INFORMATION LAW JOURNAL

A Publication of the Information Security and EDDE Committees
ABA Section of Science & Technology Law

SPRING 2015 VOLUME 6 ISSUE 2 EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.

California Data Breach Law – Rounding the Bases

By Jill Bronfman

On September 30, California attempted to step up to the plate and update its data breach privacy regulations with AB 1710. The amended portions of the law took effect January 1, 2015. The law attempts to capture existing industry practices, but commits an error or two in aligning law and technology. The amended law now requires (1) for data breach notifications, if the person or business providing the notification was the source of the breach, that the person or business offer to *Read more*

The Florida Information Protection Act and HIPAA: Practical Considerations for Regulated Entities

By Aldo M. Leiva

In 2013, when the Health Insurance Portability and Accountability Act of 1997 ("HIPAA") was revised by the HIPAA Omnibus Rule, both Covered Entities (consisting primarily of health care providers) and Business Associates (service providers to such entities) were required to update their policies, practices, and applicable contracts (i.e. Business Associate Agreements) to comply with new requirements. For such entities located in Florida (or creating, acquiring, maintaining, *Read more*

Privacy – Some Short Considerations about the Evolution of Brazilian Law

By Renato Opice Blum

Reports in international communication channels have frequently commented that the relationship between Brazilians and the internet has always been considered one of the more complex topics of conversation inside the country. The naturally sociable nature of its population and its taste for social networking has lead, in recent years, to a rise in legal issues relating to privacy and the protection of data facing legal professionals. The initial lack of attention and cautious treatment *Read more*

Right to Privacy in the Information Age: Four Lawyers Discuss If It Still Exists

By Christina M. Jeter

The right to privacy is something that many individuals hold dear. However, living in the Information Age creates unique situations which may very well test what a person deems to be "privacy." We are beyond eavesdropping as presented in *Lopez v. United States*, and even thermal imaging of walls being unconstitutional, as in *Kyllo v. United States*. Technology has advanced in ways some could have only imagined as children watching the *Jetsons* where George Jetson, *Read more*

Predictive Coding: No Longer An All-Or-Nothing Proposition

By Alex Kiles, Alexander B. Hastings and Edward H. Rippey

In recent years, predictive coding has steadily gained traction in the e-discovery landscape -- yet, many lawyers and clients remain reluctant to harness the technology's full potential. This article aims to demonstrate that predictive coding need not be an all-or-nothing enterprise. Rather, the future of e-discovery lies in leveraging technology, including predictive coding, to enhance some aspect of every case. The threshold question should not be, "Should I use predictive coding?" *Read more*

Are You a Risk to Your Own Firm or Business?

By David Willson

Despite all of the bad news and negativity in the world, most of us have a very positive or even inflated opinion of ourselves. How many people believe they are ugly, bad drivers, or disliked by others? Very few. As the owner or partner of a law firm or business-owner, you may be one of the greatest risks to your own organization. Many successful business leaders are type-A personality, extremely sure of themselves and believe their manner of doing business is better than the next guy *Read more*

California Data Breach Law – Rounding the Bases

By Jill Bronfman

On September 30, California attempted to step up to the plate and update its data breach privacy regulations with AB 1710.[1] *The amended portions of the law took effect January 1, 2015. The law attempts to capture existing industry practices, but commits an error or two in aligning law and technology.*

The amended law now requires (1) for data breach notifications, if the person or business providing the notification was the source of the breach, that the person or business offer to provide appropriate identity theft prevention and mitigation services, *if any* [italics added], to the affected person at no cost for not less than 12 months if the breach exposed or may have exposed specified personal information, (2) that companies who maintain data, in addition to those that own or license the data, now protect the data, and (3) in addition to restrictions on disclosure of social security numbers, except as specified, prohibit the sale, advertisement for sale, or offer to sell of an individual's social security number.

Bill AB 1710 ventures into de jure territory that we've seen de facto in that it suggests identity protection services for private citizens victimized by data breaches. Target,[2] for example, offered these services early in 2014 after its own data breach. Target offered 12 months of free protection via outside vendor Experian, and the new amendment to California's data breach law in AB 1710 specifies one year as a minimum. Yet a failure to make this requirement unambiguous leaves the law closer to a set of industry standards than an outright legal mandate.

The twinning of law and business practices has several interesting consequences. This is not to say that looking at existing business practices before establishing arbitrary and ideal rules is specious. The practical implications of the law can be thought of as a series of base hits rather than a triumphant "home run."

So who's on first?

The law shifts the burden of protecting personal information from data owners, who may be individuals or any category of business, to data storage companies. Companies who "maintain" this information are on the hook for identity protection services if a breach occurs, and for a host of other restrictions regarding selling SSNs and protecting personal information. In some sense, it may be easier

[1] The text of the bill is available at: http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710
[2] Data breach management offered at: https://corporate.target.com/discover/article/free-credit-monitoring-and-identity-theft-protecti

to ascertain who holds the information if the law proffers a virtual strict liability standard. If the information was exposed (or more ambiguously "may" have been exposed) from a company's database, then it could be on first for liability. Under the old standard, determining legal ownership of the data would have required, in many cases, analysis of contractual obligations and licensing trails.

On the negative side, maintenance of data may be fleeting and difficult to track as well. The term "maintain" sounds rather permanent and substantial, but is an awkward graft onto the practices for transmitting electronic information. Data can be stored in data centers for any length of time, but also, more likely so, exists in transit at any given time. Can anyone who has data on an individual computer or system be liable? The law itself does not parse the term or give it a technical definition that would allow engineers to create an information protection system to comply with the law. The definition provided by the new law is both tautological and defines maintain as not own or use.[3]

The law also does not separate liability for metadata, envelope information, and quantity of data from responsibility for content. There's a multi-variable thread in legal history of exempting content providers from liability in the telecom and Internet fields.[4]

And what's on second?

The legal field will be looking for court cases and/or enforcement actions to clarify the parameters of the law around "free," "offer," and types of identity protection services. Similarly, businesses who will need to adjust to the requirements are not only the companies who may suffer breaches, but also the companies that offer identity protection services. These companies will be in the second round of responsibility for action as well as research and development as a result of AB 1710. Various lines of identity protection services, and interface, consulting, and notification services, may arise in the wake of the changes in the law. Certainly, we'd at least see a rise in the availability and use of yearlong contracts for identity protection services, but a variety of other products and services may become available as well. Laws may create or change opportunities in markets, increasing some business opportunities while limiting others.

Third base: Data Collection Practices and Insurance Calculations

The law is clearer in the enumeration of the types of personal information deemed worthy of protection, including the affected individual's name and SSN, driver's license number or California identification card number. Per the usual U.S. bias, there's nexus between individual identity and government status as limited to the items enumerated above, financial account access, and medical information. Therefore, this law is not aimed at increasing or modifying healthcare or

[3] "The term "maintain" includes personal information that a business maintains but does not own or license." CAL. CIV. CODE 1798.81.5.

[4] See, e.g. Digital Millennium Copyright Act, http://www.gpo.gov/fdsys/pkg/BILLS-105hr2281enr/pdf/BILLS-105hr2281enr.pdf

financial regulations, or even targeting particular industries. It does, however, provide incentives to avoid collecting the specified information if there is no business necessity for doing so. In this element alone, the law may have far-reaching consequences for businesses that routinely collect myriad data elements about individuals without a present intention to use such data as part of a coherent business plan. Businesses may have considered collecting these categories of information incidentally, accidentally, or even intentionally with the thought that there would be no incremental cost and the business could evaluate its value at a later date. If the law results in loading additional costs to the side of the equation that validates indiscriminate data acquisition, we might have just an incremental benefit to individual privacy.

As is common in the U.S. system of independent state and federal regulation, the tide of compliance rises unevenly. Now that there may be a more definitive quantifiable cost associated with the disclosure of these categories of personal information in California, the cost can be weighed against the benefit (perhaps none in many business models) of collecting and retaining this information. Companies collecting personal information nationally or internationally may need to conduct this cost-benefit analysis as follows: California-specific risk (cost of cover x statistical likelihood of breach) versus wider-region benefit to the business.

Determining which jurisdiction's law offers "greater protection to personal information" may result in a burgeoning batch of case law comparing states' and vertical-specific regulations. Determining the technical parameters of each law, such as when a data record may have been exposed, and to whom, could boost consultancies and other third party vendors in the detection and notification space.

Home Base

What does the law mean for voluntary and involuntary offering of personal data by individuals? In the realm of free speech law, there is a well-known argument that laws infringing upon speech, even without effective enforcement, may reduce speech. Individuals may, on average, conform to societal norms in their speech even without the explicit prohibition of the law. In the case of the threat of data breach, some people, or the average person, may be willing to offer less in quantity, quality, or frequency of personal information due to the possibility of the information being disclosed to the public. In the course of preparing this article, several new data breaches have been covered in the media,[5] and several more may arise in the interval between drafting and publication.

So what is the effect of the new law? There may be a chilling effect due to news coverage of the law and growing public awareness of data breaches. However, there is a viable argument to be made that while the new amendments place a heavier financial burden on more companies to protect the information they maintain, to provide identity theft protection to data breach victims, and to

[5] As of this writing, http://www.bloomberg.com/news/print/2015-01-05/morgan-stanley-fires-employee-accused-of-stealing-client-data.html.

comply with restrictions on the use of SSN lists for financial gain, customers may in fact be *more* likely to reveal such information to companies under the new protective regime. Will this result in an overall enhancement and protection of individual privacy? Yes and no. As a result of this increased confidence in the data protection system, companies may be able to collect broader categories of information and gain far more value overall than before the new restrictions came to the ballpark. The law is new, and we will have to wait to see how businesses and individuals react, and how the courts interpret any cases under the new law brought before them. In both cases, the standard of play is enhanced overall.

Jillisa (Jill) Bronfman *is Program Director of the Privacy and Technology Project at the Institute for Innovation Law and Adjunct Professor of Law in Data Privacy at UC Hastings College of the Law. She was named to The Recorder's 2014 list of the 50 Women Leaders in Tech Law. The honorees were chosen by editors of The Recorder based on their recent accomplishments and because they've demonstrated the ability to lead. These are the women who lead litigation and deals; who lead in-house teams and firm practice groups; who are thought leaders; and who lead the way for other women seeking roles in the region's most dynamic sector. Also, Jill was selected as a 2014-2015 USC Annenberg Alumni Ambassador. Jill formerly was an Assistant General Counsel and Network Security and Privacy Subject Matter Expert for Verizon in the San Francisco office. At Verizon, she designed and moderated several in-house training programs in data security, compliance, and intellectual property.*

She also taught at San Francisco State University, including developing a new advanced seminar in Mobile Communications. At the National Association of Broadcasters/ Broadcast Educators' Association Conference (NAB/BEA) in Las Vegas, she presented "Mobile Communications 2014: What's After What's Next." In this presentation, she drew on her research in the field of privacy and technology to speak about the latest issues in drone regulation and the legal implications of 3D printing. Jill received a joint degree at USC in Law and Communications Management (JD/MA) and a dual undergraduate degree at UC Berkeley in Mass Communications and History. Her thesis addressed the interrelationship of science fiction set in the future and technology development. In April 2014, Jill was selected to workshop her technology-driven fiction at a juried literary conference, and in October 2014, she read her work at LitQuake, San Francisco's renowned celebration of writers and writing.

The Florida Information Protection Act and HIPAA: Practical Considerations for Regulated Entities

Aldo M. Leiva

In 2013, when the Health Insurance Portability and Accountability Act of 1997 ("HIPAA") was revised by the HIPAA Omnibus Rule, both Covered Entities (consisting primarily of health care providers) and Business Associates (service providers to such entities) were required to update their policies, practices, and applicable contracts (i.e. Business Associate Agreements) to comply with new requirements. For such entities located in Florida (or creating, acquiring, maintaining, or otherwise using protected health information of Florida residents, even if such entities were located outside of Florida), however, the enactment of the Florida Information Protection Act ("FIPA") in 2014 requires that an additional level of compliance considerations be analyzed. This article provides a summary of FIPA, and analyzes potential practical effects on health care providers (and their service providers) both in and outside the State of Florida, as well as providing FIPA practice considerations for counsel.

On June 20, 2014, FIPA was signed into law by Governor Rick Scott and the law went into effect on July 1, 2014. Enactment of FIPA served to repeal Florida's earlier data breach notification statute, Fla. Stat. § 817.5681, which had been enacted in 2005, and replaced it with Fla. Stat. § 501.171. Florida's modification of its data breach notification regime is part of a national trend among state legislatures to update data breach and data security laws, in response to well-publicized data breaches that have impacted millions of Americans in recent years.

FIPA sets forth definitions that serve to identify individuals and entities that are subject to this law, as well as the type of information that is subject to the law, triggering practical compliance considerations for any individuals or entities conducting business activities that include maintenance or use of personal data of Florida citizens or residents. While Florida's prior breach notification law was limited in application to entities that conducted business within Florida,[1] FIPA applies to entities that use personal data that is provided by individuals in Florida to such regulated entity. FIPA therefore applies to any commercial entity, even if locate in another state and even another country, provided that a Florida citizen or resident has provided such personal information to that entity. Once such entities are provided with or entrusted with personal information of Florida citizens or residents, they are now required to comply with FIPA in the event of a data breach as well as being required to proactively adopt "reasonable security measures" to protect such data, as further explained below.

[1] Fla. Stat. § 817.5681(1)(a) (2014).

FIPA expands upon the compliance obligations of "covered entities" that acquire, maintain, store, or use data containing "personal information" that has been "provided by an individual in this state to a covered entity for the purpose of purchasing or leasing a product or obtaining a service."[2] Although the term "covered entity" is also included in HIPAA, the meaning of the term under FIPA is much more expansive, as it is not exclusively limited to health care providers or other similar entities as defined under HIPAA.[3] Instead, FIPA's version of a "covered entity" includes any business or government entity[4] that collects or uses "personal information," which is defined as either, (A) an individual's first name or first initial, and last name in combination with any one or more of the following identifying elements:

(1) social security number;
(2) driver's license number, identification card number, passport number, military ID number, or other similar number issued on a government document used to verify identity;
(3) financial account number, such as credit or debit card number, in combination with any security code or password required for access to the account;[5]
(4) ANY information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
(5) Health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;[6] OR

(B) a user name or email address in combination with a password or security question and answer that would permit access to an online account.[7]

It is very important to note, however, that the term "personal information" does NOT include either information that has already been made publicly available by a federal, state, or local government entity, OR information that is encrypted, secured, or modified by any other method or technology that removes elements that will identify the individual or will otherwise render the information unusable.[8] FIPA therefore creates an incentive for regulated entities to encrypt personal information in order to avoid the compliance burdens under this statute.

As applied to those "covered entities" that are already subject to HIPAA regulations, FIPA's revised definition of "personal information" is now expanded to include health care information, subject to the

[2] Fla. Stat § 501.171(1)(c) (2014).
[3] 45 CFR § 160.103 (2014) defines "covered entity" as any of the following: (1) a health plan; (2) a health care clearinghouse; *or* (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
[4] Fla. Stat § 501.171(1)(b).
[5] These definitions were included in the prior data breach notification statute.
[6] FIPA expands upon the prior data breach notification statute by adding these two new categories of personal information that relate to health care. *See* Fla. Stat § 501.171(1)(g)(1)(a)(IV) and (V).
[7] Fla. Stat § 501.171(1)(g)(1)(b).
[8] Fla. Stat § 501.171(2).

language that limits the application of FIPA to unencrypted or de-identified information. Healthcare providers that are already considered to be "covered entities" under the HIPAA definition are therefore not subject to FIPA if (and only if) the patient information is encrypted or de-identified. However, those HIPAA "covered entities" that do not encrypt such data, but who experience a data breach of unencrypted data will be required to comply with the FIPA notice requirements, in addition to any notice requirements under the HIPAA Omnibus Rule.

FIPA establishes new notification requirements in the event of a breach of personal information. Under the earlier statute, breaches of personal information had to be reported to affected individuals within 45 days from the time the breach was discovered.[9] FIPA reduces the notification period to affected individuals to 30 days, although such notification may be delayed upon written request of law enforcement authorities, if they determine that such notification would interfere with a pending criminal investigation.[10]

FIPA states that data breach notification issued by a covered entity in compliance with its "primary or functional federal regulator" will be deemed to be in compliance with FIPA's notice requirement.[11] However, as applied to an entity subject to HIPAA regulation, this FIPA provision creates an ambiguity in compliance considerations. HIPAA requires that a covered entity provide breach notification "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach.[12] However, FIPA imposes a strict limit of 30 days for notice following discovery of the breach; therefore, it is as yet unknown whether a covered entity that notifies affected patients after the 30 day period, but achieves notification prior to HIPAA's 60 day time limit, will be able to avail itself of FIPA's "functional federal regulator" compliance language to retroactively demonstrate compliance with FIPA. Further, to add further uncertainty and ambiguity for HIPAA-regulated entities, FIPA requires that a covered entity "timely" provide a copy of the notice it has issued pursuant to applicable federal requirements, in order to be deemed to be in compliance with FIPA's notice requirements; the question arises as to whether "timeliness" will be limited to the 30 days required under FIPA.

In practice, notification within FIPA's 30 day period will satisfy HIPAA notification requirements, provided other HIPAA notification requirements are also met. Therefore, in order to ensure proper notification under both FIPA and HIPAA, an independent analysis of notification requirements (and content of same) should be performed under each statute by counsel for the regulated entity.

FIPA also requires that a covered entity notify each individual "in this state" whose personal information was or is believed to have been accessed as a result of a breach, no later than 30 days after determination of a breach or reason to believe a breach occurred. Based on this statutory

[9] Fla. Stat. § 817.5681(1)(a).
[10] Fla. Stat § 501.171(4)(a) – (c).
[11] Fla. Stat § 501.171(4)(g).
[12] 44 CFR § 164.404(b).

language, it appears that FIPA does not require notification of affected individuals who have left Florida as of the time of notification.

If the breach affects 500 or more individuals, FIPA provides that the covered entity must now also notify the Florida Department of Legal Affairs no later than 30 days after determination of the breach or reason to believe a breach occurred, although an additional period of up to 15 days may be granted for good cause, if so authorized by the Florida Department of Legal Affairs.[13] If more than 1,000 individuals are affected by the breach, the covered entity must also notify credit reporting agencies "without unreasonable delay."[14]

Despite FIPA's notification requirement to affected individuals, however, no such notification is required if, after appropriate investigation and consultation with the relevant law enforcement authorities, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or financial harm to affected individuals.[15] Any such determination must be in writing and must be submitted to the Florida Department of Legal Affairs within 30 days after the determination, and must be maintained for a period of at least five years after the breach.[16] Counsel advising HIPAA covered entities should note that while the above "risk of harm" analysis is applicable within the FIPA compliance context, HIPAA itself no longer applies the "risk of harm" standard and instead, as of enactment of the HIPAA Omnibus Rule in 2013, now emphasizes a "risk of breach to the information" analysis when assessing notification.[17] In practice, a data breach affective Florida citizens/residents will therefore trigger independent analysis on the issue of notification under each statute (HIPAA and FIPA), pursuant to the differing standards under each statute.

FIPA also imposes new requirements in situations where covered entities are notified of a data breach by third party agents that maintain, store or process personal information for a covered entity or governmental entity.[18] As provided for in the prior statute, such third party agents have no more than 10 days after a data breach to notify the covered entity on whose behalf personal information was maintained.[19] However, FIPA now requires that the notified covered entity provide notification to affected individuals within 30 days of such notification by the third party agent,[20] in contrast to the imprecise requirement in the prior statute, which provided discretion to the covered entity and third party agent to agree on notification or, failing such agreement, imposed notification requirements on whichever person that had the direct business relationship with the affected Florida state resident(s).[21]

---

[13] Fla. Stat § 501.171(3).
[14] Fla. Stat § 501.171(5).
[15] Fla. Stat § 501.171(4)(c).
[16] *Id.*
[17] 44 CFR 164.402(2)(i-iv).
[18] Fla. Stat § 501.171(6)(a).
[19] *Id.*
[20] *Id.*
[21] Fla. Stat. § 817.5681(2)(a).

This new FIPA requirement also contrasts with the 60 day notice period that applies under HIPAA, and may be used by counsel for covered entities in Florida to insist on a shorter notice period in contracts with third party agents (i.e. business associate agreements).

In addition to revised breach notification requirements, FIPA now requires that any covered entity, governmental entity, or third party agent that electronically stores regulated personal information "take reasonable measures to protect and secure data."[22] FIPA does not define the specific measures that are deemed to be "reasonable," presumably due to evolving and emerging security threats to such data. In fact, by providing such broad language as to data security measures, FIPA essentially requires regulated entities to avail themselves of emerging data security threats and to regularly conduct risk assessments of their data storage systems to identify new vulnerabilities.

FIPA now also requires covered entities and third party agents to take "all reasonable measures" to dispose of records that are no longer to be retained (except, of course, any records subject to an express or implied litigation).[23] Such measures will include shredding, erasing, or otherwise rendering the records unreadable or undecipherable.[24]

Like HIPAA, FIPA does not create a private cause of action and it is enforceable only by the Florida Department of Legal Affairs, which may deem any FIPA violations as an unfair or deceptive trade practice, and may lead to imposition of civil penalties as follows: (1) $1,000 per day for the first 30 days, (2) $50,000 for each subsequent 30 day period (up to 180 days), and (3) up to a maximum of $500,000 for any violation. Notably, these civil penalties apply per breach and not per individual affected by the breach.[25]

In summary, entities should confirm whether they have acquired, use or maintain unencrypted personal information of Florida citizens or residents, whether or not such entities do business within the state of Florida. If the analysis confirms that FIPA applies, such entities should consider identifying and implementing "reasonable measures" to secure personal information and should also adopt "reasonable measures" to dispose of such information as appropriate under applicable law. In doing so, policies and procedures reflecting FIPA notification requirements and timelines should be implemented. Lastly, HIPAA covered entities also subject to FIPA may consult with counsel to advise on whether to consider adhering to the 30 day FIPA breach notification deadline (as opposed to the 60 day HIPAA breach notification deadline), and should similarly consider whether third party agents/business associates should be required to adhere to the 30 day FIPA breach notification deadline as well.

---

[22] Fla. Stat § 501.171(2).
[23] Fla. Stat § 501.171(8).
[24] *Id.*
[25] Fla. Stat § 501.171(9).

Aldo M. Leiva, Esq. *is Chair of Data Security and Privacy Practice of Lubell Rosen, in Miami, Florida, and advises domestic and international clients on data protection issues, cybersecurity, and privacy laws. He can be reached via email at aml@lubellrosen.com or at (305) 442-9045.*

Privacy – Some Short Considerations about the Evolution of Brazilian Law

By Renato Opice Blum

Reports in international communication channels have frequently commented that the relationship between Brazilians and the internet has always been considered one of the more complex topics of conversation inside the country. The naturally sociable nature of its population and its taste for social networking has lead, in recent years, to a rise in legal issues relating to privacy and the protection of data facing legal professionals.

The initial lack of attention and cautious treatment by companies regarding data retention, for example, led to there being many cases of obtaining and misusing of information, especially in consumer relations. Large Corporations were compelled in the wake of several cases of credit card and banking transaction fraud to invest heavily in information security, something which has undeniably brought positive change.

However, in people´s private lives, largely as a result of misinformation on the part of the majority of users regarding minimum safety practices, undesirable events continued to happen intermittently. Invasion of personal devices, improper posting of content, etc., continued to be an everyday reality. To make matters worse, there was little in the Brazilian legislation that was effective in preventing or to punish such reprehensible practices

For this reason it became clear that there would need to be revision of existing legislation to take into account the new legal pressures that were arising and thus more effectively prevent malpractice. There had been widespread public outcry, demanding that the Brazilian legislature revisit old laws to make necessary adjustments and where required create new rules to abate the people´s concerns.

In criminal law, although the Brazilian Penal Code (Decree Law 2.848 / 1940) already contained applicable provisions, it was considered necessary for a specific provision to be inserted into this statute to punish the violation of computing devices belonging to others and the divulging of any content therein, this was achieved through the passing of Law 12.737/2012.

Consequently, it is now a crime in Brazil to access computers or other electronic devices without authorization. The penalties for such conduct are increased should the invasion result in economic loss or where there is disclosure, trade or transfer to a third party, for any reason, the data or information. Additionally, the penalty will also be greater in the event that the crime is committed against a public authority.

It is necessary to point out, however, that prior to the adoption of this legislation, the national legal system had already foreseen the need to deal with the disclosure of confidential information from the Government. Law 7.170 / 1983, for example, deals specifically with cases of conduct prejudicial to national security, such as the leaking of sensitive public data. This concern clearly did not appear from nowhere, in fact it sourced from news of alleged international electronic spying activity.

Concerned about this emerging situation and recognizing that the existing rules were insufficient to curb these practices, the Brazilian Federal Government once again turned to the legislature, requesting that they carry out a series of studies and approve other adjustments to protect the privacy and confidentiality of data. All of these innovations were to be consolidated in what would become known as the ¨Marco Civil da Internet¨ or the Internet Legal Framework.

In relation to consumer protection it should be noted that prior to the aforementioned adjustments and studies there were already specific rules in place provided by the Consumer Protection Code (Law. 8078/1990). This law requires all suppliers of products and services, including those online, to provide clear information to its customers and mechanisms to reimburse them where products are faulty or damaged. The issue of e-commerce and its specific demands were dealt with in 2013 decree 7.962 which introduced rules regarding the effectiveness of communication on the web with a requirement to display contracts and to facilitate customer service channels amongst other things. In addition the decree also demanded that suppliers use secure mechanisms for the processing of payments and for the treatment of customer data online.

In 2014, after considerable debate, the legislature approved law 12.965, the birth of the Internet Legal Framework. Among the relevant topics covered in this law was that of net neutrality, the period of time required for the storage of logs and of course the introduction of provisions in respect of the protection of data privacy. While one cannot dispute that the new statute contains controversial measures, the text does clearly underline the importance of concepts such as the freedom of expression, civil liability for damages and seeking the protection of privacy as being the basis for complying with the Brazilian constitutional principle of human dignity.

It is worth noting that the text adopted also emphasized the importance of preparing citizens for the safe and responsible use of the internet, protecting against undesirable practices. In addition it also provides that personal data cannot be passed to third parties without free and informed consent by the subject of the data. The statute also gives users the right to apply for the permanent deletion of their data at the end of the relationship between the parties and also considers void any contractual clauses that might result in harm to privacy or the freedom of expression.

Under this legislation data logs may only be made available by way of a court order, however public authorities may access such user information by following a procedure prescribed by the law. It should be emphasized that the law expressly and unequivocally determined that connection or internet

application providers, even if they are legal entities based abroad, must comply with Brazilian internet laws and regulations, when offering services to the Brazilian public or where at least one member of the same economic group has property in Brazil.

Also, the Internet Legal Framework requires that the records of internet applications be maintained confidentially by companies engaged in these activities in a professional manner for a period of at least six months to be made available upon receipt of a court order.

Thus it appeared that the Brazilian legal rules on privacy and data protection had arrived at near completion. However, considering that the Brazilian legal system is founded on the principle of legality (only that which the law requires), experts realized that there was considerable work to be done detailing exactly what protection the new laws really provided.

Even before the Internet Legal Framework was approved, the Federal Government itself, through its Ministry of Justice, had already proposed the drafting of a detailed opinion regarding the protection of personal data, and that this analysis (based on European directives) result in the presentation of a bill to the legislature. These studies, not yet completed and with no deadline for completion, in summary, suggest rules for database maintenance, information sharing, the assumption of confidentiality, as well as the possibility of accountability in cases of disagreement.

To complement this, the Government's proposal considers the idea of creating a kind of "code of practice". According to reports, it is suggested that private sector knowledge, already put in place by the main market players, should not neglected and could be used for attaching additional measures to the text of the law, dealing with technical standards and assisting with continuous updating.

Despite the preparation of this draft by the Government, the legislature has also moved forward with discussions regarding this issue. The Brazilian political system is composed of two houses of debate and revision, which consider a wide variety of proposals. We cite here Project No 181/2014 that originated in the Senate, and Project No 4060/2012 that came from the House of Representatives.

Curiously the Senate project cited above is intended, amongst other things, to ensure that no one can be excluded, damaged or in any way affected by decisions based on automated data analysis aimed at reviewing your profile. Already bill 4060/2012 discussed in the House of Representatives sought to establish that those responsible for databases in Brazil start to adopt, forcefully, data protection measures that are proportionate with, the current state of technology, the nature of the data and the specific characteristics of the treatment, in particular when processing sensitive data.

Two other bills worthy of mention include the PL No 3558/12 (House of Representatives) which deals with the use of biometric systems in the context of personal data protection and defines the crime of modifying data in information systems and also PL No.330/13 (Senate) which covers the establishment of rules for all levels of database managers.

All of these continuing projects are passing through bureaucratic procedures, which include the possibility of discussion at public hearings (with the participation of the general public). Each has a long way to go yet and, most likely, there will be changes in their texts before approval.

Thus it is clear that Brazil now possesses an abundance of legal regulation to address issues relating to the internet, in particular, the rights and guarantees of users. However, as in other nations, some rules will need adjustment to be improved, there will also be a ongoing need to monitor and update to ensure continued satisfactory implementation.

Thus, the science of law, not only in Brazil, as with anywhere in the world, now has the challenge of being as fast, efficient, practical and versatile as the universe offered by the Internet. The question is: can we meet this challenge, or always be one step behind?

***Renato Opice Blum**, MSc, attorney and economist**;** Vice-Chair of the Privacy, E-Commerce and Data Security Committee of American Bar Association Section of International Law. Recognized professional for 02 consecutive years in Chambers & Partners, Who's who and Best Lawyers; Invited speaker in several international conferences (EUROFORUM, LegalTech, SEDONA, ITECHLAW, HTCIA, ISSA, IAPP, Georgetown Law, etc.); Co-author of the article "Recent Development on Cyberspace Law: A View from Brazil" (THE BUSINESS LAWYER - American Bar Association – 2013), "Brazilian's Chapter" of Data Protection & Privacy Law (2nd Edition, European Lawyer - Thomson Reuters). @opiceblum; www.opiceblum.com.br*

Right to Privacy in the Information Age: Four Lawyers Discuss If It Still Exists

By Christina M. Jeter

The right to privacy is something that many individuals hold dear. However, living in the Information Age creates unique situations which may very well test what a person deems to be "privacy." We are beyond eavesdropping as presented in Lopez v. United States,[1] *and even thermal imaging of walls being unconstitutional, as in* Kyllo v. United States.[2] *Technology has advanced in ways some could have only imagined as children watching the* Jetsons *where George Jetson*, and his family, lived with technology such as flying cars that turned into briefcases, a robot as a maid, watches you could see images on and talk to others with, and even jetpacks for children to get to school.[3]

When you think about it, those items that were presented as figments of the imagination on the *Jetsons* have now become reality. From smartphones and smartwatches, to home security systems controlled from miles away, there is no question that the Information Age has brought forth a myriad of options to make life more efficient—but at what expense to privacy?

The question of whether the right to privacy in the Information Age even exists anymore was the foundation of a recent legal conference.[4] The focus of this conference centered on current topics including drones, medical technology, mall location, and DNA; the 4th Amendment and cell site location; data breaches; and how to educate ourselves when it comes to privacy and technology. Four lawyers presented their view on these topics.

CURRENT TOPICS AND TRENDS

Attorney Keith Cheresko[5] explained that when it comes to Privacy Law, there is often an overlap between state and federal laws, and even between state and municipal laws.[6] Privacy Law is a very broad area, and it touches on so many aspects of our daily lives, including for example biometrics. *Merriam-Webster* defines "biometrics" as "the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal

---

[1] Lopez v. United States, 83 S.Ct. 1381 (1963)
[2] Kyllo v. United States, 121 S.Ct. 2038 (2001).
[3] "The Jetsons is an American animated sitcom produced by Hanna-Barbera, originally airing in primetime from 1962 to 1963, then later in syndication for new episodes from 1985 to 1987 […]. It was Hanna-Barber's Space Age counterpart to The Flintstones." http://en.wikipedia.org/wiki/The_Jetsons (Last visited Feb. 15, 2015)
[4] Hosted by the Western Michigan University (WMU) Cooley Law School Journal of Practical and Clinical Law on Friday, January 30, 2015—just two days after International Privacy Law Day
[5] Principal at Privacy Associates International LLC (PAI).
[6] Keith Cheresko, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).

identity."[7] In South America, there are some Mercedes-Benz vehicles that are actually started with the touch of a thumbprint instead of a key.[8] "There is no way a person can go out and change his thumbprint"[9]—what you see is what you get. This raises a concern not only for Privacy Law, but for safety in general. Just how much damage could really be done if another person was able to "lift" your thumbprint?

Besides the question related to the use of thumbprints, another was raised regarding the relationship between Privacy Law and healthcare. With the advancements in technology during the Information Age have also come advancements in the practice of medicine. With the utilization of new medical devices, which have a technological platform allowing these devices to be controlled remotely, the legal world is presented with a new phenomenon—"death by wire."[10] Just imagine having a feud with someone who either has outright access, or can breach access, and either increase or decrease the power to your cardiac device. "Remote monitoring of implanted cardiac devices is an evolving method for regular checks of their electronic integrity and functioning. The communication with the devices is carried out unsupervised with wireless trans-telephonic or cable-dependant linkage."[11]

We are moving away from the tedious days of having to physically inspect medical devices for their effectiveness, and more towards efficiencies in medical service. By utilizing devices that can be controlled remotely, it allows more time for a doctor to see other patients, and it can lessen the amount of time a patient has to use on follow-up appointments. However, with these efficiencies comes the concern of maintaining one's privacy for his or her medical care beyond a mere lost file. If there is a breach of the information passed wirelessly between a person's medical device and the designated doctor, not only has privacy been invaded, but now there is concern that the breacher may even have the power to seriously impact the patient's life—up to and including death.[12]

Drones are another topic discussion when reviewing current areas of Privacy Law[13] (and of personal safety concern to the author, a student pilot of small airplanes). The "FAA regulations say drones shouldn't be flown above 400 feet. Higher than that, drones start to interfere with the national

---

[7] Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/biometrics (last visited Feb. 15, 2015).
[8] Cheresko, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).
[9] *Id.*
[10] *Id.*
[11] N.M. van Hemel, *Remote monitoring of implanted cardiac devices: a plea for a nationwide exploration*, Neth Heart J. 17(11), 434-37 (2009), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2779481/ (last visited Feb. 15, 2015).
[12] Cheresko, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015) (along with discussion with conference attendees).
[13] *Id.*

airspace. They can't be flown within a few miles of an airport, and they can be used only for fun—not for commercial purposes."[14] Yet, what is this "fun" people are using it for?

The situation where someone used a drone to peer into the second-story bedroom window of someone else's home[15] again raises a privacy concern. Now, a person does not have to drive to your home, or even use a ladder, or jump a fence; with the purchase of a "fun" device, someone could very well look into windows a person may think are so high up, or so far out of sight, that no one would ever be able to see into them. With the use of drones, this is changing. Someone who is knowingly subjected to the authority of the FAA, would likely be mindful of the ramifications of actions that should not be engaged in; but what about a twelve-year old boy? Is he really concerned about the FAA or your right to privacy, or is he more concerned with what is "fun" for himself?

4TH AMENDMENT AND CELL SITE LOCATION

Attorney Patrick Corbett[16] covered the 4th Amendment and cell site location, including the difference between retrieving historical information versus real-time data.[17] Relating to cell tower records, "It's not about content, or the conversation. It's about incoming and outgoing calls, length of the call, and where you are in relation to cell towers[18] … [n]evertheless, given the potentially extreme private nature of such records, the question arises regarding what level of proof law enforcement should be required to show in order to get such information."[19]

There are two cases related to the topic of cell site location and the data retrieved from such—*United States v. Skinner*[20], and *In Re Application of the United States of America for Historical Cell Site Data*.[21] [22] When it comes to historical data, it was decided in *Skinner*, one has to show there is a reasonable suspicion, and when it comes to *current* data, one only needs to show that there is relevance.[23] It was

---

[14] Sarah Gonzalez, *Where Can Drones Fly?: Legal Limits Are up in the Air*, *available at* http://www.npr.org/2014/08/10/339181964/where-can-drones-fly-legal-limits-are-up-in-the-air (Aug. 10, 2014) (last visited Feb. 15, 2015).

[15] Cheresko, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).

[16] Former professor at WMU Cooley Law School (with an extensive background in Criminal Law) and currently with the United States Attorney's Office for the Eastern District of Michigan.

[17] Patrick Corbett, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015)

[18] *Id.*

[19] PowerPoint Presentation: Patrick Corbett, *Fourth Amendment and Cell Site Location Information*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).

[20] United States v. Skinner, 690 F.3d 722 (6th Cir. 2012).

[21] In Re Application of the United States of America for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

[22] PowerPoint Presentation: Patrick Corbett, *Fourth Amendment and Cell Site Location Information*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).

[23] Corbett, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015) (discussing *Skinner*).

Skinner that helped set the foundation for pinged phone tracking. "A ping tracks the location of a cell phone by tracking the last signal."[24] "Pings are not immediately ascertainable, but within a few hours, the general location (sometimes as specific as a particular address) can be identified."[25] Well, when a person uses his or her cell phone, what about that person's privacy during use?

In *Skinner*, agents pinged the defendant's phone in order to track his progress towards a truck stop where authorities arrested him with over 1,000 pounds of marijuana.[26] The court basically held that there is "no reasonable expectation of privacy in information given off by *voluntarily* purchased cell phone, so, there is no 4th Amendment violation."[27] This means there is "no need to get a warrant based on probable cause."[28]

In the 5th Circuit case of *In re Application*, it was decided that officers only need to show relevance, because there is a "high government interest" when it comes to cell site locations, so it is reasonable.[29] Corbett shared that this particular issue remains unexplored by the U.S. Supreme Court at this time;[30] and even a review of the conference highlights presented in this very article shows that the U.S. District Courts are in fact split.

In *Riley v. California*, it was decided, by a unanimous decision, that a search warrant, based on probable cause, is necessary to search cell phones that have been retrieved incident to an arrest.[31] In *Riley*, the court stated,

> The United States and California both suggest that a search of cell phone data might help ensure officer safety in more indirect ways, for example by alerting officers that confederates of the arrestee are headed to the scene. There is undoubtedly a strong government interest in warning officers about such possibilities, but neither the United States nor California offers evidence to suggest that their concerns are based on actual experience.[32]

---

[24] *When You Simply Must Locate Someone* http://www.iiiweb.net/blog/simply-must-locate-someone-cell-phone-ping-works-wonders/ (last visited Feb. 15, 2015).
[25] *Id.*
[26] United States v. Skinner, 690 F.3d 722 (2012).
[27] PowerPoint Presentation: Patrick Corbett, *Fourth Amendment and Cell Site Location Information*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).
[28] *Id.*
[29] Corbett, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015) (discussing *In re Application*).
[30] Corbett, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).
[31] Riley v. California, 134 S.Ct. 2473 (2014).
[32] *Id.* at 2485.

The court in *Riley* discussed the primary concerns related to the destruction of cell phone data: remote wiping and data encryption.[33] "Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data."[34] "Encryption is a security feature that some modem cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that renders a phone all but 'unbreakable' unless police know the password."[35] Even the court in *Riley* recognized these Privacy Law concerns:

> The storage capacity of cell phones has several interrelated consequences for privacy. First a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[36]

The court in *Riley* recognized that a person's cell phone essentially carries his or her life's contents. Although cell phones are intricate devices for everyday life, "because of the role that these devices have come to play in contemporary life, searching their contents implicates very sensitive privacy interests that [the courts are] poorly positioned to understand and evaluate."[37] With advancements in technology access to information is heightened, including "information about the lives of ordinary Americans, and at the same time, many ordinary Americans are choosing to make public [. . .] information that was seldom revealed to outsiders just a few decades ago."[38] With these changes, "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."[39] However, even with the great

---

[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.* at 2497.
[37] *Id.* at 2497-89.
[38] *Id.*
[39] *Id.*

considerations discussed by the court, the *Riley* case does not affect the outcome of matters related to cell site location as it currently stands.[40]

DATA BREACHES AND IDENTITY THEFT

Michigan Attorney Shawn Clark[41] provided a general overview of technology to conference attendees along with legal implications tied to the areas of data breaches and identity theft. Some of the primary reasons why people should be more aware about their privacy in connection with technology is because, 1) "[p]ersonal information [is] no longer in control of the individual"[42]; 2) "[i]nformation may be collected by services and technology we use"[43]; and 3) "[i]ndividuals have no control over the security to protect this 3rd party data."[44]

In the state of Michigan, there is actually a data breach statute found in the Michigan Compiled Laws (M.C.L.).[45] Under the M.C.L., notice has to be given when there is a data breach which affects more than one person.[46] Under the same statute, data is defined as "computerized personal information."[47] Litigation hurdles that one may run into when dealing with data breaches include: 1) whether there is Article III standing, and 2) litigation may fail due to lack of actual damages.[48] In the case of *In re Sony United States* there was a data breach of 70 million user accounts.[49] "An increased risk of identity theft is not a cognizable injury for negligence action in California."[50] In order for there to be damages, "there needs to be misuse for identity theft damages."[51]

---

[40] Corbett, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).
[41] Who has an extensive background in technology, including designing and programming digital games.
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] Shawn Clark, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).
[46] MICH. COMP. LAWS § 445.72 (2011), *available at* http://www.legislature.mi.gov/(S(o5fbdq45e05aas45qlbuj055))/mileg.aspx?page=GetObject&objectname=mcl-445-72 (last visited on February 15, 2015).
[47] MICH. COMP. LAWS § 445.63 (2011), *available at* http://www.legislature.mi.gov/(S(kmzutgawyaegyy450msigjn3))/mileg.aspx?page=GetObject&objectname=mcl-445-63 (last visited on February 15, 2015).
[48] Clark, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).
[49] *Id.* (discussing In Re Sony Gaming Networks and Customer Data Security Breach Litigation, 903 F.Supp.2d 942 (S.D. Cal. 2012)).
[50] Clark, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).
[51] *Id.*

What about issues with user error? Recently, a number of celebrity photos had been made public, although they were intended to remain private.[52] This presented a question of whether the leak of photos was targeted or brute force.[53] Targeted attacks are those where "phishing techniques" such as malware by way of email is used, while brute force involves "computer automated login attempts to guess password[s]."[54] When it comes to user error, "simple passwords are the number one vulnerability."[55] The use of the same password among multiple accounts is also an issue.[56] These "targeted attacks may appear [to be] very legitimate."[57] In the case where the photos of celebrities with Apple iCloud accounts were leaked, "Apple reported no data breach in [its] iCloud service."[58] So, what can the average person do to protect privacy in the Information Age?

EDUCATING OURSELVES

Attorney Kristina Bilowus[59] shared three guidelines that can be used as a reasonable start: 1) understanding the issue, 2) law, and 3) conduct.[60] One has to consider the demographics factors such as age, gender, education, and experience with technology[61] together in order to glean the level of education needed as it relates to privacy and technology. One also has to compare privacy and technology in order to get a better understanding of where we are headed in the future.[62] The pros for privacy are "trust"[63] and "peace of mind,"[64] but there are also cons, such as "safety concerns"[65] (i.e., privacy). Tied to this are pros and cons as it relates to technology. Some pros of technology include

---

[52] *See generally* John Tozzi, *Does Apple's HealthKit App Have a Nude Celebrity Photo Problem?* (Sept. 3, 2014), *available at* http://www.bloomberg.com/bw/articles/2014-09-03/nude-celebrity-photo-leak-poses-problems-for-apples-healthkit-app (last visited Feb. 15, 2015).

[53] Clark, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).

[54] PowerPoint Presentation: Shawn Clark, *Data Breaches and Identity Theft*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).

[55] Clark, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).

[56] *Id.*

[57] *Id.*

[58] PowerPoint Presentation: Shawn Clark, *Data Breaches and Identity Theft*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).

[59] Who has conducted extensive research on topics such as the NSA and computer crimes, and also co-taught a computer crimes seminar at WMU Cooley Law School,

[60] PowerPoint Presentation: Kristina Bilowus, *Privacy & Technology: Educating Ourselves*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).

[61] Kristina Bilowus, Panelist Presentation at the WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: The Right to Privacy in the Information Age: Does It Even Exist Anymore? (Jan. 30, 2015).

[62] *Id.*

[63] PowerPoint Presentation: Kristina Bilowus, *Privacy & Technology: Educating Ourselves*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).

[64] *Id.*

[65] *Id.*

"advancement,"[66] "ease,"[67] and "necessity,"[68] while the cons include "compromising safety" and "security concerns." A review of both the pros and cons presents an underlying issue—Privacy Law in the Information Age.

As far as the law is concerned, the question of whether there should be a trade-off between privacy and security. Articles from the current news included one titled *Privacy is Dead, Invasive Technology is Here to Stay*.[69] In this article, the author asked readers to "[i]magine a world where mosquito-sized robots fly around stealing samples of your DNA. Or where a department store knows from your buying habits that you're pregnant even before your family does."[70]

Consumers have to put themselves "out there," but should be mindful of the information that is shared with others.[71] Considering where we are in society today, there should be no *real* expectation of privacy.[72] With this in mind, even those who aren't as technologically advanced as others can work to educate themselves.[73] Individuals can do so by: 1) regulating online usage; 2) being aware of what they place on social media platforms; 3) paying attention to phone plans (including data); 4) evaluating the forum they are in (i.e., work vs. home); 5) utilizing caution; and 6) staying aware and informed.[74] Practitioners can be of help when it comes to educating the general public about Privacy Law in the Information Age.[75] A helpful tool the average person can use when it comes to Privacy Law in the Information Age—S.E.L.F., which stands for to **S**tay informed, **E**ducate themselves, **L**imit ourselves, and **F**ind balance.[76]

WHERE DO WE STAND?

Security alone will not maintain privacy [, and] may conflict with privacy.[77]

---

[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.* (citing Agence France-Presse, *Privacy is Dead, Invasive Technology is Here to Stay*, Industry Week: Advancing the business of Manufacturing (Jan. 22, 2015), *available at* http://www.industryweek.com/technology/privacy-dead-invasive-technology-here-stay?page=2. (last visited Feb. 15, 2015)).
[70] Agence France-Presse, *Privacy is Dead, Invasive Technology is Here to Stay*, Industry Week: Advancing the business of Manufacturing (Jan. 22, 2015), *available at* http://www.industryweek.com/technology/privacy-dead-invasive-technology-here-stay?page=2. (last visited Feb. 15, 2015).
[71] PowerPoint Presentation: Kristina Bilowus, *Privacy & Technology: Educating Ourselves*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] PowerPoint Presentation: Keith Cheresko, *Current Privacy Law Topics*, WMU Cooley Law School Journal of Practical and Clinical Law Legal Conference: Right to Privacy in the Information Age: Does It Even Exist Anymore? (January 30, 2015) (on file with author).

I believe that the right to privacy is still in existence, however, the box in which it once fit, must now be expanded. Some would have you believe that because of advances in technology, people are willing to share everything, and really aren't concerned with privacy very much.[78] There is also a misconception that fewer people are really concerned with whom their private affairs are shared,[79] and it's okay for companies to dictate what we do with our information.[80] However, this couldn't be further from the truth. Just because we as a society happen to be more accessible does not mean that privacy should fall to wayside.

Overall, we are busier as a society, and the conveniences of technology come in handy. In fact, people look forward to new technology being introduced to make life better.[81] While on the go, a person can check e-mails between meetings right from a phone, make dinner reservations without ever speaking to a live person, and even get a live video feed of how a child is doing while in daycare.[82] These conveniences have become a necessary aspect of everyday life. Yet, simply because we have regular technological changes and updates, this does not mean the flood gates of personal information are to be busted open for the world to see.[83] If privacy wasn't such a concern to so many people, the list of current Privacy Law topics wouldn't be growing at the rate it has been.

Frankly, people really want more privacy, or better, the ability to control who their information is really shared with.[84] Just pay attention to the uproar of reactions when privacy settings are changed for peoples' Facebook pages[85]—there's a reason for this. People do not want to be dictated to when it comes to their own lives.[86] What's really wanted is a more hands-on ability when it comes to the many aspects of peoples' lives and the sharing of such.[87] The issue however, is that although people

---

[78] *See* Chris Matyszczyk, *Zuckerberg: I know that people don't want privacy*, CNET.COM, *available at* http://www.cnet.com/news/zuckerberg-i-know-that-people-dont-want-privacy/ (last visited Feb. 22, 2015).
[79] *Id.*
[80] *Id.*
[81] *See generally* Aaron Smith, *U.S. Views of Technology and the Future, Science in the next 50 years*, PEW RESEARCH CENTER, *available at* *http://www.pewinternet.org/2014/04/17/us-views-of-technology-and-the-future/* (last visited Feb. 22,2015).
[82] *See generally* *http://watchmegrow.com/parents* (last visited Feb. 22, 2015).
[83] *See generally* Thomas Claburn, *Microsoft Finds People Want More Privacy Control*, INFORMATIONWEEK.COM, http://www.darkreading.com/risk-management/microsoft-finds-people-want-more-privacy-control/d/d-id/1108342? (last visited Feb. 22, 2015).
[84] *Id.*
[85] Molly Wood, *Facebook Messenger Switch Controversy Is Part Misunderstanding, Part Mistrust*, BITS N.Y. TIMES BLOG, (Feb. 22, 2015, 10:21 PM), http://bits.blogs.nytimes.com/2014/08/08/facebook-messenger-switch-controversy-is-part-misunderstanding-part-mistrust/?_r=0.

[86] *See generally* Thomas Claburn, *Microsoft Finds People Want More Privacy Control*, INFORMATIONWEEK.COM, http://www.darkreading.com/risk-management/microsoft-finds-people-want-more-privacy-control/d/d-id/1108342? (last visited Feb. 22, 2015).
[87] *Id.*

want more privacy, even if it is in a more evolved sense as "control,"[88] enough isn't being done on a individual level to make sure this happens.[89]

It's generally known by many that the law may not always keep up with advances in the "real world."[90] Knowing this, we as individuals cannot sit and wait for someone else to step in and be a knight in shining armor ready and willing to protect all that represents us in the digital world. It takes active participation[91] to create an environment where privacy concerns are considered when future technological advancements are made.[92,93] As we move towards the days of things such as having more organs grown in labs,[94] the possible consolidation of DNA databases,[95] and cash becoming somewhat archaic,[96] we *must* remain aware—especially since there isn't one body of law that can be used for guidance in navigating the ebb and flow of that which is Privacy Law.[97] If we don't, the box that has been expanding could potentially disappear.

Christina M. Jeter *earned a Bachelor of Science in Business Administration from Central Michigan University; she also earned a Master of Science in Administration, with a concentration in Public Administration, from the same university. Christina M. Jeter is the Senior Legal Conference Editor for the WMU Cooley Law School Journal of Practical and Clinical Law. In addition, Ms. Jeter also works in management in state government for the State of Michigan where she has been directly involved throughout her career in various systems innovations and improvements. In addition to her full-time career and legal studies, Ms. Jeter is a member of a number of organizations, including several ABA sections and committees, is a volunteer intern at the 30th Circuit Court in Ingham County Michigan under the Honorable Rosemarie E. Aquilina, an intern at the WMU Cooley Law School Sixty Plus Estate Planning Clinic, finds time to volunteer for legal-based pro bono initiatives for the homeless. To balance things, she enjoys working on earning her private pilot's license and engaging in ballroom dance classes—including teaching. Christina M. Jeter is currently in her final semester of law school, and plans to take the bar exams and be admitted to practice in Michigan and New York.*

---

[88] *Id.*
[89] Shawn M. Griffiths, *People Want Online Privacy — They Just Don't Want To Do Anything About It*, IVN.US, http://ivn.us/2014/11/25/people-want-online-privacy-just-dont-want-anything/ (last visited Feb. 22, 2015).
[90] *See generally The Legislative Process*, http://www.sparknotes.com/us-government-and-politics/american-government/congress/section4.rhtml (last visited Feb. 22, 2015).
[91] *See generally* Zach Warren, *Privacy groups petition Facebook data use policy changes*, INSIDE COUNSEL, http://www.insidecounsel.com/2013/09/13/privacy-groups-petition-facebook-data-use-policy-c (last visited Feb. 22, 2015).
[92] *See Privacy versus new information technology*, EURONEWS, *http://www.euronews.com/2013/01/07/privacy-versus-new-information-technology/* (last visited Feb. 22, 2015).
[93] *See supra* note 90.
[94] *Lab-grown organs might be solution to transplant woes*, ASSOCIATED PRESS, http://www.nydailynews.com/life-style/health/scientists-work-grow-organs-transplants-article-1.1374818 (last visited Feb. 22, 2015).
[95] Gina Kolata, *Poking Holes in Genetic Privacy*, N.Y. TIMES, http://www.nytimes.com/2013/06/18/science/poking-holes-in-the-privacy-of-dna.html?pagewanted=all (last visited Feb. 22, 2015).
[96] Erika Rawes, *Is cash becoming a thing of the past?*, USA TODAY, http://www.usatoday.com/story/money/business/2014/09/06/wscs-cash-a-thing-of-the-past/15075047/ (last visited Feb. 22, 2015).
[97] *Supra* note 11.

Predictive Coding: No Longer An All-Or-Nothing Proposition

Alex Kiles, Alexander B. Hastings and Edward H. Rippey

In recent years, predictive coding has steadily gained traction in the e-discovery landscape -- yet, many lawyers and clients remain reluctant to harness the technology's full potential. This article aims to demonstrate that predictive coding need not be an all-or-nothing enterprise. Rather, the future of e-discovery lies in leveraging technology, including predictive coding, to enhance some aspect of every case. The threshold question should not be, "Should I use predictive coding?" but rather, "Where shall I use predictive coding in my case and at what stage should I phase it out?" This article briefly describes the mechanics of predictive coding and then turns to the manifold ways in which this technology can be leveraged to enhance any litigation.

A. What is Predictive Coding?

In general, predictive coding enables attorneys to review small, representative data sets for a case and then apply the review criteria to a larger set of documents -- automatically identifying responsive and nonresponsive documents as well as privileged and non-privileged documents. By examining the key characteristics of these documents and coding accordingly, a reviewer essentially "trains" the computer to categorize similar documents in the larger set. The reviewer can then edit or add to the list of relevant characteristics at any time to ensure quality control and consistency.[1] Unlike manual document review, predictive coding requires the coding and creation of a "seed set" of documents, which generally is conducted by senior attorneys with intimate knowledge of the case.

The benefits of predictive coding are multifold. It can dramatically reduce the number of documents slated for manual review, potentially reducing document review costs by 50% to 70%.[2] Understandably, computers do not suffer from the headaches, tired eyes, and boredom that may afflict lawyers spending hours parsing through thousands of documents.[3] By filtering out documents according to the

---

[1] Jason R. Baron, *Law in the Age of Exabytes: Some Further Thoughts on 'Information Inflation' and Current Issues in E-Discovery Search*, 17 RICH. J.L. & TECH. 9 (2011), *available at* http://jolt.richmond.edu/v17i3/article9.pdf.
[2] Tim Stuhldreher, *Predictive Coding Cuts Discovery Expenses*, 28 CENTRAL PENN BUS. J. 19 (2012).
[3] John Markoff, *Armies of Expensive Lawyers, Replaced by Cheaper Software*, N.Y. TIMES, Mar. 4, 2011, at A1, *available at* http://www.nytimes.com/2011/03/05/science/05legal.html?pagewanted=1&_r=1.

software's algorithm, attorneys need only review a fraction of the original set of documents.[4] Indeed, a recent study suggests that predictive coding may actually be more accurate than manual review.[5]

B. Key Components

While every case is unique, a number of key components will enable counsel to most effectively leverage predictive coding in their case:

Volume. Predictive coding works best with a large quantity of documents (*i.e.*, at least 80,000 - 100,000). Not only are the benefits of predictive coding most keenly felt when combing through a massive document set, but a sufficiently large quantity of documents also increases the effectiveness of the tool itself. The algorithms behind predictive coding generally require a significant amount of data in order to function properly.[6]

Subject Matter Expert. Perhaps the most critical component in the predictive coding process is the subject matter expert ("SME"). An SME is an individual intimately familiar with the case and tasked with coding the initial documents to train the algorithm. Under the traditional view of predictive coding, a single SME codes the seed set — the rationale being that one person ensures consistent coding decisions. However, some litigation support specialists now contend that multiple SMEs may be both more efficient and more statistically accurate than a single SME. A single SME creates a risk of an individualized error during the creation of the seed set quickly compounding, leading to an inaccurate final result. To avoid inconsistent coding decisions, multiple SMEs may find it beneficial to code the initial seed set in the same physical location so that they can discuss responsive attributes and harmonize their coding criteria. Additionally, multiple SMEs can challenge each other's coding decisions and critically engage in the coding process, a practice which may improve statistical accuracy.

Workflow. An efficient, practical and well-defined workflow is also critically important when leveraging technology to enhance a review. An e-discovery "workflow" typically consists of the processes involved when creating document batches, random sampling, keyword searching, quality control measures, training and correcting the algorithm, and measuring precision and recall. Although developing an efficient workflow maybe be time-consuming in the beginning stages of a review, it will ultimately save much time and effort in the overall review process.

---

[4] Ben Kerschberg, *E-Discovery and the Rise of Predictive Coding*, Forbes (Mar. 23, 2011, 10:04 AM), http://www.forbes.com/sites/benkerschberg/2011/03/23/e-discovery-and-the-rise-of-predictive-coding.

[5] Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review*, 17 RICH. J.L. & TECH. 11, 43 (2011), *available at* http://jolt.richmond.edu/v17i3/article11.pdf (finding that efficiency and effectiveness of technology assisted reviews surpassed traditional manual reviews).

[6] Ed Rippey et al., *Predictive Coding: E-Discovery Game Changer?*, EDDE JOURNAL (2011).

C. The Future of Predictive Coding

In today's modern world, the future of predictive coding must involve using a rigorous, statistically-based review process that leverages technology to enhance a case. Even if ultimately choosing to forego predictive coding for document production, organizations may want to consider using this technology to improve other aspects of their business. As will be discussed below, predictive coding can be effectively utilized in various models to achieve a variety of objectives:

Switching Mid-Stream. To begin, predictive coding need not be an all-or-nothing enterprise. Indeed, counsel is not required to decide at the beginning of a case whether or not to implement predictive coding. The process of initiating a review using a traditional linear model and then switching to predictive coding mid-stream can be quite seamless. If taking this route, counsel can use the documents that have already been reviewed as the initial seed set and refine from there to achieve statistically acceptable levels. Despite beginning with a manageable amount of documents, cases are often suddenly inundated with additional documents from new sources or, similarly, the scope of the case may increase through the addition of claims or counterclaims. In these situations, turning to predictive coding mid-review may be especially appropriate.

Most Responsive First. Predictive coding can also enhance traditional review by first ranking documents by responsiveness so that manual reviewers can focus on the documents the software has deemed most responsive early in the review process. In this way, if reviewers are faced with a pressing deadline and thousands of documents remain, counsel can take comfort in the fact that at least the most responsive documents have already been reviewed. This hybrid approach may enable counsel to more efficiently reach the documents at the heart of a matter in cases where time is of the essence.

Split and Outsource. As any lawyer will attest, clients are keenly cognizant of keeping discovery costs as low as possible. To help accomplish this goal, counsel may want to consider leveraging predictive coding to bifurcate the review process. Under this model, the documents deemed most responsive by the algorithm are set aside for review by attorneys with subject-matter expertise, often senior, and thus more-costly, attorneys. The second set of documents, the ones least likely to be responsive, are then outsourced to staff attorneys or other reviewers. In this way, counsel can help manage ever-mounting discovery costs without sacrificing quality.

Quality Control. Although studies are beginning to reveal that predictive coding may be more accurate than traditional manual review, counsel and clients may remain reluctant to produce documents to opposing counsel that have never been seen by human eyes. In these situations, predictive coding can be effectively used as a quality control measure to determine if manually-coded privilege and relevance tags are accurate. This added layer of security can permit counsel to remain confident that privileged documents have not inadvertently been sent to opposing counsel.

Case Preparation. Counsel may also take advantage of the benefits of predictive coding when preparing for a case. For example, predictive coding may be particularly useful in the initial stages of a case to review a client's database and quickly identify potential strengths or weaknesses for a motion for summary judgment. Counsel may also elect to use predictive coding to gather the documents best-suited to prepare a client for a deposition. The inherent flexibility of this technology enables counsel to quickly identify and organize materials specific to various deponents.

Investigations and Compliance. In the investigations context, predictive coding may prove particularly useful to counsel and their corporate clients, as it can allow counsel to rapidly review a client's data and identify inherent risks. Counsel can then use the documents deemed responsive by the software to meaningfully consult with the client and develop adequate compliance measures.

Record Retention. Finally, as part of a company's normal operations, predictive coding can be implemented to identify documents that can be deleted pursuant to the organization's document management and record retention policy. Should future disputes arise over deleted documents, counsel will be able to use the predictive coding workflow and statistical data, in addition to their client's retention policy, to craft a robust defense.

D. The Case Law

To those still grappling with whether to leverage technology, including predictive coding, to enhance their case, the trend in recent case law should provide solace. The increasing number of decisions addressing predictive coding indicate that this technology is gaining traction and legitimacy as a useful litigation tool. Indeed, the response has largely been positive with courts generally commenting on the benefits of predictive coding over manual review.[7] A number of lessons can be drawn from a survey of the cases discussing predictive coding.

First, and most importantly, courts are beginning to favor predictive coding in unwieldy e-discovery cases given the disadvantages of keyword searches and manual review.[8] Indeed, since *Da Silva Moore*[9], the landmark case first addressing predictive coding, courts have been moving towards permitting, and even encouraging, its use.[10] Even in *Progressive Casualty*, a case which ultimately rejected the use of predictive coding, the judge lauded the numerous benefits of the technology.[11]

---

[7] *See, e.g.*, *EORHB, Inc. v. HOA Holdings, LLC,* Case No. 7409-VCL, 2012 WL 4896667 (Del Ch. Ct. Oct. 15, 2012); *Dynamo Holdings Ltd. Partnership v. C.I.R.*, Nos. 2685–11, 8393–12, 2014 WL 4636526 (T.C. Sept. 17, 2014); *Bridgestone Americas, Inc. v. IBM Corp.*, No. 3:13–1196, 2014 WL 4923014, at *1 (M.D. Tenn. July 22, 2014); *Global Aerospace, Inc. v. Landow Aviation, L.P.* 2012 WL 1431215 (Va. Cir. Ct. Apr. 23, 2012).

[8] *See* Jacob Tingen, *Technologies-That-Must-Not-Be-Named: Understanding and Implementing Advanced Search Technologies in E-Discovery*, XIX RICH. J.L. & TECH. 1, 2, 8 (Nov. 26, 2012), *available at* http://jolt.richmond.edu/v19i1/article2.pdf.

[9] *Da Silva Moore v. Publicis Groupe*, 287 F.R.D. 182 (S.D.N.Y. 2012).

[10] *See, e.g.*, *National Day Laborer Organizing Network v. U.S. Immig. & Customs Enforcement Agency*, 877 F. Supp. 2d 87 (S.D.N.Y. 2012); *Gabriel Technologies Corp. v. Qualcomm Inc.*, 2013 WL 410103 (S.D. Cal. Feb. 1, 2013), *aff'd*, 560 F. App'x

Second, as in other aspects of e-discovery, courts generally value cooperation and are reluctant to allow predictive coding if one party acts unilaterally and fails to consult opposing counsel or the court before employing the technology.[12] Nevertheless, some courts are also concerned with the potential cost of *not* using predictive coding and may permit it if it serves the goal of proportionality.[13] Parties may determine that it is best not to wait until late in the discovery process to raise predictive coding for the first time.

Finally, at least one court has determined that it lacked the power to compel documents contained in a party's seed set.[14] This may assuage fears counsel may hold that if they fully abide by their duty to cooperate, opposing counsel will be entitled to input in the coding of the seed set. Counsel may also worry that by using predictive coding they will be required to automatically produce the documents the algorithm deems responsive without first having the opportunity to double-check them for privilege. Nevertheless, this worry may be overstated as a recent case from Magistrate Judge Francis suggests otherwise.[15]

E. Conclusion

Technology assisted review has become a rapidly growing industry and many vendors now offer services to assist counsel and their clients with leveraging technology to enhance their case in the manners identified above. It is important to remember at the early case assessment stage that predictive coding can be used for all or some (or even no) parts of a litigation -- depending on the specific circumstances. And, with the judiciary on board, as the case law suggests, it is readily apparent that counsel and their clients will continue to develop innovative methods to harness fully the potential of this technology.

Alex Kiles *(akiles@cov.com) is a litigation and white collar investigations associate and member of the E-Discovery Practice Group at Covington and Burling, LLP.* ***Alexander Hastings*** *(ahastings@cov.com) is a government contracts and litigation associate and a member of the firm's E-Discovery Practice Group.* ***Edward Rippey*** *(erippey@cov.com) is a partner at the firm, handles complex commercial litigation, and is Chair of the E-Discovery Practice Group.*

---

966 (2014); *In re Biomet M2a Magnum Hip Implant Prods. Liab. Litig.*, No. 3:12–MD–2391, 2013 WL 1729682, at *1 (N.D. Ind. Apr. 18, 2013).

[11] *See Progressive Cas. Ins. Co. v. Delaney*, 2:11-CV-00678-LRH, 2014 WL 3563467 (D. Nev. July 18, 2014).

[12] *See, e.g.*, *id*.

[13] *See Global Aerospace v. Landow Aviation*, No. 2:11–cv–00678, 2012 WL 1431215 (Vir. Cir. Ct. Apr. 23, 2012).

[14] *In re Biomet M2a Magnum Hip Implant Prods. Liab. Litig.*, No. 3:12–MD–2391, 2013 WL 6405156, at *2 (N.D. Ind. Aug. 21, 2013).

[15] *See In Chen-Oster v. Goldman Sachs & Co.*, No. 10 Civ. 6950, 2013 WL 3009489 (S.D.N.Y. June 18, 2013) (concluding that parties are entitled to review documents the software has marked responsive prior to producing them, unless parties agree otherwise).

Are You a Risk to Your Own Firm or Business?

By David Willson

Despite all of the bad news and negativity in the world, most of us have a very positive or even inflated opinion of ourselves. How many people believe they are ugly, bad drivers, or disliked by others? Very few. As the owner or partner of a law firm or business-owner, you may be one of the greatest risks to your own organization. Many successful business leaders are type-A personality, extremely sure of themselves and believe their manner of doing business is better than the next guy or gal. In business this is exactly what is needed, and that is why many are so successful. But, when it comes to cyber-security this attitude creates a blind side to the realities of how vulnerable we really are.

This article discusses four factors impacting law firm owners/partners and business owners that may significantly increase cyber risk, and thus potential liability, loss of business and reputation:

- "Optimism bias" and complacency;
- "Convenience v. security";
- The "emperor has no clothes" syndrome; and,
- Self-imposed ignorance.

First, it's safe to say, and hopefully all will agree, cyber-security, data breaches and hacking, have become a very big deal. If you have not heard about the data breaches at Target, Home Depot, Sony, and now Anthem, then you must be living under a rock. As Monica says in an episode of "Friends," "It just got interesting!"[1] The level of concern, especially amongst business owners, is definitely ramping up. I am increasingly hearing from clients and potential clients that their customers and potential customers are asking if they are secure. Most inquiries have likely been prompted by these high profile breaches, the astronomical amounts of money they are costing, and the fact that some executives lost their jobs or resigned, not to mention the increasing number of class action lawsuits with both consumers and banks, seeking to hold someone liable.[2] In fact, banks recently, in order to mitigate their liability and loss, asked Congress to hold retailers responsible for breaches to their businesses.[3]

---

[1] "Friends - It Just Got Interesting," Season 5 Episode 24, YouTube, 14 Oct. 2012.
[2] *See* Judge Magnuson's Ruling in, "In re: Target Corporation Customer Data Security Breach Litigation," filed 2 Dec. 2014, at: http://cdn.arstechnica.net/wp-content/uploads/2014/12/document3.pdf.
[3] Berger, Dan, "Congress Must Make Retailers Responsible for Data Breaches," American Banker, 15 Jan. 2014.

The first factor adding to our risk is a theory called, "optimism bias."[4] Below are some survey questions I frequently use when speaking at conferences:

1. Do you believe your firm or business will be breached this year?
2. If yes, is there an 80% or 30% chance of the breach?
3. Do you believe another firm/company, or, "the other guy," will be breached this year?
4. Is there a 30% chance or 80%?

Most surveyed believe they will not be breached or there is a low probability. Conversely most believe the "other guy" will be breached and there is a very high probability.

Why? What have you done differently? Is your security better than Target, Home Depot, NSA, the Pentagon, Lockheed-Martin, the local Liquor store? Remember the movie, "My Cousin Vinny?" Joe Pesci, who plays Vinny Gambini, is defending his nephew and his nephew's friend who are accused of robbing a convenience store and murdering the clerk. Vinny is questioning a witness to the crime who states that when he began to make his breakfast, eggs and grits, he saw the defendants go into the convenience store. The witness then testifies that 5 minutes later he sees the two boys leave the store when he is about to eat his breakfast:

"Vinny Gambini: So, Mr. Tipton, how could it take you five minutes to cook your grits, when it takes the entire grit-eating world twenty minutes?

Mr. Tipton: [a bit panicky] I don't know. I'm a fast cook, I guess.

Vinny Gambini: I'm sorry; I was all the way over here. I couldn't hear you. Did you say you were a fast cook? That's it?

[Mr. Tipton nods in embarrassment]

Vinny Gambini: Are we to believe that boiling water soaks into a grit faster in your kitchen than on any place on the face of the earth?

Mr. Tipton: I don't know."[5]

Ask yourself, "Do the standard security practices work better on your network, or do you use magic security practices no one else is aware of?" Whether you are the victim of a random drive-by breach or specifically attacked like the law firms targeted by China in order to gain mergers and acquisition data

[4] Shah, Sonali, "Cyber Security Risk: Perception vs. Reality in Corporate America," Wired, Mar. 2014, citing Tali Sharot, "Tali Sharot: The optimism bias | Talk Video | TED.com, May 2012.
[5] IMDb, "My Cousin Vinny Quotes."

on their clients, you are under attack and you will likely fair no better than most, certainly the big guys.[6]

So, what may cause us to believe our security is better? This attitude can blind us to reality, especially because it leads us to become complacent and not concern ourselves with security. As stated above, most of those surveyed believe their security is pretty good, certainly better than their neighbor's, and the chances of suffering a breach are fairly low. In reality most firms/businesses either will be or have already been breached.[7] Amazingly, most business owners who claim they won't be breached also had little to do with the implementation of their own security and likely do not really understand it.

Passively assuming someone else, like your outsourced IT Company or your in-house IT department, is identifying and addressing the threats and risks is not an adequate form of risk management. Even if your firm/business has or uses a CFO aren't you familiar with and understand the finances and budget of your firm/business? To ignore this would be dangerous and potentially negligent. So, why do we ignore our security? We need to get better acquainted with the security currently employed and identify potential risks. As the lawsuits mount after the above-mentioned recent high profile breaches and CEO's are fired or resign, you can no longer take a hands-off complacent attitude when it comes to technology, cyber-security and risk.

The next factor is what I refer to as "convenience v. security." Technology has been both a blessing and a curse. Most of us have a love-hate relationship with our computers and mobile devices. Very rarely do you hear people say, "I love my smart phone or iPad, or whatever device," but, we can't live without them. In fact, some people are so obsessed that they are willing to camp out in front of the store for days to be the first to get the latest and greatest device. What we love about them is the convenience and security threatens that convenience. Most people find the security practices tiresome, awkward, and annoying. For instance, do you password protect your smartphone or mobile device? Passwords are annoying though, right? So, a lot of people either don't use one or use a very easy password, like 1234. In 2014 3.1 million smartphones were stolen.[8] The number lost is probably at least equal to or greater than that. What would a thief or someone who found your smartphone or mobile device have access to if it was stolen or lost? Do you have to log into your social media on your mobile device or can you login automatically? If automatically then that person now has access to all of your social media, email, texts, contacts, etc. But, we find the security rules for our devices inconvenient and so either ignore them or attempt to make them as simple as possible or find a workaround. As Job stated, "Shall we indeed accept good from God, and shall we not accept adversity?"[9] Shall we accept the

---

[6] Riley, Michael A., and Pearson, Sophia, "China-Based Hackers Target Law Firms to Get Secret Deal Data," BloombergBusiness 12 June 2012.

[7] Cowley, Stacey, "FBI Director: Cybercrime will eclipse terrorism," CNNMoney, quoting Robert Mueller, Director of the FBI, speaking at the 2012 RSA Conference: "There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again, ..."

[8] "Smart phone thefts rose to 3.1 million last year, Consumer Reports finds," ConsumerReports.org, May 2014.

[9] New King James Bible, Job 2:10.

convenience of technology and ignore the risks? Think about the volumes of data that your firm deals with, creates, receives, transmits, and carries around monthly. It is all at risk. Are you willing to increase that risk because you find security rules inconvenient?

The third factor is called the "emperor has no clothes" syndrome. The job of securing the network, all mobile devices, and anything else related to technology and the information that flows across it has fallen in the laps of the IT Company or department. Granted, many firms or businesses have hired CISOs (chief information security officers) and other experts, but the majority of businesses and law firms have not. Some IT professionals may be skilled and thus able to serve a dual-role as security and IT professionals, but most are not. So, the battle begins. That is, the battle for budget. Now, if you are the IT guy, your primary focus is likely "uptime" and making sure everyone can access the network. Security, unfortunately, plays second fiddle, and revealing how vulnerable the network is may not bode well if the boss is constantly hearing the negative. In some cases the IT department or company doesn't know the full risk or extent of the vulnerabilities, but this is unlikely. What is more likely is that they know but are hesitant to reveal how bad it really is, how vulnerable you really are, for fear of the impression it will create, e.g. maybe they are not able to fully secure the network or are just looking for more money. Regardless of the reason or reasons, the message about how much risk exists gets lost and never conveyed to leadership. This is a risk in and of itself. IT departments and companies are playing with fire if they don't reveal the true risks and vulnerabilities and allow the leaders to address them. Have you have seen some of the TV ads for anti-virus companies that claim to speed up and protect your computer? Whether their contract says it or not, many of them are making it appear that they will make you 100% secure. Well, they aren't and they can't. If you purchase their product and then get a nasty virus and lose some or all of your data you will be pretty mad and likely consider suing. Owners, partners, managers, leaders, if you are given the impression your network is secure, or not told about how vulnerable it is and therefore assume it is secure, what will your reaction be when you are breached? Likely, what the *#$&? IT departments and companies, tell the truth, the whole truth and nothing but the truth, they need to know. Owners, partners, managers, leaders or bosses, you need to know how bad it is in order to evaluate and mitigate the risks, so go ask.

The final factor is self-imposed ignorance, which comes with a downplaying of the threat, maybe some "optimism bias," and, as mentioned above, ignorance of the seriousness of the risks facing the firm or business. When I speak to companies about cyber-security and the need for a risk assessment, I hear far too often: "I'm not worried, I don't have anything the hackers want to steal;" "I'm not worried, my business is too small;" or, "I'm not worried, our IT guys make us use really good passwords and we have cyber insurance." Wow! That's like saying; "I will never get in a car accident because I am a great driver." Some things you just can't control. There is an old saying that goes: "There are two things you can count on, death and taxes." I would add a third, getting hacked! It will happen. In fact it probably already has and you don't even know it.

There are many tips, procedures and techniques you can implement to improve your security, but, in my opinion, the first place to start and most important is to do a self-risk assessment:

- Understand the information you collect;

- How it flows across your network;

- What devices it resides on;

- Who has access to it;

- How it is kept secure, and;

- Who you are connected to, (e.g. ISP, Cloud provider, other services, etc.).[10]

If an incident occurs or a client asks what you did or are doing to secure data, responding with, "I don't know, ask my IT guy," or, "We use really good passwords," is not sufficient and will significantly increase your liability and make you look incompetent about an issue that is foremost on most people's minds these days.

The point is, take an active role. You need to lead and manage the process. Don't just hand it over to someone else like the IT department or an IT guy or company, and forget about it. Never assume your security is great, good or even adequate. It's not. Security is not a set and forget concept but a process. Manage it. At any given time you must be able to articulate what you have done to protect data and the firm or business. Pointing to the IT guy or someone else is not a risk management solution or a valid response during an incident response investigation. Are you a basic, progressing or advanced organization?[11] Take charge, take control, and manage.

David Willson *is a retired Army JAG. Among his assignments he worked at NSA and helped to establish CYBERCOM and provided legal advice for many cyber operations and policy. He is owner of Titan Info Security Group and is licensed in CO, NY and CT. He specializes in risk management and cyber security helping companies and law firms lower the risk of a cyber incident and reducing the potential liability if and when the firm or its vendor is compromised and all of the client information is stolen. He also provide cyber security awareness training and assists with other unique cyber issues related to discovery, evidence, trial prep, forensics and more. His website is at www.titaninfosecuritygroup.com and he can be contacted at 719-648-4176, or david@titaninfosecuritygroup.com*

---

[10] If seeking resources to assist in your self-assessment, you can email me for a free two-page "Cyber Self-Assessment" form, or, for a more extensive checklist approach that will generate a report, see the Homeland Security Cyber Resilience Self Assessment Package: https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf, and the User Guide: https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf.

[11] *See*, "Security Maturity graphic," Enterprise Strategy Group, Nov. 2014, at: http://krebsonsecurity.com/wp-content/uploads/2014/11/SecurityMaturity.png.

Editor's Message

With this issue, we are not only well into the sixth year of publishing each quarter the *Information Law Journal* (previously published separately as the *Information Security and Privacy News* and the *EDDE Journal*), but are continuing to welcome authors and readers from similar committees across the ABA, including members from the Antitrust Section. This issue presents articles from lawyers and technologists focusing on various aspects of leading-edge domestic and international practice. The first article was written by Jill Bronfman of the UC Hastings College of the Law, discussing the new California data breach statute. The second article is from Aldo M. Leiva, partner at Lubell Rosen, covering Florida and HIPAA considerations for regulated entities. The third article is by frequent contributor Renato Opice Blum, explaining the evolution of Brazilian privacy law. The fourth article is from Christina Jeter, relaying the analysis of four lawyers on whether privacy still exists. The fifth article is from the team at Covington & Burling LLP led by partner Edward H. Rippey, covering the e-discovery issues for predictive coding. The sixth article is from David Willson of the Titan Info Security Group, on whether business leaders pose a cyber-security risk to their own firms.

Thank you to all of the authors. I continue to ask that all readers of the *Information Law Journal* to share with their fellow professionals and committee members by writing an article for this periodical. Our next issue (Summer 2015) will come out in June 2015. There are many of you who have not yet been able to share your experience and knowledge by publishing an article here but please consider doing so to widen the understanding of all of our readers. Every qualified submission meeting the requirements explained in the Author Guidelines will be published, so please feel free to submit your articles or ideas, even if you are not quite ready for final publication. The issue following Summer (Autumn 2015) will be published in September 2015. As always, until then… and Happy St. Paddy's Day.