrets that the industry would not particularly want you to know—such as what a lower sugar or salt claim really means (it means they've raised one of the other three ingredients to compensate) or how expensive ingredients are removed to save money (think Cheez Whiz with no cheese).

Yet the industry is not depicted as an uncomplicated villain. Although Ron Suskind says on the back jacket that the book is about a "processed food industry that's making a fortune by slowly poisoning an unwitting population," I found the accountabilities less simplistic than that. In part, the food and beverage industry is also a victim of its own marketing success. If the public wanted carrots, they'd give us carrots. As an ex CEO of Philip Morris put it: "People could point to these things and say 'they've got too much sugar, they've got too much salt'…. Well, that's what the consumer wants and we're not putting a gun to their head to eat it…if we give them less, they'll buy less, and the competitor will get our market.

So you're sort of trapped." Even the author admits that a salt-free version of Cheez Its("which normally I can keep eating forever") "felt like straw, chewed like cardboard, and had zero taste."

Unfortunately this highly readable and well researched book is longer on problems than solutions. After comprehensively describing the vicious circle we find ourselves in, Moss summarizes prescriptions (such as they are) in his last chapter, "We're Hooked on Inexpensive Food." He gives up quickly on any notion that the food industry will be leaders in finding a solution. He tells of checking out claims that Nestle® (the largest food manufacturer in the world, described as so rich it is a "Swiss bank that prints food") was doing innovative work in nutritional science, only to find its results disappointing. "The food that people bought in the grocery store was so perfectly engineered to promote over consumption that Nestlé's scientists…were finding it impossible to come up with viable solutions." While the company did take steps to reduce sugar, fat, and salt across its portfolio, Moss concludes it is not the World Health Organization—just a company doing what companies do, making money. Moss believes that the deep dependence the food industry has on sugar, salt, and fat compels even the best companies to produce foods that undermine a healthy diet. Nor, says Moss, will the regulators save us from ourselves. Most regulatory initiatives do not seem reasonable or terribly smart. Finally, the economics are against us—it costs more money to eat healthier, fresher foods than cheap processed foods.

The best Moss offers are some tricks (some taken from Overeaters Anonymous and its like) to avoid marketing tactics companies pursue to draw us in. Seizing control to ward off unhealthy dependence on processed food is the best we can do, he tells us sadly. "Only we can save us," he says. "After all, we decide what to buy. We decide how much to eat.

Corporate Counsel Section Committee Chairpersons

CLE and Meetings
Steven G. Nachimson
Compass Group U.S.A, Inc.
3 International Drive, 2nd Fl.
Rye Brook, NY 10573
steven.nachimson@compass-usa.com

Anne S. Atkinson
Pryor Cashman LLP
7 Times Square
New York, NY 10036-6569
aatkinson@pryorcashman.com

Diversity
Thomas A. Reed
1172 Park Ave., Ste. 15-c
New York, NY 10128
tomreed2@me.com

INSIDE/Publications
Allison B. Tomlinson
Gensler
1230 Avenue of the Americas, Ste. 1500
New York, NY 10020
allison_tomlinson@gensler.com

Janice Handler
handlerj@aol.com

Kenneth G. Standard Diversity Internship Program
David S. Rothenberg
Goldman Sachs
200 West Street, 40th Fl.
New York, NY 10282
david.rothenberg@gs.com

Membership
Joy D. Echer
Foot Locker, Inc.
Law Department
112 West 34th Street
New York, NY 10120
jecher@footlocker.com

Thomas A. Reed
1172 Park Ave., Ste. 15-c
New York, NY 10128
tomreed2@me.com

Pro Bono
Cynthia Beagles
The American Kennel Club, Inc.
260 Madison Avenue
New York, NY 10016
ccb@akc.org

Technology and New Media
Fawn M. Horvath
Macy's, Inc.
11 Penn Plaza, 11th Fl.
New York, NY 10001
fawn.horvath@macys.com

Natalie Sulimani
Sulimani Law Firm
116 West 23rd Street, Ste. 500
New York, NY 10011
natalie@sulimanilawfirm.com

NEW YORK STATE BAR ASSOCIATION
CORPORATE COUNSEL SECTION
One Elk Street, Albany, New York 12207-1002

ADDRESS SERVICE REQUESTED

NON PROFIT ORG.
U.S. POSTAGE
PAID
ALBANY, N.Y.
PERMIT NO. 155

Inside is a publication of the Corporate Counsel Section of the New York State Bar Association. Members of the Section receive a subscription to the publication without charge. Each article in this publication represents the author's viewpoint and not that of the Editors, Section Officers or Section. The accuracy of the sources used and the cases, statutes, rules, legislation and other references cited is the responsibility of the respective authors.

Accommodations for Persons with Disabilities:
NYSBA welcomes participation by individuals with disabilities. NYSBA is committed to complying with all applicable laws that prohibit discrimination against individuals on the basis of disability in the full and equal enjoyment of its goods, services, programs, activities, facilities, privileges, advantages, or accommodations. To request auxiliary aids or services or if you have any questions regarding accessibility, please contact the Bar Center at (518) 463-3200.

ISSN 0736-0150 (print) 1933-8597 (online)

Inside

Section Officers

Chairperson
Howard S. Shafer
Shafer Glazer LLP
90 John Street, Ste. 701
New York, NY 10038-3202
hshafer@shaferglazer.com

Chairperson-Elect
Thomas A. Reed
1172 Park Avenue, Ste. 15-c
New York, NY 10128
tomreed2@me.com

Vice-Chairperson
Joy D. Echer
Foot Locker, Inc.
Law Department
112 West 34th Street
New York, NY 10120
jecher@footlocker.com

Secretary
Yamicha Stephenson
PO Box 1444
Morningside Station
New York, NY 10026
yamicha.stephenson@gmail.com

Treasurer and Vice-Chairperson
Jeffrey P. Laner
77-10 34th Avenue
Jackson Heights, NY 11372
jlaneresq@nyc.rr.com