McDermott
Will & Emery

Privacy and Data Protection

2014 YEAR IN REVIEW

In 2014, regulators around the globe issued guidelines, legislation and penalties in an effort to enhance security and control within the ever-shifting field of privacy and data protection. The Federal Trade Commission confirmed its expanded reach in the United States, and Canada's far-reaching anti-spam legislation takes full effect imminently. As European authorities grappled with the draft data protection regulation and the "right to be forgotten," the African Union adopted the Convention on Cybersecurity and Personal Data, and China improved the security of individuals' information in several key areas. Meanwhile, Latin America's patchwork of data privacy laws continues to evolve as foreign business increases.

This report furnishes in-house counsel and others responsible for privacy and data protection with an overview of key action points based on these and other 2014 developments, along with advance notice of potential trends in 2015. McDermott will continue to report on future updates, so check back with us regularly.

Heather Egan Sussman
Co-Chair, Privacy and Data Protection Group
Boston

Rohan Massey
Co-Chair, Privacy and Data Protection Group
London

Daniel F. Gottlieb
Co-Chair, Privacy and Data Protection Group
Chicago

TABLE OF CONTENTS

TABLE OF CONTENTS

Data brokers, the FTC's expanding reach, several notable Supreme Court cases and record FCC fines were just a few hot topics in the United States this year. In Canada, new anti-spam legislation affects all companies sending commercial electronic messages to Canadian individuals.

UNITED STATES

38.8833° N, 77.0167° W

FTC Continues to Expand Its Role as All-Purpose Data Privacy and Security Regulator

David Quinn Gacioch and Bridget K. O'Connell

As data breaches became a near-daily headline in 2014, and as millions of consumers face having their personal data compromised by cyberattacks, the Federal Trade Commission (FTC) has continued expanding its role as the leading U.S. data privacy and security regulator across states and economic sectors. Notable 2014 developments in two key cases underscore the FTC's expanding reach into the cybersecurity realm, and numerous FTC settlements and other announcements demonstrate that the FTC is policing a wide variety of issues related to consumer data privacy and security.

WYNDHAM AND LABMD: CHALLENGES TO FTC ENFORCEMENT AUTHORITY ONLY MAKE IT STRONGER

The vast majority of privacy and data security cases in which the FTC commences enforcement proceedings result in settlements. As a result, courts do not have the opportunity to adjudicate the substantive contours of the FTC Act in the privacy and data security area, or the boundaries of the FTC's enforcement authority in this area. This situation has left the FTC with largely unchecked authority to assert its own (expansive) view of what its enabling statute requires and prohibits. Two cases entered 2014 as exceptions to that rule, and important developments in those cases led the year's privacy and data security enforcement headlines.

In its 2012 Arizona federal court complaint against Wyndham Worldwide Corporation and affiliates, the FTC alleged that Wyndham acted in both a "deceptive" and an "unfair" manner, in violation of Section 5 of the FTC Act, by failing to maintain reasonable and appropriate security measures for consumer data. It claimed that Wyndham's failure to maintain appropriate cybersecurity measures resulted in three data breaches that exposed more than 600,000 consumer payment cards to hackers and resulted in more than $10 million in fraud losses. Notably, the FTC stressed allegations that Wyndham failed to act in accordance with its own stated privacy policies, in keeping with the FTC's broader theme of enforcing privacy promises.

Rather than entering into a negotiated consent decree with the FTC, Wyndham took the unprecedented step of challenging the FTC's authority to police data cybersecurity issues, seeking dismissal of the FTC's claims. In early 2013, an Arizona federal district court judge transferred the case from Arizona to New Jersey, where the parties continued to litigate Wyndham's dismissal motions.

In April 2014, the New Jersey federal judge issued a landmark ruling denying Wyndham's motion to dismiss, holding that the FTC, as general matter, does have the authority to bring enforcement actions over "unfair" data security practices under the FTC Act, and that the FTC is not required to promulgate regulations to specifically alert companies as to what it considers unfair or deceptive acts in the data security context before bringing such enforcement actions. Importantly, the judge limited her decision to the specific facts alleged against Wyndham by the FTC, explaining that her ruling "does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked" and stressing that a final decision on the merits of the FTC's claims remained "for another day."

Two months later, the court denied Wyndham's bid to dismiss itself and two subsidiaries from the suit, which would have left only a third subsidiary—the one at which the FTC's allegations were most directly aimed—to defend. In a ruling that privacy professionals representing large organizations should note, the judge ruled that the FTC had sufficiently alleged that the Wyndham entities were a "common enterprise" to keep all four entities potentially on the hook for any liability that might result. This common enterprise standard appears to differ from modern corporate veil-piercing law and significantly extends the FTC's enforcement reach within corporate families.

In July 2014, over the FTC's opposition, the judge granted Wyndham the right to appeal her April decision to the U.S. Court of Appeals for the Third Circuit, which will hear Wyndham's appeal in early 2015. The Third Circuit's decisions regarding the extent of the FTC's authority to enforce the unfairness prong of Section 5 of the FTC Act in the data security area, and

"Notable 2014 developments in two key cases underscore the FTC's expanding reach into the cybersecurity realm."

whether the FTC must promulgate interpretive rules before taking such enforcement action, will be among the most highly anticipated privacy and data security developments of 2015.

Many groups are interested in the outcome of this case: data privacy and consumer advocacy groups have filed *amicus* briefs in support of the FTC, urging the Third Circuit to uphold the district court ruling, while industry groups, including the U.S. Chamber of Commerce, have urged the Third Circuit to overrule the lower court's decision and side with Wyndham. The FTC and Wyndham continue to spar over discovery issues in the lower court while the appeal is pending—which has the potential to cast light on internal FTC enforcement guidelines in this area (or its lack thereof)—and recently have been ordered into mediation by the federal judge.

Following in Wyndham's footsteps, defendant LabMD is seeking to halt a 2013 FTC enforcement action against it that arises out of the FTC's claims in an administrative proceeding that LabMD failed to reasonably protect consumer electronic personal health information by, among other things, insufficiently training employees, failing to maintain a comprehensive information security program and failing to adequately secure its networks against intrusion. In January 2014, the FTC unanimously denied LabMD's bid to dismiss the administrative complaint based on arguments that the Health Insurance Portability and Accountability Act of 1996 precludes FTC privacy and data security enforcement action against covered entities and business associates, and that the FTC's failure to establish rules interpreting the FTC Act's requirements in the data security context means that any enforcement action violates due process.

In addition to seeking dismissal from the FTC itself, LabMD had, in late 2013, filed actions in both the U.S. District Court for the District of Columbia and

the U.S. Court of Appeals for the 11th Circuit seeking to derail the FTC's enforcement action. In the space of two days in February 2014, an 11th Circuit panel dismissed LabMD's petition on jurisdictional grounds, and LabMD voluntarily dismissed its district court case. The following month, LabMD filed a new lawsuit in Georgia federal court, and the FTC moved to dismiss that lawsuit a few weeks later. The court sided with the FTC in May, dismissing the case on grounds that the FTC's January decision denying LabMD's motion to dismiss did not constitute final agency action. LabMD appealed that decision back to the 11th Circuit, which received briefing over the summer and in August decided that it would hear oral argument in the case. Its decision, like the Third Circuit's in *Wyndham*, is likely to be among the most important privacy and data security enforcement developments in 2015. For the latest on such developments, visit McDermott's Of Digital Interest blog at www.ofdigitalinterest.com.

The underlying administrative proceedings against LabMD are ongoing and have been fraught with spectacle. In fact, the relationship between the FTC and a third-party company that provided it with one of the key pieces of evidence about LabMD's alleged lack of data security precautions has even become the subject of congressional inquiry—interrupting the administrative trial in June.

While appellate court guidance in 2015 is likely to shape the future bounds of the FTC's enforcement authority in the privacy and data security area, the FTC has not slowed its enforcement efforts while awaiting such guidance. To the contrary, it entered into or finalized numerous settlement agreements with companies over data security issues in the past year:

- In December 2013, with Goldenshores Technologies, LLC, resolving allegations that the company's Brightest Flashlight application for Android devices "deceived consumers about how their geolocation information would be shared with advertising networks and other third parties" (20-year consent decree, requiring policy and procedure changes, but no monetary payment or independent monitoring)
- Also in December 2013, with Accretive Health, Inc., resolving allegations that the medical billing and hospital revenue management company maintained "inadequate data security measures" that "unfairly exposed sensitive consumer information to the risk of theft or misuse" (20-year consent decree, requiring policy and procedure changes and independent biennial audits, but no monetary payment)
- In January 2014, with GMR Transcription Services, Inc., resolving claims that the medical transcription company's "inadequate data security measures unfairly exposed the personal information of thousands of consumers on the open [i]nternet, in some instances including consumers' medical histories and examination notes" (20-year consent decree, requiring policy and procedure changes and independent biennial audits, but no monetary payment)
- In February 2014, with TRENDnet, Inc., over purportedly "lax security practices" with respect to the company's web cameras that "led to the exposure of the private lives of hundreds of consumers on the internet for public viewing" (20-year order, requiring policy and procedure changes and independent biennial audits, but no monetary payment)
- In March 2014, with rent-to-own retailer Aaron's, Inc., resolving allegations that the company "knowingly played a direct and vital role in its franchisees' installation and use of software on rental computers that secretly monitored consumers, including taking webcam pictures of them in their homes" (20-year order, requiring policy and procedure changes, but no monetary payment or independent monitoring)
- Also in March 2014, with Fandango and Credit Karma, resolving claims that the companies' mobile applications did not protect consumers' personal information from interception by third parties and that the companies misrepresented the security of their mobile applications to consumers (20-year order for each company, requiring policy and procedure changes and independent biennial audits, but no monetary payment)
- In May 2014, with Snapchat, resolving allegations that the company "deceived consumers with promises about the disappearing nature of messages sent through [its messaging] service"

"In April 2014, the New Jersey federal judge issued a landmark ruling denying Wyndham's motion to dismiss."

and also "deceived consumers over the amount of personal data it collected and the security measures taken to protect that data from misuse and unauthorized disclosure" (20-year consent order, requiring policy and procedure changes and biennial independent audits, but no monetary payment)

- In September 2014, with Yelp Inc. and TinyCo, Inc., resolving claims that each company "improperly collected children's information" through various mobile applications, in violation of the Children's Online Privacy Protection Act Rule (federal court consent judgment for each company, with injunctive provisions requiring policy and procedure changes for the next 10 years, plus a $450,000 civil penalty for Yelp and a $300,000 civil penalty for TinyCo)
- In October 2014, a $10.2 million settlement with multiple participants in an alleged "scam that sent unwanted text messages to millions of consumers, many of whom later received illegal robocalls, phony 'free' merchandise offers, and unauthorized charges crammed on their mobile phone bills," that also included numerous injunctive provisions memorialized in multiple federal court judgments
- In November 2014, with TRUSTe, Inc., resolving claims that the company "deceived consumers about its recertification program for [companies'] privacy practices, as well as perpetuated its misrepresentation [of itself] as a non-profit entity" (20-year consent decree, requiring policy and procedure changes and disgorgement of $200,000 in fee receipts, but no independent monitoring)
- Settlements with 14 U.S. companies over the course of the year, resolving alleged false claims by the companies that they complied with the U.S.-EU Safe Harbor Framework for international privacy protection

In 2015 the FTC likely will have another busy year in the privacy and data protection enforcement area, unless the *Wyndham* and *LabMD* appellate court decisions markedly reshape the present legal landscape by ruling against the agency. Companies can best position themselves with respect to the FTC and other regulators in this area by carefully comparing their privacy and data protection practices both to industry best practices and to their own public disclosures. The FTC's enforcement focus is likely to remain on firms the agency perceives to have fallen behind industry norms for technological safeguards and consumer transparency—particularly for purposes of increasing profitability—and especially on firms it believes have deceived consumers by making privacy and security disclosures that do not match actual practices.

FTC: Don't Act Like a Jerk

Manoj Khandekar and Heather Egan Sussman

In April 2014, the Federal Trade Commission (FTC) accused the operator of Jerk.com of misrepresenting to users the source of the personal content that Jerk.com used for its purported social networking website and the benefits derived from a user's purchase of a Jerk.com membership. This case is a lesson for operators of online sites and services: be transparent and truthful about your data collection practices and sources, or face the wrath of the FTC.

According to the FTC, Jerk.com improperly accessed personal information about consumers via Facebook, used the information to create millions of unique profiles identifying subjects as either "Jerk" or "Not a Jerk," and falsely represented that a user could dispute the label and alter the information posted on the website by paying a $30 subscription fee. The interesting issue in this case is the FTC's tacit enforcement of Facebook's privacy policies governing the personal information of Facebook's own users.

MISREPRESENTING THE SOURCE OF PERSONAL INFORMATION

Although Jerk.com represented that its profile information was created by its users and reflected those users' views of the profiled individuals, Jerk.com in fact obtained the profile information from Facebook. In its complaint, the FTC alleged that Jerk.com accessed Facebook's data through Facebook's application programming interfaces, which are tools developers can use to interact with Facebook, and downloaded the names and photographs of millions of Facebook users without consent. The FTC used Facebook's various policies as support for its allegation that Jerk.com improperly obtained the personal information of Facebook's users and misrepresented the source of the information. The FTC noted that developers accessing the Facebook

platform must agree to Facebook's policies, which include the following:

- Obtaining users' explicit consent to share certain Facebook data
- Deleting information obtained through Facebook once Facebook disables a developer's Facebook access
- Providing an easily accessible mechanism for consumers to request the deletion of their Facebook data
- Deleting information obtained from Facebook upon a consumer's request

Jerk.com used the data it collected from Facebook not to interact with Facebook but to create unique Jerk.com profiles for its own commercial advantage.

MISREPRESENTING THE BENEFITS OF SUBSCRIPTION

According to the FTC, Jerk.com represented that purchase of a $30 subscription would enable users to obtain "premium features," including the ability to dispute information posted on Jerk.com, alter or delete their Jerk.com profile, and dispute false information on their profile. Users who paid the subscription often received none of the promised benefits. The FTC noted that contacting Jerk.com with complaints was difficult for consumers, because Jerk.com charged users $25 to e-mail the customer service department.

A hearing is scheduled for January 2015. Notably, the FTC's proposed order enjoins Jerk.com from using in any way the personal information that Jerk.com obtained prior to the FTC's action—meaning the personal information that was obtained illegally from Facebook.

FTC Issues Report on Data Broker Industry, Calls for Legislation

Julia Jacobson, Manoj Khandekar and Scott Weinstein

In late May 2014, the Federal Trade Commission (FTC) released its study of data brokers, the industry responsible for amassing and analyzing big data. The study, "Data Brokers: A Call for Transparency and Accountability" (Data Broker Report), describes what the FTC found when it "pulled back the curtain" on how the big data industry operates.

The FTC's interest in the data broker industry is no surprise. One year before issuing the Data Broker Report, the FTC participated in a worldwide data privacy sting organized by the Global Privacy Enforcement Network. Following this operation, the FTC announced that it had sent warning letters to 10 data brokers that were willing to sell consumer information without abiding by the requirements of the Fair Credit Reporting Act.

The Data Broker Report divides data broker services into three categories, noting that each of the nine data brokers studied operates within one or more of these categories:

- Marketing products, which include information about customers' interests, analytics tools or marketing scores
- Risk mitigation products, which enable data broker clients to verify customers' identities or detect fraud
- People search products, which aggregate publicly available data sources to create a data set used by businesses and consumers alike to track someone down

The FTC also learned that data brokers collect data from three main sources: government sources; other publicly available sources, including social media, blogs and the internet; and commercial sources, such as retailers and catalog companies. The data brokers not only use the raw data they obtain from these sources, but also make inferences from the raw data to create derived data. For example, a data broker may infer that a consumer who purchases a magazine about home improvement is a homeowner.

Even though the Data Broker Report considers each of these three product categories separately, the risks arising from each category overlap.

LACK OF TRANSPARENCY AND INCREASING INDUSTRY COMPLEXITY

The Data Broker Report expresses concern that consumers do not understand data brokers' data collection activities, finding that "Consumers are largely unaware that data brokers are engaging in these practices and, to the extent that data brokers offer consumer explanations and choices about how the data brokers use their data, their information may be difficult to find and understand." Data

brokers collect from many sources and from each other, creating a complex web of data collection and sharing that is nearly impossible to unwind. Further, data brokers have varying methods for assessing the reliability of source information. Only two of the nine data brokers investigated require the data source to promise that either it or its sources provided consumers with notice about information-sharing practices and an opportunity to opt out of sharing.

POTENTIAL FOR DISCRIMINATION

The Data Broker Report echoed the White House's concern that using inferences from data to profile customers may cause discrimination, intentionally or unintentionally, on the basis of race, ethnicity, age, economic standing or health status: "a client [of a data broker], for example, can request a list of consumers who are 'Underbanked' or 'Financially Challenged' in order to send them an advertisement for a subprime loan or other services." Although such targeting may be legal, the FTC reasons that, at a certain point, the placement of a person into one of these categories (a classification that may or may not be accurate) might affect that person's ability to obtain products or services because they don't receive marketing materials about such services.

LACK OF CONSUMER CONTROL OVER DATA COLLECTION AND USE

One of the key concerns expressed by the FTC is the absence of consumer control over data collection and use in the data broker industry, particularly for marketing products. The FTC recommends legislation creating a "centralized mechanism, such as an [i]nternet portal," that consumers could access to learn about data broker information collection (including the fact that data brokers derive inferences from the data they collect), and that would enable consumers to learn how to opt out from having data brokers use such information for marketing purposes. For risk mitigation products, the FTC recommends requiring the consumer-facing company to identify the data brokers upon which it relied in making any decision that adversely affects a consumer's ability to complete a transaction or obtain a benefit. The FTC also recommends transparency about data sources. As discussed in "Consumer Health Information" on page 35, the FTC would like Congress to protect sensitive information, such as certain health information, by requiring data sources to obtain affirmative consent before collecting and sharing such information with data brokers.

DOWNSTREAM THIRD-PARTY ACCESS TO DATA

Although some of the studied data brokers signed contracts with their clients that described the permitted and prohibited uses of the data products, the FTC is concerned that downstream entities receiving data from data brokers (rather than directly from the data source, *i.e.*, consumers) could use the data illegally in ways that harm consumers—for example, to make eligibility determinations and to discriminate. Consequently, the FTC recommends that data brokers take reasonable precautions to ensure that downstream users of their data do not use it for eligibility determinations or for unlawful discriminatory purposes.

SECURITY RISKS FROM UNLIMITED DATA RETENTION

Some data brokers store information indefinitely. The FTC raised concerns that "unscrupulous actors" might be attracted to these data storehouses that offer profiles of consumers' habits over time and thereby enable the prediction of passwords, challenge questions or other authentication credentials. The FTC recommends that, to the extent practical, data brokers collect only the data they need and securely dispose of data as it becomes less useful.

COMMENT

Not surprisingly, industry groups criticized the Data Broker Report. In particular, critics noted that the FTC's study did not find evidence of actual harm to consumers, and that the efforts of many data brokers to provide consumers access to and choice concerning their data obviates the need for Congress to pass legislation. While congressional action is uncertain, increased FTC scrutiny and possible enforcement actions likely await the data broker industry in 2015.

EU-U.S. Safe Harbor Program

Ann Killilea

It has been a controversial year for the EU-U.S. Safe Harbor Program. Some EU data protection authorities expressed disdain for U.S. government surveillance and voiced concerns about third-party access to

personal data transferred from the European Union to the United States. They questioned the effectiveness of the EU-U.S. Safe Harbor Program, designed to protect EU personal information consistent with the requirements of the EU Data Protection Directive, and threatened to suspend the program.

Despite pressure from the European Parliament to suspend the program, the European Commission did not do so and instead offered 13 recommendations intended to improve the data-transfer program in late 2013. One of the recommendations asked for increased Federal Trade Commission (FTC) enforcement of Safe Harbor commitments made by certified companies, and emphasized that the European Union is watching the FTC closely for an enforcement response.

In March 2014, the European Parliament passed a resolution calling for immediate suspension of the Safe Harbor framework. The predicate for this resolution is that "companies identified by media revelations as being involved in the large-scale mass surveillance of EU data subjects by the U.S. NSA are companies that have self-certified their adherence to the Safe Harbour."

THE FTC'S ENFORCEMENT ACTIONS

Prior to 2014, the FTC reached 10 Safe-Harbor-related settlements, including some settlements that addressed substantive violations of the Safe Harbor Program. One year ago, prior to the European Commission's 13 recommendations, FTC Chairwoman Edith Ramirez noted that "[e] nforcement of the U.S.–EU Safe Harbor framework is a Commission priority." Since January 2014, the FTC has announced settlements with 14 companies. The complaints primarily allege that the companies deceptively claimed, either through statements in their privacy policies or by displaying the Safe Harbor certification mark on their websites, that they held current certifications under the Safe Harbor framework, when in fact they had allowed their certifications to lapse. The FTC has focused its recent Safe Harbor enforcement attention on these lapsed certification cases rather than on substantive violations of the privacy principles.

On August 13, 2014, the CDD filed an extensive brief-like "Request For Investigation" challenging the FTC to investigate Safe Harbor violations by 30 companies involved in data marketing and data profiling activities.

The 30 companies targeted by the CDD's filing include data brokers, data management platforms, data profilers and mobile marketers. The CDD states that these companies engage in "commercial surveillance of EU consumers . . . without consumer awareness or meaningful consent." It asserts that these companies use and share EU consumers' personal information to create digital profiles and analyze each consumer's behavior, and to make marketing and related decisions regarding each individual. The CDD states that its filing provides "factual information and legal analysis on probable violations of Safe Harbor commitments that materially mislead EU consumers." These purported violations do not fit the pattern of FTC enforcement to date.

The CDD filing articulates five major themes regarding alleged "patterns of deception." The filing asserts that the companies in question do the following:

- Fail to adequately disclose their actual data collection practices in their privacy policies and Safe Harbor declarations
- Misrepresent legal facts of importance to EU consumers by claiming that they are only acting as data processors (subject to less stringent EU regulatory obligations) and not as data controllers
- Fail to provide meaningful, easy-to-find opt-out mechanisms that EU consumers can use to stop the collection and use of their personal data
- Create the misleading impression that, because the companies may not collect a consumer's name or government-issued ID number, they only collect and use anonymous or non-personal data
- Merge with and acquire other companies to expand their data collection and profiling abilities, but fail to disclose these business events adequately to EU consumers

The CDD supplemented its filing with draft complaints crafted for each of the 30 companies. These draft complaints scour each company's corporate websites, product data sheets, financial reports to the U.S. Securities and Exchange Commission (SEC), and other publicly available materials for personal-data-

"Pressure on the FTC to enforce the Safe Harbor Program undoubtedly means pressure on companies to ensure proper compliance."

related representations. These complaints provide the FTC with all relevant company representations and articulate in detail why the representations are non-compliant or false. Further, based on this evidence and analysis, each draft complaint contains a customized recitation of the possible Safe Harbor violations.

"These are the largest price tags in FCC history."

The CDD's filing, accurate or not, puts added pressure on the FTC to examine these companies for violations of their Safe Harbor commitments. The FTC has not yet publicly responded to this challenge, but in this situation, silence likely precedes action. The CDD's challenge will not go unanswered by the FTC, and the European Union will continue to watch the FTC for a robust response.

NEXT STEPS

While it is unclear what else the FTC may have planned, pressure on the FTC to enforce the Safe Harbor Program undoubtedly means pressure on companies to ensure proper compliance. The FTC likely will answer the CDD's challenge and appropriate its investigatory work to probe the practices of these targeted data mining and data broker companies. Any Safe Harbored company therefore should take the following steps:

- Recertify its Safe Harbor status prior to the annual recertification date and ensure that its status is marked "current" on the U.S. Department of Commerce website
- Remove all references to the Safe Harbor program from publicly available privacy policies and statements if the company's certification status is unclear
- Review all publicly available materials, corporate websites, marketing collateral and SEC disclosures to ensure that any representations are in line with the Safe Harbor principles, particularly the notice, choice and onward transfer requirements
- If a company engages in data mining and data tracking activities and is not one of the 30 companies named in the CDD filing, conduct this review urgently and ensure that any statements that do not accurately indicate how data is used, and to whom it is provided, are removed or revised immediately
- Ensure that "personal data" is defined broadly to include data elements that by themselves do not identify any individual but can be re-engineered to locate an individual, disclose an individual's identity, or locate or contact an individual's device
- Refrain from assuring users that certain data elements are anonymous and not personally identifiable, because such representations are becoming suspect and may be deemed to be misleading if such data can be re-engineered to re-identify an individual or contact an individual's device

The drama surrounding the Safe Harbor Program continues to create uncertainty for well-intentioned multinational companies seeking to legitimize their data transfers and choosing Safe Harbor as their preferred compliance method. Yet, the Safe Harbor Program motivates companies to develop corporate-wide data protection programs compliant with the EU Data Protection Directive, and for that deserves continued applause.

FCC Cracks Down on Consumer Privacy Violations

Marcos Daniel Jiménez, Audrey Pumariega and David A. Roller

Failing to protect customers' private information is not just bad public relations; now more than ever, it could lead to hefty fines. Federal Communications Commission (FCC) fines for data breaches recently have increased dramatically, as the FCC expands its focus beyond technical data to personally identifiable information (PII). In view of these developments, the increasing transition of data storage to offsite locations and the migration of data to cloud-based services accessed by mobile devices, protecting data should be a top priority for business leaders.

FCC AND FTC AUTHORITY

The Communications Act of 1934 and the Telecommunications Act of 1996 charge the FCC with regulating, monitoring and enforcing various guidelines in the telecommunications industry. Until recently, the FCC's main focus was customer proprietary network information (CPNI). CPNI is mostly the technical data associated with a mobile consumer's phone use, including phone numbers

called, call duration and location at the time of a call. Information such as social security numbers, addresses and driver's license numbers is PII that historically has been within the Federal Trade Commission's (FTC's) purview.

RECENT FCC ACTIVITY

Despite increasing enforcement activity over the past five years, the FCC has focused primarily on CPNI infractions in relatively small cases. That changed in September and October 2014, when the FCC announced a $7.4 million settlement with Verizon for alleged CPNI infractions, and a $10 million forfeiture against TerraCom and its affiliate, YourTel America, for alleged PII violations. These are the largest price tags in FCC history.

The TerraCom/YourTel forfeiture is significant not just because of its dollar figure, but because it is the first time the FCC has addressed PII violations. In a Notice of Apparent Liability, the FCC relied on the word "privacy" in two section headings in the Communications Act to drastically expand the scope of CPNI to include any proprietary information.

This controversial decision prompted two FCC commissioners to dissent. One commissioner criticized the FCC's "novel legal interpretations," and another commented on the FCC's "shaky legal ground" in using section headings as a source of authority. Both commissioners expect future litigation in response to the FCC's decision.

The Telephone Consumer Protection Act

Matthew L. Knowles and Matthew R. Turnell

The year 2014 has seen a continued stream of large settlements and proposed settlements in cases filed under the Telephone Consumer Protection Act (TCPA), including cases against Capital One ($75.5 million), Bank of America ($32 million), Discover Financial Services ($8.7 million) and Vivint Home Security ($6 million). Many other putative TCPA class actions are settled confidentially on an individual basis.

While some cases involve debt collection or other calls to leads that were generated "organically" by the business placing the calls, many TCPA cases stem from leads sold by data brokers. Placing calls to these leads using automatic dialers or artificial voice equipment can be perilous. Data brokers' assurances of proper consent and TCPA compliance are comforting until a company faces a multimillion

dollar TCPA class action, at which point a broker's representations alone will do little to satisfy aggressive plaintiffs' lawyers.

THE PROBLEM: TCPA AND DATA BROKERS

The TCPA's basic requirements should be well known to businesses that operate call centers. It is unlawful to place a call to a mobile number using an automatic telephone dialing system or an artificial or pre-recorded voice without the prior express written consent of the party called. Likewise, prior express consent is required for telemarketing calls to residential lines made with an artificial or pre-recorded voice.

The Federal Communications Commission's 2012 TCPA rulemaking, which took effect in October 2013, increased the degree of consent required for calls to mobile numbers: express consent must now be written. Likewise, several recent decisions have emphasized that the consent required is that of the called party, rather than the person whom the caller intended to reach. This distinction is crucial when dealing with leads that might not reflect whether a number has changed hands or been ported to a mobile phone. Indeed, the most serious risk comes with calls placed to mobile numbers using an artificial telephone dialing system, because the prohibition on such calls is both the broadest and the most litigated aspect of the TCPA's rules relating to voice calls. When purchasing leads, it is common for entities to require that the leads be "TCPA compliant" or that the data broker secure prior express consent for each lead. The realities of litigation, however, show that these contractual representations alone are not enough.

Under the TCPA, the burden is on the caller to prove consent. It doesn't matter whether the data broker (or whomever the caller obtained the lead from) secured the required consent unless the caller can prove it when a lawsuit arises. Likewise, the consent must be broad enough to permit a call from the caller in question, not just the entity that collected the number in the first place. In an industry where data brokers collect and sell millions of leads each month, the detail required to prove consent for each call can be a major hurdle.

SOLUTIONS: MITIGATING TCPA RISK

A careful plan to avoid TCPA violations and document consent for calls can help make a business a less attractive target for class action plaintiffs. The first and most important step is to avoid placing calls that will draw TCPA scrutiny in the first place. Callers should identify cell phone numbers (*e.g.*, by scrubbing leads with a cell block) and not place autodialed calls to those numbers. Likewise, when dialing residential numbers, callers should avoid using an artificial or pre-recorded voice.

The next layer of defense is to keep clear evidence of how each call was made and the consent for each lead. Contracts with data brokers should set out in detail the required disclaimers and other consent requirements for the leads. Callers should also capture screen shots and otherwise document the consent disclosures on the websites from which leads are gathered. This documentation is particularly useful early in the life of a putative TCPA class action, because it can help convince plaintiffs that the case will be long and fact-intensive, and that they should find a more vulnerable target.

Contracts with data brokers also should include clear indemnification and defense language. While such terms come at a premium, giving the data broker a stake in the risk will help ensure that the broker does everything possible to comply with TCPA. Data brokers operate in a commoditized and fast-paced industry, however, and there is no assurance that a broker will be extant (and solvent) when a claim arises. Instead of relying on contractual indemnity alone, callers should secure a robust and TCPA-specific insurance policy to help mitigate their risk.

COMMENT

Data brokers are here to stay. Businesses that run call centers are increasingly seeking higher quality leads to maximize their sales while minimizing the costs of call center operations. Settlements and new litigation during 2014 show that TCPA liability can be an existential threat to smaller businesses and a major legal risk to even the largest companies, particularly when leads are purchased through data brokers. By taking careful steps to limit TCPA liability, callers can mitigate risk and make their businesses a less attractive target for TCPA plaintiffs.

The Children's Online Privacy Protection Act

Julia Jacobson and Manoj Khandekar

The Federal Trade Commission (FTC), which is responsible for enforcing the Children's Online Privacy Protection Act (COPPA), implemented regulations in April 2000 known as the COPPA Rule. In December 2012, the FTC issued an amended COPPA Rule that became effective July 1, 2013. Several 2014 developments in the wake of the amended COPPA Rule are worth noting.

TWO NEW COPPA SAFE HARBOR PROGRAMS APPROVED

In general, COPPA and the COPPA Rule prohibit operators of websites, mobile applications or other digital services (collectively, digital services) from knowingly collecting personal information from children under age 13 unless and until the digital service operator has verifiable parental consent (VPC). A digital service operator must make "reasonable efforts" to obtain VPC and may use any method to obtain VPC that is "reasonably calculated to ensure that the person providing consent is the child's parent." The COPPA Rule provides for four "non-exhaustive" VPC methods, and the FTC also considers requests for approval of VPC methods. The FTC-approved VPC methods often are referred to as Safe Harbor programs.

In 2014, the FTC announced its approval of two new VPC methods: the kidSAFE Seal Program (in February) and the Internet Keep Safe Coalition (iKeepSafe) (in August). With the addition of these two new Safe Harbor programs, businesses can choose from seven Safe Harbor program options. Having more options is helpful for a business with a digital service subject to COPPA, especially given the complexities of COPPA compliance in general and obtaining VPC in particular.

STUDENTS' PERSONAL INFORMATION

In July 2014, the FTC released updates to its COPPA FAQs to address (among other things) the issue of student privacy. The FTC offered guidance about when an educational institution can consent on a parent's behalf to collection of personal information from students under age 13 through a digital service. The COPPA FAQs explain that an educational institution can give this consent if the information collected is for the use and benefit of the educational institution (*e.g.*, for homework help lines, individualized educational modules, and online research and organizational tools) and not for any commercial purpose. When an educational institution provides consent on behalf of parents, digital service operators may rely on its consent as long as the method of obtaining consent is reasonably calculated to ensure that it is actually the educational institution providing consent (and not, say, a child pretending to be a teacher or a principal). The digital service operator also must comply with all of COPPA's other requirements.

A BAD REVIEW FOR YELP

In September 2014, the FTC announced a settlement under COPPA with Yelp, the online service through which consumers can read and write reviews about local businesses. Under the settlement, Yelp agreed to pay $450,000 to settle the FTC's charges that Yelp knowingly and without VPC collected personal information from children under the age of 13 through its mobile app in violation of COPPA. Under the amended COPPA Rule, COPPA has a broader scope than digital service operators might realize. COPPA applies not only to digital services that are directed to children, but also to any general-audience digital service when the operator of the digital service has "actual knowledge" that the service is collecting personal information from children under age 13 without VPC. COPPA does not require operators of general-audience digital services to ask users for age or date of birth information. Under the actual-knowledge test, however, if the digital service collects information that establishes that a user is under 13, the digital service must be COPPA compliant, which means obtaining VPC before collecting personal information from the under-age-13 user. The FTC concluded that Yelp had actual knowledge that it was collecting personal information from children under age 13 because the registration page on Yelp's app asked users to enter their date of birth but did not block access to the app for users who were too young (*i.e.*, under age 13).

The Yelp settlement is a warning to digital service operators: if a general-audience digital service asks a user for his or her birth date, any user who supplies a birth date that indicates he or she is under age 13

"With the addition of these two new Safe Harbor programs, businesses can choose from seven Safe Harbor program options."

must be blocked from using the digital service. Other helpful age screening tips are as follows:

- Request birth date in a neutral manner, without indicating the age of eligibility—*i.e.*, avoid statements such as "You must be age 13 or older to register."
- Present a neutral onscreen error message when a user is under age 13, such as "Sorry, you are not eligible," rather than "Sorry, you are under age 13."
- Deploy a cookie or other functionality to prevent an underage user whose access was blocked from using the back button (or similar technique) to re-enter a different birth date.

Update on State Law Enforcement

David Quinn Gacioch

"The FCC also stepped up its enforcement related to privacy and data security."

In 2014, the Federal Trade Commission (FTC) continued to solidify its role as the leading U.S. enforcement authority on privacy and data protection issues. State attorneys general and the U.S. Department of Health and Human Services Office for Civil Rights (OCR) continued to play the important parallel roles they have developed in recent years, with the attorneys general expanding their use of joint, multi-state investigations. Perhaps most notably, other regulators such as the U.S. Securities and Exchange Commission (SEC) and the Federal Communications Commission (FCC) joined the fray, underscoring the ever-growing scope of privacy and data security issues and their importance to the broader U.S. economy.

This article briefly recaps the highlights of the last 12 months of non-FTC enforcement activity in the United States and concludes with steps that privacy professionals, as well as lawyers and business leaders more generally, can take to minimize the chance of enforcement activity against their organizations and to best position their organizations should such activity nonetheless occur.

STATE ATTORNEYS GENERAL: EXPANDED FOCUS ON JOINT ENFORCEMENT ACTIVITY

In 2014, the attorney general offices (AGOs) of several U.S. states continued to investigate (and occasionally settle) allegations around data breaches and other privacy issues. Notably, 2014 saw a significant uptick in reported joint, multi-state investigations as the number of breaches reported by large organizations and affecting millions of consumers shot up.

In January, AGO representatives from Connecticut, Florida, Illinois, Massachusetts and New York announced that they (apparently alongside AGOs from dozens of other states) were jointly investigating the massive Target, Neiman Marcus and Michaels Stores payment card system intrusions that occurred during the 2013 holiday season.

A similar multi-state investigation of an Experian business unit called Court Ventures and its data-sharing partner U.S. Info Search was announced in April, involving the AGOs of Connecticut, Illinois, Iowa, Massachusetts and possibly other states. The investigation concerned allegations that the companies had allowed access to social security numbers, bank account information and other sensitive data for more than 200 million U.S. consumers to a Vietnamese man pretending to be a private investigator, after which the man resold the data to others purportedly engaged in hacking and identity theft activities.

In May, the Connecticut, Florida and Illinois AGOs quickly launched investigations into a cyberattack that eBay had announced could affect as many as 145 million of its users. According to eBay, the attack had targeted a database containing user passwords along with several other categories of personally identifiable information, and had been perpetrated via compromised employee log-in credentials. New York Attorney General Eric Schneiderman also commented on the incident, calling for eBay to provide free credit monitoring services to all affected consumers.

In September, the California, Connecticut, Illinois, Iowa, Massachusetts and New York AGOs (likely among several others) launched a joint investigation into a malware-based breach at Home Depot that targeted payment card information for 56 million customers in the United States and Canada, along with 53 million customer e-mail addresses, stemming from network access obtained through a third-party vendor's log-in credentials.

The same month, the Illinois AGO announced that it was leading a multi-state investigation into a data breach involving 216 Jimmy John's sandwich shops across 37 states.

In October, the Connecticut and Illinois AGOs announced an investigation into a cyberattack on JPMorgan Chase that had occurred over the summer, parallel to a Federal Bureau of Investigation probe that had started several weeks earlier. Shortly before the AGO announcements, JPMorgan Chase disclosed that the attack had compromised contact information for approximately 76 million individual customers and seven million small business customers.

Later the same month, the Connecticut AGO announced an initial inquiry into the October 21 announcement by Staples Inc. of a "potential issue involving credit card data." Other AGOs are expected to join this inquiry as it progresses.

All of the aforementioned investigations remain ongoing as of the date of publication.

The largest single-jurisdiction enforcement action related to privacy and data protection in 2014 belonged to the Puerto Rico Health Insurance Administration, which in February notified contractor Triple-S Salud, Inc., of its intention to impose a $6.8 million civil monetary penalty and other sanctions in the wake of a 2013 breach in which the Medicare health insurance claim numbers of approximately 70,000 Medicare beneficiaries were improperly exposed in mailings. This proposed sanction, to be levied on the basis of Health Insurance Portability and Accountability Act of 1996 (HIPAA) related provisions in the Health Insurance Administration's contract with Triple-S, exceeds by a significant margin any HIPAA-based settlement or imposed penalty amount to date. Triple-S has contested the penalty, and the case presently is pending in the U.S. District Court for the District of Puerto Rico.

Other 2014 state settlements in the privacy and data protection area included the following:

- The New Hampshire Bureau of Securities Regulation settling with Edward D. Jones & Co., L.P., (for $750,000 plus policy and procedure changes) allegations that the company made unsolicited telephone calls to individuals who had placed themselves on the national Do-Not-Call list
- The Maryland AGO following the FTC's lead in settling with Snapchat (for $100,000 plus required disclosure enhancements) over allegations that the company deceived consumers about whether their messages on its system could be saved by other users
- The Massachusetts AGO's July settlement with a Rhode Island hospital (for $150,000 plus policy and procedure changes) over the 2012 loss of unencrypted back-up tapes allegedly containing personal and protected health information of approximately 12,000 Massachusetts residents
- The Vermont AGO's July settlement with a local country store operator (for $3,000 plus policy and procedure changes) over the latter's purported failure to timely report a 2013 website intrusion that allegedly compromised the payment card information of more than 700 customers
- The California AGO's January settlement with a leading health insurance provider (for $150,000 plus policy and procedure changes) over allegations that the insurer took too long (four months) to notify more than 20,000 current and former employees of a 2011 data breach involving their social security numbers and other personal information
- A multi-faceted $28.4 million settlement announced in October between the California AGO and rent-to-own giant Aaron's, Inc., that dealt in part with allegations that Aaron's had allowed its franchisees to install software on rented laptop computers that would allow them to spy on consumers in various ways

Finally, several state AGOs took other steps this year to raise their profiles in the privacy and data protection area, such as testifying before Congress (Illinois), issuing guides to various stakeholders on compliance with disclosure requirements and protection against data breaches (California), filing "friend of the court" briefs in litigation brought by private plaintiffs (California), publicly seeking meetings with leading companies to discuss privacy concerns about new products (Connecticut) and issuing summary reports around data breach incidents (California, Illinois, New York and others).

OTHER AGENCIES ENTERING THE PRIVACY AND DATA PROTECTION ENFORCEMENT ARENA

Several new regulators threw their hats into this increasingly crowded ring in 2014. For example, after having issued lower-level guidance in 2011 to public companies around disclosure and reporting of data-related incidents and threats, the SEC in April 2014 announced that it would test the readiness of broker-dealers and investment advisers it regulates to deal with cyberattacks on data in their charge. SEC Commissioner Luis Aguilar followed that announcement up with comments directed at the importance of data security issues, and the responsibilities of corporate boards of directors to proactively address them, at a New York Stock Exchange conference in June. While no formal SEC enforcement actions in this space have been publicly announced yet, they are likely to appear sooner rather than later.

The FCC also stepped up its enforcement related to privacy and data security. The agency long has played an important role in implementing and enforcing the Telephone Consumer Protection Act and the national Do-Not-Call registry, and levied multimillion-dollar fines under both regimes in 2014. In September and October, however, the agency made an unprecedented foray into other areas of privacy and data protection with its $7.4 million settlement with Verizon and its $10 million fine on TerraCom and YourTel America, along with its announcement that it was joining the Global Privacy Enforcement Network alongside the FTC. See "FCC Cracks Down on Consumer Privacy Violations" on page 14 for more information on recent FCC developments.

The Consumer Financial Protection Bureau also received at least one enforcement referral from an arm of the advertising industry's self-regulatory body over concerns about SunTrust Banks, Inc.'s practices with respect to tracking the online activities of users of its website. The U.S. Department of Health and Human Services Office of Inspector General recently put HIPAA Security Rule compliance on its 2015 investigation priorities list (following its 2014 focus on appropriate safeguards for medical devices that collect sensitive personal information about patients). Even the Federal Aviation Administration has taken steps to police the use of unmanned aerial vehicles for purposes such as aerial photography.

KEY TAKEAWAYS

Increasing numbers of reported data-related incidents affecting larger numbers of consumers are attracting more U.S. regulatory agencies and regulatory

budget dollars to the privacy and data protection area. Companies that collect, store, use and transmit sensitive consumer information—even those that do nothing more than accept payment cards—should expect multi-layered regulatory scrutiny in the event of any breach or whistleblower complaint. It remains true, however, that only a very small percentage of reported data-related incidents lead to formal regulatory enforcement actions or settlements. Most such incidents are not investigated at all beyond review of the initial breach report, or are resolved quickly with regulators providing technical assistance.

The keys to remaining off of the regulatory radar screen and securing favorable outcomes when incidents do arise remain the same as in past years:

- Dedicate the necessary time and resources to ensure compliance with applicable law and industry-standard practices before a breach occurs.
- Practice what your privacy disclosures preach.
- In the event of an incident, act quickly to gather the key facts and to make notifications.
- Be cooperative where possible, but stand firm on legal and factual issues where such stands are justified.

Illinois Attorney General Lisa Madigan summed this advice up well when she told Congress in February that state AGOs typically focus their investigations on whether companies took "reasonable steps" to protect customers' data before a breach and whether those companies notified their customers within a reasonable time period after the breach occurred. Companies should consult counsel experienced in the privacy and data protection requirements governing their specific industries and operating geographies in order to most effectively and efficiently put this guidance into practice.

Florida Law Requires Businesses to Ramp Up Data Protection or Face Steep Penalties

Marcos Daniel Jiménez and Robert M. Kline

On July 1, 2014, the Florida Information Protection Act took effect and requires virtually every business that acquires an individual's personal information to implement policies and procedures to protect that information if it is kept in electronic form. It is critical that business owners both in and out of Florida appreciate the Act's broad definition of personal information. An individual's name combined with any of the following constitutes personal information:

- Social security number
- Driver's license number
- Passport number
- Government identification number
- Credit card or debit card number with security code or password
- Medical records
- Health insurance information

Notably, personal information even includes an online username or e-mail address "in combination with a password or security question and answer that would permit access to an online account."

In the event of a data breach, businesses must provide notice of the breach, with few exceptions, within 30 days to all affected and potentially affected individuals in Florida. If the breach affects 500 or more individuals in Florida, the business also must provide notice to the Florida Attorney General's Office (AGO) within 30 days of the breach. Notice to the AGO must include, among other things, a synopsis of the events surrounding the breach, the number of individuals in Florida who may have been affected by the breach and the steps taken to rectify the breach. If the data breach affects more than 1,000 individuals in Florida, the business must notify all consumer reporting agencies that compile and maintain files on consumers on a U.S.-wide basis, as defined in the Fair Credit Reporting Act. The Florida Information Protection Act imposes additional obligations on entities that have been contracted to maintain or process personal information on behalf of the government or another business.

Violations of the Act expose businesses to significant liability. For example, the AGO may fine a business up to $500,000 in civil penalties for failing to provide timely notice to individuals who are affected or potentially affected by a breach. Moreover, a violation of the Act

"It is critical that business owners both in and out of Florida appreciate the Act's broad definition of personal information."

may be grounds for a claim for actual damages under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA), which allows for treble damages and an award of attorney's fees to the prevailing party. In light of the ever-increasing frequency of cyberattacks and data breaches, the significant exposure created by the Act and the willingness of courts to certify class actions under FDUTPA, it is critical that businesses develop, document and implement comprehensive policies and procedures regarding the management of consumer records.

Large and small business owners alike that encounter personal information in the ordinary course of business should consult an experienced data privacy counsel regarding the Act. In the unfortunate but all too common event of a data breach, independent outside counsel can determine what notice to provide, when to provide it and to whom it must be provided. Such counsel also should communicate with the AGO on behalf of the business to provide an additional layer of credibility and, ideally, help the business avoid steep civil penalties.

Kentucky Becomes 47th State with a Data Breach Notification Law

Heather Egan Sussman

"The Kentucky law is similar to many other state breach notification laws."

On April 10, 2014, Kentucky became the 47th state to enact breach notification legislation. Under the new law, companies that conduct business in Kentucky and hold the consumer data of Kentucky residents will be required to disclose data breaches involving the unauthorized acquisition of unencrypted computerized data of Kentucky residents. Companies must disclose the breach in the "most expedient time possible" and "without unreasonable delay" to any state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The Kentucky law is similar to many other state breach notification laws. For example, the Kentucky law defines "personal information" as an individual's first name or first initial and last name in combination with either the individual's social security number; driver's license number; or account, credit or debit card number in combination with any required security or access code. In addition, the legislation permits companies to provide notification in written or electronic form through e-mail, major state-wide media or an alert on their website, and allows for the delay of notification if a law enforcement agency determines the action will impede its criminal investigation.

Notably, the law does not require notification to the state attorney general, but does require that notification be given to consumer reporting agencies and credit bureaus if the breach affects more than 1,000 individuals.

Now that Kentucky has a data breach notification law, only Alabama, New Mexico and South Dakota do not have a comprehensive notification law outside of the public sector.

Delaware Data Disposal Law Requires Action by Affected Businesses

Heather Egan Sussman and Manoj Khandekar

While the federal government continued its inaction on data security bills pending in Congress in 2014, some U.S. states were busy at work on this issue. A new Delaware law, H.B. 295, signed into law on July 1, 2014, and effective January 1, 2015, provides for a private right of action in which a court may order up to triple damages in the event a business improperly destroys personal identifying information at the end of its life cycle. In addition to this private right of action, the Delaware attorney general may file suit or bring an administrative enforcement proceeding against the offending business if it is in the public interest.

Under the law, personal identifying information is defined as a consumer's first name or first initial and last name in combination with any one of the following data elements that relate to the consumer, when either the name or the data elements are not encrypted:

- Signature
- Full date of birth
- Social security number
- Passport number, driver's license or state identification card number
- Insurance policy number
- Financial services or bank account number

- Credit card or debit card number
- Any other financial information
- Confidential health care information, including all information relating to a patient's health care history, diagnosis, condition, treatment or evaluation obtained from a health care provider that has treated the patient, that explicitly or by implication identifies a particular patient

This new law exempts from its coverage banks and financial institutions that are subject to the Gramm-Leach-Bliley Act. In contrast, it only exempts health insurers and health care facilities if they are both subject to and in compliance with the Health Insurance Portability and Accountability Act (HIPAA), and only exempts credit reporting agencies if they are both subject to and in compliance with the Fair Credit Reporting Act (FCRA).

Given how broadly the HIPAA and FCRA exemptions are drafted, plaintiffs' lawyers likely will argue for the private right of action and triple damages in every case where a HIPAA- or FCRA-covered entity fails to properly dispose of personal identifying information, arguing that such failure evidences non-compliance with HIPAA or FCRA, thus canceling the exemption. Some courts, however, have refused to allow state law claims of improper data disposal to proceed where they were preempted by federal law.

Companies that collect, receive, store or transmit the personal identifying information of residents of the state of Delaware (or any of the more than 30 states that have data disposal laws on the books) should examine their data disposal policies and practices to ensure compliance with these legal requirements. In the event that a business is alleged to have violated one of these state data disposal laws, it should consider all available defenses, including the potential for a preemption argument.

California Legislation Expands Privacy and Security Laws

A. Marisa Chun, Han (Jason) Yu and Kate Hammond

California continues to be a leader when it comes to protecting data privacy. At the end of September 2014, California Governor Edmund G. Brown, Jr., approved six bills designed to enhance and expand California's privacy laws. These new laws are scheduled to take effect in 2015 and 2016. Businesses should be mindful of the new laws and their respective requirements when dealing with personal information and responding to data breaches.

EXPANSION OF PROTECTION FOR CALIFORNIA RESIDENTS' PERSONAL INFORMATION – AB 1710

Under current law, any business that owns or licenses certain personal information about a California resident must implement reasonable security measures to protect the information and must notify affected persons in the event of a data or system breach. Current law also prohibits individuals and entities from posting, displaying or printing an individual's social security number, or requiring individuals to use or transmit their social security number, unless certain requirements are met.

Assembly Bill 1710 makes three notable changes to these laws. First, in addition to businesses that own and license personal information, businesses that maintain personal information must comply with the law's security and notification requirements. Second, in the event of a security breach, businesses must not only notify affected persons, but also provide "appropriate identity theft prevention and mitigation services" to the affected persons at no cost for at least 12 months, if the breach exposed or may have exposed specified personal information. Third, in addition to the current restrictions on the use of social security numbers, individuals and entities may not sell, advertise to sell or offer to sell any individual's social security number.

EXPANSION OF CONSTRUCTIVE INVASION OF PRIVACY LIABILITY – AB 2306

Under current law, a person can be liable for constructive invasion of privacy if he or she uses a visual or auditory enhancing device and attempts to capture any type of visual image, sound recording or other physical impression of another person in a personal or familial activity under circumstances in which that person has a reasonable expectation of privacy. Assembly Bill 2306 removes the limitation requiring the use of a "visual or auditory enhancing device" and imposes liability for the use of any type of device.

"Assembly Bill 2306 removes the limitation requiring the use of a 'visual or auditory enhancing device.' "

The law will continue to impose liability on those who acquire an image, sound recording or physical impression of a person, knowing that it was unlawfully obtained. Those found liable under the law may be subject to treble damages, punitive damages, disgorgement of profits and civil fines.

PROTECTION OF PERSONAL IMAGES AND VIDEOS ("REVENGE PORN" LIABILITY) – AB 2643

Assembly Bill 2643 creates a private right of action against a person who intentionally distributes by any means, without consent, material that exposes a person's intimate body parts or shows the person engaging in certain sexual acts, with knowledge that the victim had a reasonable expectation that the material would remain private.

THE STUDENT ONLINE PERSONAL INFORMATION PROTECTION ACT – SB 1177

The Student Online Personal Information Protection Act prohibits an operator of an internet website, online service, online application or mobile application that is used, designed and marketed primarily for K-12 school purposes from taking the following actions:

- Knowingly engaging in targeted advertising to students or their parents or guardians on the site, service or application
- Engaging in targeted advertising on a different site, service or application using any information that was acquired from the operator's site, service or application
- Using information created or gathered by the operator's site, service or application to generate a profile about a student
- Selling a student's information
- Disclosing certain information pertaining to a student

The Act also requires the operator to maintain reasonable security measures to protect the student's information from unauthorized access, destruction, use, modification or disclosure.

PROTECTION OF STUDENTS' SOCIAL MEDIA INFORMATION – AB 1442

Assembly Bill 1442 regulates the use of students' social media information. If a school intends to implement a program to gather students' social media information, the school must notify students and parents or guardians about the proposed program and provide an opportunity for public comment. If the program is adopted, the school must only gather or maintain information that pertains directly to school or student safety, provide the student with access to his or her information and an opportunity to correct or

delete such information, destroy information after the student turns 18 or is no longer enrolled at the school, and notify each parent or guardian that the student's social media information is being collected.

The law also imposes requirements on third parties that are retained by schools to gather students' social media information. Under the law, a third party may not use the information for any purpose other than to satisfy the contract, may not sell or share the information, and must destroy the information immediately upon conclusion of the contract.

PROTECTION OF STUDENTS' RECORDS IN DIGITAL STORAGE SERVICES – AB 1584

Assembly Bill 1584 permits a school to use a third party for the digital storage, management and retrieval of student records, or to provide digital educational software, or both. In order to protect student records, any contract with a third party must contain certain provisions, including a statement that all of the records remain the property of, and under the control of, the school; a description of the procedures that will be used to notify affected students, parents or guardians in the event of any unauthorized disclosure; a prohibition against using any student's information for any purposes other than those required by the contract; and a certification that students' information will not be available to the third party upon completion of the contract.

California Attorney General Issues Guidelines for Do-Not-Track Disclosure Law Compliance

Han (Jason) Yu

To address online tracking—namely, the collection of personal information about consumers over time as they move across different websites and online services—major browser companies had implemented so-called do-not-track (DNT) technology in their browsers by 2013. This technology involves a web browser communicating a consumer's DNT request (signal) as part of the HTTP header information to websites that the consumer visits. Web browsers only send DNT signals and do not enforce them, however, meaning that a website can choose whether to honor or disregard the signals.

Consequently, although browser DNT signals have existed since late 2010, consumers have no idea how websites and online services are responding to their browsers' DNT signals. In an effort to rectify this, the California Online Privacy Protection Act of 2003 (CalOPPA) was amended in 2013 to require that websites and online services disclose in their privacy policies how they respond to web browsers' DNT signals. This DNT disclosure law went into effect on January 1, 2014.

The CalOPPA amendment does not define what constitutes a DNT signal, and currently no uniform technology standard exists for DNT signals. As a result, the online industry was uncertain how to comply with the new DNT disclosure law. On May 21, 2014, the California attorney general issued guidelines entitled "Making Your Privacy Practices Public" (AG Guidelines), which provide much-needed clarity regarding the DNT disclosure law.

"Consumers have no idea how websites and online services are responding to their browsers' DNT signals."

Per the AG Guidelines, CalOPPA does not require commercial websites and online services to honor DNT signals, but to disclose how they respond to such signals. DNT disclosure is required only if a commercial website or online service engages in the collection of personally identifiable information about a consumer's online activities over time and across third-party websites or online services. This means that if the operator of a website or online service does not engage in online tracking of individual consumers over time or across third-party sites or services, such operator need not include a DNT disclosure in its privacy policy.

The AG Guidelines also clarify that under the 2013 amendment, the operator of a website or online service that is required to make a DNT disclosure in its privacy policy may do so in one of two ways: either by including in the privacy policy a description of how the site or service responds to a DNT signal (direct-disclosure option), or by including a clear and conspicuous link in the privacy policy to a program or protocol that offers consumers a choice about online tracking, provided that the linked location contains a description of the program or protocol and a description of the effects of such program or protocol on consumers who participate in it (linking option). The AG Guidelines recommend the direct-disclosure option as the preferred method that provides greater

"CalOPPA does not require commercial websites and online services to honor DNT signals, but to disclose how they respond to such signals."

transparency, and treats the linking option as the less transparent method.

For the direct-disclosure option, the AG Guidelines further recommend that websites and online services clearly label the section in their policies regarding online tracking—for example, with headings such as "How We Respond to Do-Not-Track Signals," "Online Tracking" or "California Do-Not-Track Disclosures"—in order to make it easy for consumers to locate. The AG Guidelines recommend that online operators consider the following questions when describing how they respond to DNT signals:

- Do you treat consumers whose browsers send a DNT signal differently from those without one?
- Do you collect personally identifiable information about a consumer's browsing activities over time and across third-party websites or online services if you receive a DNT signal?
- If you continue to collect personally identifiable information about consumers with a DNT signal as they move across other sites or services, how do you use the information?

The AG Guidelines recommend that online operators consider the following questions when using the linking method:

- Do you comply with the linked program or protocol? (Your answer should be yes, and should be stated as such in your privacy policy.)
- Does the page to which you link contain a clear statement about the program or protocol's effects on the consumer (*i.e.*, whether participation stops the collection of a consumer's personally identifiable information across websites or online services over time)?
- Does the page to which you link make it clear what a consumer must do to exercise the choice offered by the program or protocol?

In addition to disclosure regarding response to DNT signals, the DNT disclosure law requires the operator of a website or online service to state in its privacy policy whether other parties are or may be engaged in online tracking of an individual consumer (*i.e.*, collecting personally identifiable information about an individual consumer's online activities over time and across different sites or services) when the consumer is using the operator's site or service. This second requirement applies to all commercial websites and online services that collect personal information about California residents, regardless of whether they are also subject to the DNT signal response disclosure requirement. The AG Guidelines recommend that online operators consider the following questions when preparing disclosure about third-party tracking:

- Are only approved third parties on your site or service collecting personally identifiable information from consumers who use or visit it?
- How would you verify that authorized third parties are not bringing unauthorized parties to your site or service to collect personally identifiable information?
- Can you ensure that authorized third-party trackers comply with your DNT policy? (If not, disclose how they might diverge from your policy.)

The AG Guidelines make it clear that a robust and reader-friendly privacy policy disclosure about online tracking is the best way to ensure compliance with CalOPPA. At the same time, because the 2013 amendment neither prohibits online tracking nor requires websites and online services engaging in online tracking to respond to web browsers' DNT signals, websites and online services remain free to decide whether and how they respond to DNT signals.[1]

Article III Standing in Privacy Cases

Anthony A. Bongiorno and Bridget K. O'Connell

In 2014, more than 43 percent of U.S. companies experiencing a data breach.[2] Prior to 2014, the plaintiffs' bar was unsuccessful in translating data breaches into fruitful class action litigation, but two recent decisions in high-profile cases suggest that the tide may be turning.

BACKGROUND

It is elementary that, in order to proceed in any lawsuit, plaintiffs in federal court are required to establish

1 Earlier in 2014, Yahoo! and AOL announced that they will not follow web browsers' DNT signals, citing the lack of a standard on DNT technology as the reason. Facebook also announced that it will not honor DNT signals on Microsoft's Internet Explorer.

2 2014 Ponemon Institute Report.

Article III standing under the U.S. Constitution. This requires three elements: injury-in-fact, causation and redressability. Traditionally, plaintiffs in data breach cases struggled to define a "harm" sufficient to demonstrate injury-in-fact and confer Article III standing. Last year in *Clapper v. Amnesty International USA*, the Supreme Court of the United States emphasized the longstanding principle that alleging future harm alone is not enough; a plaintiff must allege that the future harm is "certainly impending." Accordingly, certain types of future harm, such as potential future payment card fraud resulting from a data breach, have been deemed too speculative or attenuated to qualify as injury-in-fact for Article III standing.

RECENT DECISIONS

In January 2014, a federal district court judge ruled in *In re Sony Gaming Networks and Customer Data Security Breach Litigation* that the plaintiffs had Article III standing—despite the fact that the plaintiffs had not alleged actual harm, such as the misuse of their personal information. Instead, the court found that the plaintiffs had satisfied the injury-in-fact prong of Article III standing on the basis of their allegations that their personal information was collected by the defendant, wrongfully disclosed through a data breach, and potentially could result in future payment card fraud or identity theft. The court found that these allegations sufficiently demonstrated a "credible threat of impending harm."

Although the plaintiffs in *Sony Gaming* cleared the Article III injury-in-fact hurdle, the court dismissed many of their negligence-based and contractual claims, finding that the plaintiffs had failed to allege facts showing causation and damages on those claims. Some of the plaintiffs' claims based on state unfair and deceptive trade practice statutes did, however, survive the defendant's motion to dismiss.

Similarly, the court in *In re Adobe Systems Inc. Privacy Litigation* denied part of the defendant's Article III standing motion to dismiss. The court found that the risk identified by the plaintiffs that their personal data obtained by hackers from the defendant's servers would be misused in the future was "immediate and very real." In *Adobe*, hackers deliberately targeted the defendant's servers and spent weeks collecting personal data for millions of customers, including names, addresses and payment card data. Based on those facts, the court concluded that the plaintiffs did not have to wait until they experienced fraud or identity theft in order to have standing to sue. The court found that the plaintiffs sufficiently alleged that the threat of future harm was "concrete and imminent." The court also credited the plaintiffs' allegations that they had been harmed based on costs they incurred to mitigate the risk of future identity theft or fraud by purchasing data monitoring services. As in *Sony Gaming*, the court dismissed certain of the plaintiffs' causes of action, finding that the plaintiffs did not adequately plead any harm resulting from the defendants' alleged delay in notifying its customers of the data breach.

Despite these two cutting-edge rulings, the future of data breach class-action litigation is murky. After the plaintiffs in *Sony Gaming* partially survived the defendant's motion to dismiss, the defendant agreed to settle the plaintiffs' claims for $15 million in games, online currency and identity theft reimbursement to customers affected by the data breach. While the plaintiffs in *Adobe Systems* also defeated a motion to dismiss, the litigation is still in its beginning stages. Information obtained by either side during the discovery process could radically shape the parties'—and the court's—analysis of whether the "immediate and very real" threat of harm is borne out by the evidence.

Other plaintiffs in 2014 have not been so fortunate. Over the last 12 months, several other courts have dismissed class action cases based on a lack of harm to consumers following data breaches. The majority of courts have not been willing to view an increased risk of future harm (such as payment card fraud or identity theft) as sufficient to confer Article III standing after the Supreme Court's decision in *Clapper*.

The Supreme Court may decide to weigh in again on the Article III injury-in-fact issue in its 2014-2015 term if it hears the case of *Spokeo, Inc. v. Thomas Robins*. *Spokeo* is not a data breach case, but it raises similar issues about the potential for future harm resulting from personal data. Spokeo is a people search engine that compiles information about individuals on its website. The plaintiff claimed that Spokeo posted false information about him that may damage his future employment prospects. The U.S. Court of Appeals for the Ninth Circuit held that the plaintiff had satisfied the Article III injury-in-fact requirement simply by pleading a violation of his statutory rights under the Fair Credit

> "The court found that the plaintiffs sufficiently alleged that the threat of future harm was 'concrete and imminent.' "

Reporting Act. Spokeo contends that the plaintiff has not shown any injury, and petitioned the Supreme Court to hear the case and resolve confusion about the Article III injury-in-fact requirement. This case, if heard, would be an opportunity for the Supreme Court to provide much-needed clarification about whether an allegation of the threat of future harm is sufficient to confer standing.

2014 Data Breaches Highlight a Broad Range of Risks

Matthew L. Knowles, Anthony A. Bongiorno and Matthew R. Turnell

This year saw two remarkable trends with respect to large-scale data breaches. First, leaks and attacks have continued and even accelerated, including a number of data breaches whose scope exceeded the Target breach that dominated headlines in 2013. Second, the public appears to have lost interest as stories of massive data breaches have become routine. For example, while the Target breach was the subject of both extensive media coverage and broad public attention, a 2014 breach of almost identical scale at Home Depot failed to attract nearly the same widespread concern.

"The bottom line is simple: encrypt your data."

While public interest may have waned, the number of attacks in 2014, the diverse means through which they were carried out and the heavy cost of responding to these data breaches all show that privacy professionals must remain on guard. Five breaches in particular illustrate the scope and broad nature of data security risks, and demonstrate that a robust compliance and security program is necessary to defend against an expansive profile of risks.

JPMORGAN CHASE

In July 2014, JPMorgan Chase announced that hackers had gained access to a number of its servers and had harvested account data for millions of customers. By early October, the number of accounts affected increased to 76 million households and seven million small business accounts. Even more troubling, hackers reportedly had "root access" (the highest level of access) to a number of JPMorgan's servers.

Rather that attempting to steal money directly from accounts, the hackers apparently harvested an even more valuable resource: customer data. The attack has the hallmarks of an extended operation, where hackers plan to monetize the data collected during the breach through use in future phishing and other attacks. The JPMorgan attack underscores the fact that "mere" customer data—even without credit card and account numbers—is one of the most valuable resources that businesses hold and hackers desire.

HOME DEPOT

As in the 2013 Target attack, hackers used malware installed on retail point-of-sale terminals to launch a massive attack on Home Depot. Hackers stole credit card data for more than 60 million customers using malware that went unnoticed from April to September 2014, and wasted no time in posting the data for sale online. Putative class action plaintiffs launched another wave of opportunistic litigation as soon as Home Depot announced the breach.

MOLINA HEALTHCARE

In early May 2014, Molina Healthcare announced a very different kind of data breach. A routine mailing sent to thousands of customers inadvertently contained customers' social security numbers. Paired with the customers' mailing addresses, these postcard mailings offered an easy target for data fraud.

The breach came about when Molina's vendor accidentally substituted social security numbers for the tracking numbers that were supposed to be printed on the cards. There is no word why the vendor needed access to social security numbers in the first place, which highlights the importance of minimizing and compartmentalizing data storage and transmission whenever possible.

AMTRAK

The strangest data breach of the year comes from Amtrak, the quasi-public entity that runs the United States' passenger rail system. In 2014 Amtrak discovered that an employee had earned $850,000 over 20 years by stealing and selling Amtrak's customer data. Even stranger is who was purchasing this stolen data: the U.S. Drug Enforcement Agency (DEA). The DEA bribed the employee to leak this data despite the fact that the DEA had access to the same data through official channels. While bizarre, this attack demonstrates the threat of corrupt insiders and the fact that even careful monitoring and compliance audits might not be enough to protect company data.

ORANGEBURG-CALHOUN TECHNICAL COLLEGE

A 2014 data breach affecting students of Orangeburg-Calhoun Technical College illustrates the continued threat from one of the most common and easily avoided data breaches. After a laptop disappeared from a staffer's office, the college learned that the missing computer contained records—including social security numbers—for at least 20,000 students. In the wake of the breach, the college launched a process to fully encrypt all machines containing user data, a step that would have averted the breach in the first place.

This fact pattern is repeated across the United States at hospitals, doctors' offices, schools, businesses and other places where sensitive data is stored. The bottom line is simple: encrypt your data.

COMMENT

While the sheer number of data breaches in 2014 resulted in less media coverage and public scrutiny of each individual case, the costs of responding to a breach remain substantial. Prevention can be challenging and expensive, but the continued risks of data breach leave companies and institutions no choice but to invest in data security.

Microsoft Warrant Litigation

Bridget K. O'Connell and Anthony A. Bongiorno

On December 4, 2013, Magistrate Judge James C. Francis IV of the U.S. District Court for the Southern District of New York signed a search warrant issued by the U.S. Department of Justice to Microsoft Corporation. The warrant required the company to turn over e-mails and other records for a particular Microsoft e-mail user account. While issuance of a warrant is generally a routine matter, in this case it triggered strong opposition. The outcome of the litigation will have a significant impact on U.S. corporations with international business operations.

The government's authority to issue the warrant stems from the Stored Communications Act (SCA), which requires internet service providers to produce certain types of information, including the contents of a user's e-mail account, pursuant to a warrant. The warrant mandated that Microsoft produce e-mails from one specific e-mail account. Those e-mails were stored on a Microsoft-owned server located in Dublin, Ireland. Instead of turning over the e-mails, Microsoft moved to quash the warrant. Microsoft argued that warrants issued by federal courts only apply to search and seizure of property located within

the United States, and that the government cannot compel a company to turn over records stored on servers located outside the United States pursuant to an SCA warrant. Microsoft contended that complying with the warrant could violate other countries' data privacy laws as well as international law principles of comity, sovereignty and reciprocity.

Microsoft lost its argument at the district court level and has now appealed to the U.S. Court of Appeals for the Second Circuit. Microsoft has refused to comply with the warrant while the appeal is pending and has stipulated that it is in contempt of the warrant in order to expedite appellate review.

In recommending that the district court deny Microsoft's motion to quash, Magistrate Judge Francis described an SCA warrant as a "hybrid: part search warrant and part subpoena," because it requires the company to search for its own records, whereas a traditional warrant allows the government to search for and seize records. U.S. District Judge Loretta Preska, who adopted the magistrate's order and denied Microsoft's motion to quash, viewed the issue as "a question of control, not a question of location," and found that Microsoft had control over the non-U.S. data described in the warrant.

Companies that conduct multi-country operations and use non-U.S. servers are concerned about the ruling. Several companies submitted *amicus* briefs in support of Microsoft's position at the district court level, citing fears about potential sanctions by foreign governments for complying with an SCA warrant in conflict with the data privacy laws of the country in which servers are located.

The e-mails stored on Microsoft's Dublin server present a further layer of concern from a data privacy standpoint: Microsoft argues that the e-mails are not its own business records, but rather an individual's electronic correspondence that is merely hosted on Microsoft's server. If the ruling stands on appeal, the U.S. government will be able to obtain information—regardless of its location, and including not only a company's own records but also documents, such as e-mails, created by individuals and stored on a company's non-U.S. server—under the theory that the information is controlled by the company. The Second Circuit is expected to hear Microsoft's closely watched appeal in 2015.

Supreme Court Prohibits Warrantless Mobile Phone Searches, Underscores Individual Right to Privacy

Matthew R. Turnell, Bridget K. O'Connell and Devin Cohen

In June 2014, the Supreme Court of the United States released a unanimous decision prohibiting law enforcement officials from searching the mobile phones of individuals placed under arrest without either a search warrant or the owner's consent. In each of two companion cases, *Riley v. California* and *United States v. Wurie* (the latter arising from a federal prosecution in Massachusetts), police officers placed the suspect under arrest and searched a mobile phone that was in the suspect's immediate possession without consent or a warrant, based upon a longstanding exception to the warrant requirement covering searches "incident to arrest." While the U.S. Constitution generally requires either a valid warrant or voluntary consent before officers can search one's person, home or other effects, the search incident to arrest exception allows law enforcement to search an arrested person and his or her immediate effects (such as pocket contents) under the justification that such searches help ensure officer safety and prevent destruction of evidence.

The Supreme Court ruled that the search incident to arrest doctrine does not permit the routine search of a mobile phone present on a suspect's person at the time of arrest. It concluded that less intrusive measures, such as examining a phone's exterior and securing it out of the arrestee's (physical and digital) reach, could address law enforcement's concerns for officer safety and protection of evidence. The Supreme Court went on to reject the contention that searching a mobile phone is "materially indistinguishable" from searching other physical items on one's person, such as a wallet, agenda or backpack. The Supreme Court noted that comparing the search of such physical objects to a search of a mobile phone "is like saying a ride on horseback is materially indistinguishable from a flight to the moon . . . Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet or a purse."

The Supreme Court's decision to exclude mobile phone searches from the search incident to arrest

doctrine does not necessarily leave law enforcement without other avenues for accessing phone contents. Most importantly, officers may still request consent to search an arrestee's phone. The Supreme Court also suggested that officers may access a phone's contents to the extent necessary to disable auto-locking features that would render the phone inaccessible after a warrant could be obtained. Finally, the Supreme Court left open the possibility that "exigent circumstances" might justify certain warrantless phone searches without consent in certain cases.

At least one state court has taken the Supreme Court decision in *Riley* a step further, indicating that cell phone search warrants violate the Fourth Amendment's particularity requirement if they do not limit the content that the government can access. In *Nebraska v. Henderson*, the Nebraska Supreme Court held that the scope of the search warrants used by police was overbroad and should have been restricted to "only that content that [wa]s related to the probable cause that justifie[d] the search." The Nebraska Supreme Court also rejected the lower court's reasoning that no warrant was required to search Henderson's phone, citing the Supreme Court's ruling against warrantless cell phone searches in *Riley*.

MOBILE PHONES RAISE NEW PRIVACY CONCERNS

The *Riley* decision is rooted in a determination that the storage capacity of a mobile phone is vastly greater than any other physical object a person typically carries. As a result, privacy considerations with respect to mobile phones must be viewed differently than those applicable to other physical objects. The Supreme Court outlined four factors that make mobile phones unique:

- Mobile phones collect numerous distinct types of information, which taken together can reveal more than each could separately. The Supreme Court noted that even applications on a person's mobile phone reveal a great deal of personal information that would be unavailable from a search of his or her person.
- Each specific type of information on a mobile phone is more detailed than what would be available through a search of other physical objects. For example, unlike a wallet, a mobile phone can hold thousands of pictures, along with the dates and locations of each image.
- A mobile phone can give a chronology of all communications with other persons, which can go as far back as the date of purchase of the phone, or even earlier.
- Finally, the use of mobile phones, which contain what the Supreme Court describes as "a cache of sensitive personal information," has become commonplace in modern life; it is rare that the average U.S. citizen does not have a cell phone on or near his or her person at almost all times.

In sum, the Supreme Court's decision recognizes the significance of an individual's expectation of privacy in content stored on or accessible through mobile phones in a manner that could potentially affect other contexts and mediums—such as the collection, storage and brokering of a user's web browsing or other digital data without clear user consent to do so.

APPLICATION TO INDIVIDUALS

The *Riley* decision may provide clients facing white-collar investigations with stronger means to object to providing data stored on mobile devices. As a practical matter, however, clients often seek to cooperate with such investigations, so they likely would consent in any event. By contrast, in situations where company representatives or individual executives may be facing imminent arrest, they should consult with an experienced white-collar defense lawyer before offering any statements or consent to search a mobile device to law enforcement. A person can always decide to cooperate after consulting with counsel, but it may be impossible to undo the damage caused by a statement made or search consent given before legal consultation has occurred. In addition, to the extent the law enforcement officer seeks to invoke one of the "exemptions" addressed by the Supreme Court's decision, the executive or company representative who is under arrest should ask the officer to simply secure the phone without accessing its contents until he or she can consult with a lawyer about providing consent to the search. If a law enforcement official insists upon taking steps designed to ensure future access (*e.g.*, disabling the auto-lock feature), the executive should request that the officer take all such actions only while the executive is watching in order to ensure the actions taken are indeed limited to those necessary to accomplish the stated purpose.

"Privacy considerations with respect to mobile phones must be viewed differently than those applicable to other physical objects."

APPLICATION TO EMPLOYERS

Given that the Supreme Court's decision is grounded in the Fourth Amendment, some may argue that it is not directly applicable to the private workplace context. However, federal courts historically have been willing to rely upon Fourth Amendment precedent to decide analogous issues in the private employment context, particularly in cases where there may be little other relevant precedent. Since the *Riley* decision clearly signals a pro-privacy approach to mobile device use, employers should re-examine their current policies that address employees' use of mobile devices in order to ensure that such policies clearly spell out expectations with respect to privacy and mobile phone use, and address procedures for commonly encountered workplace issues, including dual-use devices (those that are used for both personal and business use). Employers should also revisit current policies for reviewing mobile device contents in connection with internal investigations and for activating litigation holds, and procedures for handling mobile devices and their contents in cases of departing employees.

Finally, in light of the Supreme Court's decision, employers should consider providing clear notice to employees regarding potential inspections and monitoring of mobile devices used for work, ensure that they have defensible and legitimate business interests in conducting the monitoring, and consider effective ways to obtain employees' consent prior to inspecting or monitoring contents of mobile devices used for work-related purposes.

Following these practical tips can help balance individual privacy rights with an employer's legitimate business interests in light of the Supreme Court's decision.

The NIST Cybersecurity Framework

Ann Killilea and Heather Egan Sussman

Responding to an Executive Order, the National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity on February 12, 2014. Developed in cooperation with the private sector, the Framework is intended to provide a *voluntary* risk-based program for owners and operators of critical infrastructure. It offers organizations a set of best practice approaches for assessing and mitigating their cybersecurity risks.

The Framework provides a common language regarding cybersecurity issues, enabling important discussions to take place between an organization's IT professionals and an organization's business professionals who might be uncomfortable with the seemingly complicated language of IT security. The Framework's common-sense approach allows an organization and its directors to identify and improve upon current cybersecurity procedures. Although the Framework was developed for the 16 critical infrastructure sectors, it is applicable to all companies (at least for now) on a voluntary basis.

THE CYBERSECURITY FRAMEWORK'S COMPONENTS

The Framework contains three primary components: the Core, Implementation Tiers and Framework Profiles.

The Framework Core is a set of cybersecurity activities and applicable references established through five concurrent and continuous functions—Identify, Protect, Detect, Respond and Recover—that provide a strategic view of the lifecycle of an organization's management of cybersecurity risk. Each of the Core functions is further divided into categories tied to programmatic needs and particular activities. The Core functions can be thought of as the Framework's foundation for how an organization should view its cybersecurity practices:

- Identify its most critical intellectual property and assets
- Develop and implement procedures to protect them
- Assign resources to timely detect a cybersecurity breach
- Institute procedures to both respond to and recover from a breach, if and when one occurs

The Framework Implementation Tiers describe the level of sophistication and rigor an organization employs in applying its cybersecurity practices, and provide a context for applying the core functions. Consisting of four levels from Partial (Tier 1) to Adaptive (Tier 4), the tiers describe approaches to cybersecurity risk management that range from informal and ad hoc (a low grade) to agile and risk-

FUNCTIONS	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

NIST Cybersecurity Framework Core Structure

informed (a high grade). The Implementation Tiers allow an organization to give itself a grade on its level of cybersecurity readiness.

The Framework Profile allows organizations to clearly articulate the goals of their cybersecurity program. The Framework is risk-based, and therefore the controls and process for its implementation change as the organization's level of risk changes. Building upon the Core and the Implementation Tiers, a comparison of the Profiles (*i.e.*, Current Profile versus Target Profile) allows for the identification of desired cybersecurity outcomes and gaps in existing cybersecurity procedures.

THE BENEFITS OF THE FRAMEWORK

While it is a voluntary standard and thus lacks the force of law, the Framework provides organizations with several benefits, each of which supports a stronger cybersecurity posture, including a common language, the ability to verifiably demonstrate due care via Framework adoption, improved ability to track compliance, better vendor management and improved cost efficiency in cybersecurity spending. It may not yet be a required standard, but it is considered a best practice in managing risk. It uses the vocabulary of risk management (rather than IT security) to communicate about cybersecurity—a vocabulary well-understood by senior management and boards of directors.

RECOMMENDED NEXT STEPS

The Framework may evolve into another compliance requirement, but it also provides real benefits to its users. Against this backdrop, companies in any industry trying to make sense of what they should do next with respect to cybersecurity and its emerging standards should consider taking the following steps:

- Assign an accountable function to become knowledgeable about the NIST Framework and related ongoing governmental developments.
- Use the Framework's recommended approach to undertake a review of the company's infrastructure and security protocols.
- Examine the company's existing security protocols (for example, those instituted in response to the statutory, contractual and regulatory requirements for the protection of personal data) and develop a current profile of the company's existing security posture.
- Establish the overall desired security objective—in other words, identify where the security profile should be in light of the company's industry, type of information processed and other relevant factors.
- Develop a gap analysis of action steps needed to arrive at the desired objective.
- Prioritize those actions steps, available resources and an appropriate timeline.

- Where possible, use the Framework's language and approach, because even if the Framework is voluntary at this point, it could become the standard by which companies are measured going forward.

Advertising, Marketing and Promotions: Right of Publicity and Celebrity Endorsements

Han (Jason) Yu and Sarah Bro

When privacy is considered in the context of advertising, marketing and promotions, most marketing professionals are highly aware of issues pertaining to the collection and management of personally identifiable information, advertising directly to children, and the necessity of clear and up-to-date privacy policies. Often, however, advertising campaigns or promotions are developed and launched without considering the right of publicity and the liabilities that can arise from overlooking this important legal issue. The right of publicity is fundamentally tied to the right of privacy and is sometimes interconnected with intellectual property laws.

"While most right-of-publicity cases to date have involved celebrities, any individual has a protectable right of publicity."

The right of publicity is an individual's right to control the commercial use of his or her identity. Historically an offshoot of an individual's right to privacy, the "right of publicity" was first introduced by the U.S. Court of Appeals for the Second Circuit in the 1953 case *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.* Over the years, the right of publicity has evolved into a property right allowing an individual to recover damages for the economic value of a defendant's unauthorized commercial exploitation of the individual's identity (name, likeness, voice, signature, distinctive appearance, *etc.*) While most right-of-publicity cases to date have involved celebrities, any individual has a protectable right of publicity. Currently, the right of publicity exists only under state laws, and there is no federal law protecting such right. Nineteen states recognize the right of publicity via statute, and 28 more recognize the right under common law. Certain states, including California, recognize a post mortem right of publicity.

The most common example of a right-of-publicity violation is when a business runs an advertisement or promotion that uses the identity of an individual (whether in text, photos, artwork, videos, audio or some other tangible form) without permission. Violations can occur in both traditional media (television, radio, print) and digital media.

In recent years, more businesses have turned to social media as a new platform for running advertising and promotions. According to a 2013 University of Massachusetts report, 34 percent of *Fortune* 500 companies actively blog, 77 percent maintain active Twitter accounts, 70 percent have Facebook pages and 69 percent have YouTube accounts. It is estimated that more than 90 percent of marketers are now using social media. Accordingly, marketing and advertising professionals have more opportunities than ever to run afoul of right-of-publicity laws.

While unauthorized use of a photograph of a third party in connection with an advertisement or promotion may be a clear violation of that third party's right of publicity, other less obvious uses of an individual's name, image or likeness also may be considered a violation. Some of the most recent disputes in this area are illustrative of the wide range of circumstances and facts that can lead to claims of right-of-publicity violations.

In February 2014, the U.S. Court of Appeals for the Seventh Circuit ruled in *Michael Jordan v. Jewel Food Stores, Inc.*, that Jewel did not have the right to publicly congratulate Jordan on his Hall of Fame induction in an ad featuring the supermarket's logo and motto in connection with Jordan's familiar No. 23 on a pair of white and red shoes. The advertisement was found to be commercial speech and thus was subject to the question of whether it improperly suggested a connection, association or endorsement by Jordan.

In March 2014, when paparazzi captured actress Katherine Heigl carrying Duane Reade bags in New York City, the pharmacy chain tweeted the paparazzi photo with the caption "Even @KatieHeigl can't resist shopping #NYC's favorite drugstore." Heigl filed a $6 million suit, including a claim for misappropriating her right of publicity. The suit was dropped after the parties reached an undisclosed settlement agreement and Duane Reade made a contribution to a foundation affiliated with Heigl.

Over the past year, several class action lawsuits have been filed in California, Florida and Ohio against websites such as JustMugShots.com and MugshotsOnline.com, which monetize the display and removal of mug

shots. The lawsuits claim that the websites violate the applicable right of publicity statutes to the extent that they use the likeness of the individuals depicted in the mug shots for commercial gain.

In April 2014, Elvis Presley Enterprises filed suit against firearm manufacturer Beretta, claiming the gun company created a wide-reaching Elvis-themed advertising campaign that could be found on the Beretta Facebook page and that included Elvis impersonators at a Beretta tradeshow booth in Las Vegas.

On October 8, 2014, Eagles front-man Don Henley filed suit in California district court against Wisconsin-based clothing manufacturer Duluth Trading Co. after the company sent an e-mail advertisement for its henley shirts that encouraged customers to "Don a Henley and Take It Easy" (seemingly a reference to the Eagles' song "Take it Easy.") Among the causes of action, Henley alleged a violation of the California Statutory Right of Publicity under California Civil Code Section 3344.

These disputes are only a few examples of the growing number of cases that involve the right of publicity and the ever-changing landscape of social media and technology. Marketing and advertising professionals should make concerted efforts to scrutinize all materials and ensure that the proper permissions are obtained from any and all individuals whose identities are incorporated in their campaigns, whether or not they are celebrities.

SPECIAL FOCUS ON U.S. HEALTH CARE

Consumer Health Information

Jennifer S. Geetter, Julia Jacobson and Scott Weinstein

The availability and variety of mobile health apps in the United States continues to grow. One industry analyst reported a 62 percent increase in use of mobile health apps during the first six months of 2014, compared to a 33 percent increase in use for the mobile app industry in general.[3] Consumers increasingly see their mobile devices as tools for making healthy choices, tracking diet and exercise programs, and managing and recording health information for ongoing health concerns. Developers have launched new platforms in response to this demand, and these platforms have the potential to increase the mobile health app user base exponentially in a short period of time and consolidate industry-driven privacy platforms.

Amid this increasing mobile health app use, the Federal Trade Commission (FTC) held a seminar on May 7, 2014, that focused on consumer-generated health information (CHI). CHI is data generated by a consumer's use of a mobile app, website or other digital service that relates to his or her health. FTC Commissioner Julie Brill opened the seminar by stating that she believes CHI is more sensitive and in need of more privacy-sensitive treatment than other consumer-generated data. The seminar explored the following key issues.

WHAT ARE CONSUMERS' EXPECTATIONS ABOUT HOW THEIR CHI IS USED AND PROTECTED?

Some speakers expressed concern that consumers mistakenly believe the privacy and security of the health information they share through their mobile devices is automatically protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA, however, only protects individually identifiable health information created or received by covered entities (*i.e.*, health plans, most health care providers and health care clearinghouses) and business associates (*i.e.*, the third parties that support covered entities). Since HIPAA regulations govern the regulated entities' and not necessarily the data itself, health information that is not collected or maintained by or on behalf of a covered entity or business associate is generally not regulated by HIPAA. As a result, most health data generated by consumers through mobile apps or other digital service operators is not covered by HIPAA.

Health information obtained by commercial entities not subject to HIPAA is still generally regulated by the FTC under Section 5 of the FTC Act. Under the FTC Act, the FTC has broad power to enjoin unfair and deceptive business practices.[4] During the past

3 See http://www.flurry.com/blog/flurry-insights/health-and-fitness-apps-finally-take-fueled-fitness-fanatics (last accessed November 19, 2014).

4 States also have the power to regulate CHI under state consumer protection laws, which, like Section 5 of the FTC Act, prohibit unfair and deceptive trade practices.

"This wide variation makes it difficult to determine what information collected by mobile apps and other digital services is truly health information."

few years, the FTC has brought numerous actions against businesses operating digital services that were not transparent about how and what information was collected from consumers and how the collected information was used, shared and secured.

WHAT IS CONSUMER HEALTH INFORMATION?

Traditional medical information is clearly health information. Diet and exercise information, while clearly health-related, can reveal a little or a lot about a consumer's health, depending on its content. Other information—such as shopping habits—may not look like health information but, when aggregated with other consumer information, may reveal information about a consumer's health. This wide variation makes it difficult to determine what information collected by mobile apps and other digital services is truly health information.

HOW SENSITIVE IS CHI?

The perceived sensitivity of health information generated or derived from mobile apps and other digital services can vary greatly depending on the individual from whom it is collected and the context in which it is collected and used. This creates a "moving target" for app developers in developing their privacy policies. Although a consumer may not perceive heart rate and exercise data collected by a mobile fitness app to be "sensitive," the consumer may consider the use of this information to draw conclusions about his or her weight offensive. If these data points are further used as the basis for financial- or health-risk rating, the stakes become much higher for both consumers and regulators.

Although these and other concerns about CHI were raised during the seminar, the FTC did not offer clear guidance for developers and operators of health- and fitness-related mobile apps and other digital services. It is clear, however, that the FTC is watching how digital services collect and process CHI. Until guidance is available, stakeholders in the health-related digital economy should consider implementing privacy-sensitive and transparent methods for collecting, using and sharing CHI, and should evaluate agreements with "downstream" recipients of CHI to determine whether representations made to consumers at the time of collection match the agreement terms, as well as long-term strategic priorities.

HHS – OCR Enforcement Development

Edward G. Zacharias

This was an active year for the federal government's enforcement of the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations (collectively referred to herein as HIPAA). So far in 2014, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) has entered into settlement arrangements with six covered entities to resolve alleged violations of HIPAA. While at first glance this may not seem like substantial enforcement activity, it represents the greatest number of HIPAA settlements by OCR in any calendar year to date.

OCR has been increasingly vocal about HIPAA enforcement being an agency priority, possibly in response to congressional pressure to meet its statutory enforcement mandate and a recent Office of Inspector General investigation criticizing OCR's enforcement practices. In addition, the agency's pipeline of active investigations has likely increased in recent months in response to the lower breach reporting threshold that was adopted in the final HIPAA Omnibus Regulations and became effective on September 23, 2013. While there has recently been a notable amount of turnover in top-level HIPAA staff at OCR, there is nothing to suggest that the new leadership will not make enforcement an ongoing priority in the years to come.

The HIPAA settlement arrangements between covered entities and OCR in 2014 are briefly described below.

SKAGIT COUNTY, WASHINGTON

OCR's first HIPAA settlement of the year was entered into on March 6, 2014, with a county government. OCR opened an investigation of Skagit County, Washington, upon receiving a December 9, 2011, breach notification that money receipts with electronic protected health information (ePHI) of seven individuals were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the county. OCR's investigation revealed a broader exposure of ePHI for 1,581 individuals whose information was accessible on the county's public web server. Many of the accessible files involved ePHI of a sensitive nature, including information concerning

the testing and treatment of infectious diseases. OCR's investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security and Breach Notification Standards (*e.g.*, failure to notify the affected individuals of the breach, lack of sufficient policies and procedures, failure to train county workforce). The investigation was settled through the execution of a resolution agreement that included a payment of $215,000 and a corrective action plan (CAP). The CAP has a three-year term and requires Skagit County to take the following actions, among others:

- Post a notification of the breach on the home page of the county's website for 90 days and in major print or broadcast media
- Update its privacy, security and breach notification policies and procedures subject to OCR's review
- Submit hybrid entity documents designating its covered health care components to OCR, and implement hybrid entity and related safeguards
- Report to OCR any violations of its HIPAA policies and procedures by workforce members
- Submit annual compliance reports to OCR

QCA HEALTH PLAN, INC.

On April 14, 2014, OCR entered into a resolution agreement and CAP with QCA Health Plan, Inc., to settle alleged violations of the HIPAA Privacy and Security Standards. OCR began investigating QCA after receiving a breach notification from the insurer on February 21, 2012, that an unencrypted laptop containing the ePHI of 148 individuals was stolen from a workforce member's car. In addition to the unauthorized disclosure of ePHI, OCR's investigation revealed that QCA had not taken the following actions:

- Implemented policies and procedures to prevent, contain and correct security violations
- Conducted an assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the ePHI it held
- Implemented security measures sufficient to reduce any identified risks and vulnerabilities to a reasonable and appropriate level
- Implemented appropriate physical safeguards for workstations that accessed ePHI

The investigation was settled through the execution of a resolution agreement that included a payment of $250,000 and a CAP. The CAP has a two-year term and requires QCA to take the following actions, among others:

- Provide OCR with an updated risk analysis and corresponding risk management plan that includes specific security measures to reduce the risks to and vulnerabilities of its ePHI
- Retrain its workforce
- Report to OCR any violations of its HIPAA policies and procedures by workforce members
- Submit annual compliance reports to OCR

CONCENTRA HEALTH SERVICES

On April 21, 2014, OCR entered into a resolution agreement and CAP with Concentra Health Services to settle alleged violations of the HIPAA Privacy and Security Standards. The settlement resulted from an investigation initiated by OCR upon receiving a December 2011 breach report that an unencrypted laptop was stolen from a Concentra physical therapy center. The total number of affected patients was unclear. OCR alleged that Concentra failed to remediate and manage its lack of encryption, which was identified as a potential source of vulnerability in Concentra's HIPAA risk assessment. For instance, only 434 out of the covered entity's 597 laptops were encrypted. OCR also alleged that Concentra had failed to implement policies and procedures to prevent, detect, contain and correct security violations. Prior to this incident, Concentra had been subject to two security breaches involving stolen, unencrypted laptops that each affected more than 500 individuals, as well as 16 additional breaches affecting fewer than 500 individuals. The investigation was settled through the execution of a resolution agreement that included a payment of $1,725,220 and a CAP. The term of the CAP is two years and requires Concentra to take the following actions, among others:

- Conduct and submit for OCR's approval periodic risk analyses, including assessments of potential risks and vulnerabilities to the confidentiality of Concentra's ePHI
- Implement risk management plans and provide OCR with evidence of such implementation and timelines for any expected remediation actions

"The investigation was settled through the execution of a resolution agreement that included a payment of $215,000 and a corrective action plan."

- Provide to OCR periodic encryption status updates
- Provide security awareness training to its workforce members
- Submit annual compliance reports to OCR

COLUMBIA UNIVERSITY AND NEWYORK-PRESBYTERIAN HOSPITAL

On May 7, 2014, OCR entered into a resolution agreement and CAP with each of the trustees of Columbia University in the City of New York (CU) and NewYork-Presbyterian Hospital (NYP) to settle alleged violations of the HIPAA Privacy and Security Standards. The settlements arose from OCR investigations of CU and NYP following their September 27, 2010, joint notification to OCR of the unauthorized disclosure of ePHI for 6,800 individuals, including patient status, vital signs, medications and laboratory results.

NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The breach was caused when "a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally owned computer server on the network containing NYP patient ePHI." Deactivation of the server resulted in ePHI being accessible on internet search engines. The breach was discovered when an individual complained after finding the ePHI of the individual's deceased partner, a former NYP patient, on the internet.

OCR stated that its investigation found that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI, and therefore "neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI." OCR also alleged that NYP had failed to implement appropriate policies and procedures for authorizing access to its databases, and had failed to comply with its own policies on information access management.

In order to resolve the alleged violations, NYP entered into a resolution agreement with OCR that included a payment of $3.3 million and a three-year CAP. Similarly, CU entered into a resolution agreement with OCR that included a payment of $1.5 million and a three-year CAP. Under the CAPs, NYP and CU each agreed to take the following actions, among others:

- Conduct and submit to OCR a risk analysis
- Implement a risk management plan
- Develop processes to evaluate environmental or operational changes to information systems that affect the security of ePHI
- Revise policies and procedures on information access management and device and media controls
- Develop/update a mandatory privacy and security awareness training program for workforce members with access to ePHI
- Investigate and notify OCR of any failures by workforce members to comply with HIPAA policies and procedures
- Submit annual compliance reports to OCR

PARKVIEW HEALTH SYSTEM, INC.

On June 17, 2014, Parkview Health System, Inc., entered into a resolution agreement and CAP with OCR to settle alleged violations of the HIPAA Privacy Standards resulting from a June 4, 2009, incident that involved paper medical records. OCR opened an investigation after receiving a complaint from a retiring physician alleging that Parkview had violated the HIPAA

Privacy Rule when returning approximately 5,000–8,000 of the physician's medical records. Parkview had taken custody of the records while assisting the retiring physician in transitioning her patients to new providers and was considering purchasing some of the records upon the physician's retirement. OCR alleged that Parkview did not appropriately safeguard the records when returning them to the retiring physician. To settle the allegations, Parkview entered into a resolution agreement with OCR that included a payment of $800,000 and a CAP. The CAP has a one-year term and, in part, requires Parkview to adopt and implement a policy governing the safeguarding of non-electronic PHI, train its workforce on the policy, notify OCR of any violations of the policy and submit a report to OCR regarding its compliance with the CAP.

CANADA

45.4000° N, 75.6667° W

Canada's Anti-Spam Law Fully Effective January 15, 2015

Julia Jacobson

In December 2010, Canada enacted an anti-spam law known as Canada's Anti-Spam Law (CASL) to reduce unsolicited e-mail, text messages and other commercial electronic communications. Generally, CASL applies to a "commercial electronic message" (CEM) if a computer system located in Canada is used to send or access the CEM.

A CEM is a message sent by "any means of telecommunication" (text, voice, sound or image) to an "electronic address" (e-mail, instant messaging, telephone or similar account) that is "intended to encourage participation in a commercial activity." CASL also applies to the installation, direction of the installation or the updating of a computer program by a person or business (installer) on the computer system of another person (installee) if the installer is in Canada or the installee's computer system is located in Canada. Certain kinds of electronic messages—such as those that are between family members, in response to a request or legally required—are exempt from CASL's requirements.

For CEMs, CASL became effective on July 1, 2014, and for computer programs, CASL goes into effect on January 15, 2015. CASL also includes a three-year transitional period for its consent requirements.

CONSENT REQUIREMENT

If a CEM is subject to CASL, the sender must have or obtain consent from the recipient before sending the CEM, the CEM must identify and include contact information for the sender, and the CEM must contain an unsubscribe mechanism through which a recipient can withdraw consent to receive CEMs from the sender. If installation or updating of a computer program is subject to CASL, the installer must have or obtain express consent from the installee before installing or updating, unless the computer program falls into one of the exceptions to the express consent requirement. Generally, consent must be sought separately for sending a CEM and installing or updating a computer program.

Implied Consent

A recipient's consent to receive CEMs from a sender is implied until June 30, 2017, if prior to July 1, 2014, the sender had a relationship with the recipient that has included the sending of CEMs and the recipient has not opted out. For example, if a recipient provided his or her e-mail address to a sender before July 1, 2014, the sender can continue to send CEMs to the recipient based on implied consent until the recipient opts out. The CEM must comply with the other CASL requirements (sender identification and unsubscribe mechanism) described herein.

An installee's consent to updates or upgrades to a computer program is implied until January 15, 2018, for any software installed prior to January 15, 2015.

Express Consent

Unless a CEM qualifies for implied consent, express consent is required. When seeking express consent, the sender must describe to the person from whom consent is sought the purpose for which consent is sought and include information that identifies the sender (including any person on whose behalf consent is sought). If a sender had a recipient's valid express consent prior to July 1, 2014, that express consent remains valid even if the request for consent did not contain the required identification information.

"The CEM sender or installer bears the burden of proving that consent was obtained in compliance with CASL."

Unless a computer program qualifies for implied consent, express consent is required. When seeking express consent, the installer must disclose the purpose(s) for which consent is sought, information that identifies the installer (including any person on whose behalf consent is sought), and the function and purpose of the computer program. The installer is required to disclose more information if the computer program has certain functions, such as collecting personal information, changing existing settings or enabling the installee's computer system to communicate with another system without the installee's authorization.

Express consent is deemed to have occurred for the installation of a computer program if it is reasonable to believe that the installee consented to the installation and the computer program is a cookie, HTML, JavaScript, an operating system or a program that is executable only though another computer program to which the user had already expressly consented. Express consent also is deemed to have occurred when a telecommunications service provider installs a computer program solely to protect the security of its network from a current and identifiable threat, update or upgrade the network, or correct a failure in the operation of a computer system or program.

FORM OF CONSENT

Consent may be oral or written. The CEM sender or installer bears the burden of proving that consent was obtained in compliance with CASL. Oral consent must be verifiable "by an independent third party" or in "a complete and unedited audio recording of the consent." Acceptable forms of written consent include a check box or an icon that requires proactive action, or a combination of the two. If an online form relates to a request for information or a "quote or estimate" for a product or service, the sender is only allowed to send messages in response to the particular request, not CEMs generally, and only for a period of six months.

WHEN CONSENT IS NOT REQUIRED

CEMs do not require prior consent in the following instances:

- The CEM is an inquiry or application related to the recipient's commercial activity.[5]
- The CEM provides a quote or estimate requested by the recipient.
- The CEM facilitates, completes or confirms a commercial transaction that the recipient previously agreed to enter into with the sender.
- The CEM contains warranty information, product recall information, or safety or security information about a product or service that the recipient uses, has used or has purchased.
- The CEM provides notification of factual information about a subscription, membership or similar relationship between the sender and recipient.
- The CEM provides information directly related to an employment relationship or related benefit plan in which the recipient participates or is enrolled.
- The CEM delivers a product or service, including updates or upgrades, under the terms of a prior transaction between the sender and recipient.

CEM REQUIREMENTS

If CASL applies to a CEM, the CEM must include clear identification of the sender(s) and a description of how the recipient can "readily contact" at least one of the senders for at least 60 days after the date that the CEM is sent, as well as a statement that the CEM recipient can withdraw consent to receive CEMs from the sender(s) and an electronic consent withdrawal (unsubscribe) mechanism.

ENFORCEMENT

CASL is supplemented by the Canadian Radio-television and Telecommunications Commission's (CRTC's) Electronic Commerce Protection Regulations and the Electronic Commerce Protection Regulations issued by the governor general in council.

The CRTC has authority to impose an administrative monetary penalty up to C$1 million per violation for an individual and C$10 million for a business. CASL contains a list of non-exhaustive factors that CRTC will use to determine the penalty amount, including the penalty's purpose, the violation's nature and scope, whether the violator has a history of violations of CASL or other Canadian privacy laws, and whether the violator obtained financial benefit from the violation.

SUGGESTED COMPLIANCE STEPS

- Confirm that all CEMs sent after July 1, 2014, to residents of Canada or from systems located

5 Note that "commercial" is not defined in CASL and generally is not linked solely to profit-making activities.

in Canada include the aforementioned sender identification and unsubscribe mechanism. Note that the unsubscribe mechanism requirements are similar to the requirements of the U.S. CAN-SPAM Act.

- Develop and deploy a mechanism for obtaining express consent within the meaning of CASL before sending CEMs subject to CASL to residents of Canada who were not, as of July 1, 2014, receiving CEMs from the business.
- Design a consumer-friendly mechanism for obtaining express consent from residents of Canada from whom the business currently has implied consent within the meaning of CASL.
- When the business receives an e-mail list from a third party, investigate whether the third party has consent to send CEMs to residents of Canada and, if so, whether the consent is express or implied.
- Supplement existing recordkeeping systems to include thorough records of how, when and from whom express consent to receive CEMs is obtained from residents of Canada.
- Evaluate and modify as needed current systems for honoring unsubscribe requests.
- Determine whether the business is installing any computer program from a system in Canada or onto a computer system (including smart phones) located in Canada, and develop a compliance plan consistent with CASL's January 15, 2015, deadline.

MEXICO

19.0000° N, 99.1333° W

As Data Privacy Violations Increase, So Do Fines

Effie D. Silva

Mexico has a data protection law consistent with a constitutionally protected right to safeguard private personal data. Mexico's Federal Law on Protection of Personal Data Held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) became effective in July 2011 and was followed by the enactment of Mexico's Privacy Law Guidelines, issued in April 2013. Similar to the EU Data Protection Directive, the Privacy Law Guidelines restrict the collection, use and disclosure of personal data. They set forth rules requiring multinationals that process personal data to notify individuals of processing activities and significant security breaches, and include rules specific to cloud computing that trigger fines ranging from $500,000 to $1.6 million (per violation) for serious violations, and sometimes imprisonment. Where sensitive personal data is breached, or where breaches of other personal data reoccur, the sanctions are doubled. In May 2014, mandatory guidelines were released on the implementation of self-regulatory schemes under the law. These additional guidelines require that private parties adopt policies governing personal data management, assign roles and responsibilities to ensure compliance, conduct administrative reviews and apply corrective actions, and impose sanctions.

Article 64 of the Privacy Law Guidelines empowers the authorities to issue fines and up to three years of imprisonment for data controllers for any security breach of databases under their control. In 2014, the Institute of Access to Information and Data Protection (IFAI) reported that in 2013 it issued fines totaling approximately $3.7 million for violations of data privacy laws. That number is expected to increase significantly for 2014, as will be disclosed by the IFAI in early 2015. Indeed, the IFAI recently reported its "anticipation of issuing an abundance of fines" following an unprecedented increase in violations in Mexico.

To prove its commitment to enforcing compliance with the new data laws, in 2014 IFAI issued a $1.3 million fine against Banamex, Mexico's second largest bank, for privacy violations. The IFAI also issued just over $778,000 in fines against the wireless telephone company Telcel, which is owned by telecommunications company América Móvil. Telcel was sanctioned for an alleged failure to process customer data lawfully, fairly and proportionately (a fine of approximately $132,671); alleged failure to obtain consent for disclosure (approximately $142,147); alleged misuse of customer data (approximately $227,436); and alleged failure to keep customer data confidential (approximately $248,758). It also has been reported that IFAI has opened a number of new investigations as a result of the increased number of data protection complaints filed over the past few years.

"In May 2014, mandatory guidelines were released on the implementation of self-regulatory schemes under the law."

Big data and the use of cookies were particularly hot topics in 2014 among European authorities, which continue to address the balance of privacy rights versus legitimate business interests. In South Africa the first sections of the Protection of Personal Information Act came into effect, establishing the Information Regulator, while the African Union took initial steps toward adopting a European-style privacy regime.

EUROPE

45.0000° N, 90.0000° E

Article 29 Working Party Statement on the Impact of Big Data

Rohan Massey

On September 16, 2014, the Article 29 Working Party, an independent European advisory body on data protection and privacy, issued and adopted a statement on big data's impact on the protection of individuals in relation to the processing of their personal data in the European Union. While the Working Party broadly supported the view that big data could bring many potential benefits to EU citizens, it contended that such benefits could only be achieved if users' privacy expectations are appropriately met and their data protection rights respected.

BACKGROUND

Big data is a broad term used for a variety of data processing operations, some of which are well identified, others less so. An example of big data in action is the growing trend of consumer product companies monitoring social media sites for insight into customer behavior and preferences, as well as product perception. Given that big data operations largely rely on extensive processing of EU citizens' personal data, this topic raises important social, legal and ethical questions regarding privacy and data protection rights.

The EU Data Protection Directive (95/46/EC) applies to the processing of personal data in big data operations and ensures a high level of protection for individuals by providing them with specific rights that cannot be waived. Under the Data Protection Directive, data controllers may collect personal data only for specified, explicit and legitimate purposes, and may not process such data in a manner incompatible with those purposes (*i.e.*, the purpose limitation principle). Further, the processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected (*i.e.*, the data minimization principle).

COMMITMENT TO EU DATA PROTECTION PRINCIPLES

Various stakeholders have argued that the data protection principles and obligations under EU law should be substantially reviewed to cater to developments in big data operations. For example, the existing principles of purpose limitation and data minimization are core issues for big data operators, and stakeholders have argued that the law should instead focus on a "use model," *i.e.*, a risk-based approach that takes into consideration only the use of personal data and the potential risk of harm to individuals from the use of such data.

The Working Party rejected this notion, however, and emphasized that EU data protection principles are still valid and appropriate (albeit subject to improvements). The Working Party acknowledged that developments in big data might require a pragmatic and innovative approach to the application of existing EU data protection principles. It maintained, however, that compliance with the existing EU legal framework is a key element in creating and maintaining the trust that any stakeholder needs in order to develop a stable business model based on the processing of such data. Complying with this framework and investing in privacy-friendly solutions is therefore essential to ensure fair and effective competition between economic players in the relevant markets. Furthermore, the Working Party commented that the purpose limitation principle is necessary to ensure that companies that built monopolies or dominant positions before the development of big data technologies hold no undue advantage over newcomers to these markets.

"The Working Party's statement reinforces the status and principles of the Data Protection Directive."

COMMENT

The Working Party's statement reinforces the status and principles of the Data Protection Directive. The statement recognizes purpose limitation as a core data protection principle, but also recognizes that courts should be innovative in their application of the Data Protection Directive in order to cater to developments in big data.

As this area develops in an international context, both competition and compliance issues may be raised within EU Member States' regulatory data protection and privacy frameworks. The Working Party supports increased cooperation between the data protection authorities and the competent global authorities to develop unified guidance and joint enforcement procedures.

Article 29 Working Party Statement on the Risk-Based Approach

Rohan Massey

On May 30, 2014, the Article 29 Working Party published its statement on the role of a risk-based approach in data protection legal frameworks, confirming its support for such an approach, particularly in relation to the proposed reform of the current data protection legislation.

"Adoption of the risk-based approach should in no way weaken individuals' rights regarding their personal data."

BACKGROUND

The Working Party has always supported the inclusion of a risk-based approach in the EU data protection legal framework. The risk-based approach broadly calls for increased obligations proportionate to the risks involved in data processing. Such a provision can pose a burden on data controllers that may be perceived as unbalanced.

The risk-based approach must result in the same level of protection for data subjects regardless of the size of the particular organization or the amount of data processed. This approach is not an alternative to established data protection rights but should be considered a "scalable and proportionate approach to compliance." Therefore low-risk data processing may involve less stringent obligations on data controllers than comparatively high-risk data processing.

KEY MESSAGES

The Working Party provided 13 key messages on this issue:

- Protection of personal data is a fundamental right under Article 8 of the Charter of Fundamental Rights. Consequently, any data processing operation should respect this right.
- The rights granted to data subjects under EU law should be respected regardless of the level of risk.
- The levels of accountability obligations will vary according to the processing risk, but controllers should always be able to demonstrate compliance with their data protection obligations.
- The fundamental principles of data protection applicable to data controllers should remain the same regardless of the processing and the risks for the data subjects. Such principles should be inherently scalable.
- Accountability obligations for data controllers should be varied according to the type of processing undertaken and the privacy risks for data subjects. Not every accountability obligation will always be necessary.
- Documentation of processing activities can also differ according to the risk of the processing, but all controllers should document to some extent their processing activities for the purposes of transparency and accountability.
- Objective criteria should be used when determining the risks and the extent to which processing could potentially negatively affect a data subject's rights, freedoms and interest.
- A data subject's rights and freedoms primarily concern the right to privacy but may also concern other fundamental rights, such as freedom of speech, thought and movement; prohibition on discrimination; and the right to liberty, conscience and religion.
- The risk-based approach requires additional measures when specific risks are identified, and the data protection authorities should be consulted when particularly risky processing has been identified.
- Pseudonymizing techniques are important safeguards that can be taken into account when assessing compliance, because they allow data to be collected without requiring the identity of individuals, and therefore reduce risk to individuals. Such techniques alone do not justify a reduced regime on accountability obligations.
- The risk-based approach goes beyond a harm-based approach that considers only damage. Instead it takes into consideration every potential and actual adverse effect, both at an individual level and for society generally.
- The legitimate interest pursued by data controllers or third parties is not relevant when assessing the risks for data subjects.
- Under the proposed General Data Protection Regulation, data protection authorities will have an active role in respect of the risk-based approach, including developing guidelines on impact assessments and targeting enforcement activity on areas of greater risk, among other things.

COMMENT

The Working Party's statement confirms its general support for the inclusion of a risk-based approach in the EU data protection framework. There are various examples of the existing application of a risk-based approach under the current EU Data Protection Directive (95/46/EC) and from the proposed General Data Protection Regulation. The key issue is that the risk-based approach is to effect "scalable and proportionate" compliance rather than to provide an "alternative to well-established data protection rights." Adoption of the risk-based approach should in no way weaken individuals' rights regarding their personal data.

This clarification of the Working Party's position on the risk-based approach is important because it clears the misconception that the approach will reduce the data protection rights afforded to data subjects. A risk-based approach should simply require a data controller whose processing is relatively low risk to have fewer compliance obligations than a data controller whose processing is comparatively high risk.

CJEU Strikes Down Data Retention Directive as Invalid

Sharon Tan and Robert Lister

On April 8, 2014, the Court of Justice for the European Union (CJEU) ruled that the EU Data Retention Directive (06/24/EC) was invalid. This decision is expected to have wide-reaching implications for privacy laws across the European Union.

BACKGROUND

The Data Retention Directive is a product of heightened security concerns in the aftermath of terrorist attacks around the world, and allows national authorities to access the data processed or generated by communications providers on an almost unlimited basis for the prevention, investigation, detection and prosecution of organized crime and terrorism.

To enable such access, the Data Retention Directive imposed obligations on communications providers to retain certain data for between six months and two years. In particular, communications providers were required to retain traffic and location data as well as data necessary to identify users. The Data Retention Directive did not, however, permit the retention of communications' content or the information consulted by users. For example, authorities could require a mobile phone network provider to retain the time and location at which a text message was sent, but could not require the provider to retain the content of the message.

THE RULING

The CJEU held that the requirement imposed on internet service providers and telecom companies to retain data for up to two years entailed a wide-ranging and serious interference with the fundamental rights to respect for private life and the protection of personal data. The CJEU found that the retained data revealed a large amount about the private lives of individuals. For example, the data enabled the identification of the time, place, frequency and persons with whom users had communicated. From this data, a clear picture could be formed of an individual's private life, including his or her daily habits, permanent or temporary places of residence, movement and activities, social relationships and social environments frequented.

MAIN CONCERNS

While the CJEU accepted communications providers' retention of data for use by national authorities for purposes of legitimate general interest, such as the fight against serious crime or public security generally, it ruled that the Data Retention Directive went further than was necessary to fulfill those objectives and thereby violated the principle of proportionality.

In summary, the CJEU had the following concerns with the Data Retention Directive:

- **Generality** – The Data Retention Directive applied to all individuals and electronic communications without exception.
- **No objective criteria** – The Data Retention Directive did not stipulate any objective criteria or procedures with which national authorities should comply in order to access the data.
- **No proportionality of retention period** – The minimum retention period of six months failed to provide for different categories of data to be sufficiently distinguished or for the possible utility of the data in relation to the objectives pursued. Furthermore, the Data Retention Directive did not provide any objective criteria by which to

determine the data retention period that would be strictly necessary according to the circumstances.

- **Insufficient safeguards** – The Data Retention Directive failed to provide sufficient safeguards against abuse and unlawful access or use of the data.
- **Cross-border mobility** – There was no requirement to retain the data in the European Union to ensure compliance with EU or national data protection laws.

COMMENT

The declaration of invalidity takes effect from the date of the Data Retention Directive's entry into force, *i.e.*, May 3, 2006. Communications providers are likely to experience a period of uncertainty about their ongoing obligations, especially in relation to data they currently hold, until the European Commission clarifies the scope of their new obligations and whether it intends to amend the Data Retention Directive or repeal it. EU Member States are also under an obligation to review, and where necessary redraft, their domestic laws to ensure compliance with the ruling.

As with most European legislation, any legislative changes must be reviewed and discussed by the various European institutions in order to become law, a process that usually takes years. It is expected that legislative procedures will commence in 2015. In the interim, the European Commission has stated that it will assess the ruling and its effects, and respond with practical guidance.

EU Data Protection Reform Timeline

Rohan Massey

"The earliest that there could be agreement on the draft regulation is likely to be the first half of 2015."

On March 12, 2014, the European Parliament voted in favor of new data protection laws. The formal First Reading vote confirmed the text of the new draft regulation that was initially approved by the European Parliament's LIBE Committee in October 2013. The Council of Ministers will still have to review the proposed regulation, however, and any amendments the Council makes must then be agreed with the European Parliament.

BACKGROUND

The proposed data protection regulation is intended to replace the EU Data Protection Directive (95/46/EC). Given the changes in technology and the increased availability of personal data in the past 20 years, the European Commission has realized the need to update the existing framework.

The new data protection rules aim to give individuals more control over their personal data and make it easier for companies to work across borders by harmonizing laws between all EU Member States. The fines for breaching data protection rules have also been significantly increased to a maximum of EUR 100 million or 5 percent of global turnover, whichever is greater.

THE LEGISLATIVE PROCEDURE

The ordinary legislative procedure to approve draft regulations in Europe takes approximately two years. In this time period, the draft regulation will be reviewed by the European Parliament (through five committees that are directly involved in the reforms: JURI, ITRE, IMCO, EMPL and LIBE), the Council of the European Union and the European Commission. Once the regulation is agreed and adopted, there will be an additional two-year period before it comes into force to allow businesses time to prepare for the new laws.

The European Parliament and the LIBE Committee have driven the progress on new data protection laws, but there has been frustration with the Council of Ministers for its slow progress. In particular, LIBE Committee Rapporteur Jan Philipp Albrecht stated that any further postponement of the new laws would be irresponsible. EU citizens expect stronger data protection regulation to be introduced, and since Member States have been negotiating these issues for two years, a timely conclusion should be achieved soon. Similarly, Vice President Viviane Reding, who initially proposed the revision of the data protection framework in January 2012, welcomed the resolution with the suggestion to the Council that reform is a necessity and is now irreversible.

The European Commission and the European Parliament's rapporteur had hoped to reach an agreement with the Council in one reading and publish the final regulation before the Parliament dissolved for the May 2014 elections, but the Council did not reach a common position on the draft regulation at First Reading. The next step will be the full Ordinary Legislative Procedure (formerly known as the co-

decision procedure), which is based on the principle of parity and requires the European Parliament and the Council to reach agreement together. There is no formal time limit for this process, but once the Council reaches a common position, the European Parliament usually has three or four months to approve, reject or amend the Council proposal, after which time the Council can take another three or four months to respond. Failing agreement, a Conciliation Committee will be convened, and if it can agree upon a compromise text, that text will be submitted for agreement by the Council and the European Parliament.

COMMENT

Although proposals for the reform of European data protection rules were first introduced in 2012, it is a long process for draft proposals to become law, and there are many hurdles throughout the process where proposals can fail. The First Reading by the Council crystalizes the position of the European Parliament but does not prevent a future European Parliament from rejecting the whole proposition on a Second Reading.

The Council is still reviewing the draft regulation at a technical level, and negotiations on the proposed text between the Council and the European Parliament will begin only once the Council is ready. The earliest that there could be agreement on the draft regulation is likely to be the first half of 2015; the expectation would then be that the revised data protection framework would come into force in 2017.

Although agreement on the draft regulation may appear to be some time away, the potential fines

for breaching the new data protection rules are so significant that companies might consider it prudent to monitor the regulation's progress.

UNITED KINGDOM

51.5000° N, 0.1167° W

ICO Publishes Report on Big Data

Rohan Massey and Robert Lister

On July 28, 2014, the Information Commissioner's Office (ICO), the UK data protection authority, published a report on how businesses can and must ensure that their use of big data operates within national and EU data protection legislation. The report clarifies how data protection principles apply to the use of personal information in big data and highlights the particular legal issues that businesses should consider in order to ensure compliance. In addition, the report directly addresses questions raised by certain commentators as to whether current legislation is suitable for big data.

"The fairness obligation requires data controllers to be transparent when they collect personal information."

BACKGROUND

The term big data generally refers to the high-speed analysis of very large datasets, often including data from different sources. Examples referenced in the report include meta-data from internet searches, credit and debit card purchases, social media postings and mobile phone location data. Big data is frequently analyzed using algorithms and repurposed by businesses to tailor their products and services to individual customers or to specific customer characteristics. The report notes that the public sector increasingly is using big data analytics for purposes such as scientific research, national security and government transparency.

The ICO's interest in big data stems from the potential data protection and privacy risks related to personal information. Datasets containing no personal information or anonymized data are of little concern to the ICO, but when personal information is used, the relevant data controller and any processors are required to comply with the EU Data Protection Directive (95/46/EC) and any applicable national implementing legislation, such as the UK Data Protection Act 1998 (DPA).

The ICO recognizes that big data involves rapid technological development and that its potential uses are increasingly expansive. Accordingly, the ICO's intention in publishing the report was to review big data's primary data protection and privacy issues balanced against the potential benefits of its application, and to contribute to current debate on the topic.

KEY MESSAGES

Fair Processing

The ICO's primary concern is that businesses using personal information ensure that their processing activities are "fair," in particular where processing may affect individuals. Although big data operations are often highly complex, data controllers are not excused from complying with their obligations under the DPA. The fairness obligation requires data controllers to be transparent when they collect personal information, clearly explain what information will be collected and how it will be used, and obtain data subject consent where required. The ICO report also suggests that the fairness concept involves a wider assessment of whether the processing would fall within the reasonable expectations of data subjects, taking into account the reasons that the data was submitted originally.

Conditions of Processing

The ICO clarifies the three processing conditions most likely to apply to commercial big data uses. At least one of these must be satisfied in order to comply with the DPA.

First, a data processor may obtain freely given, specific and informed consent. Data subjects must be able to understand the intended purposes for which their data is collected and must give a clear indication that they consent to the collection. If an organization decides to use the personal information for a purpose other than that to which the subjects originally consented (or in a manner not immediately apparent to the data subject), data controllers should make their data subjects aware of this change and obtain opt-in consent where such different purposes may affect data subjects (*e.g.*, processing activities aimed at discovering information about particular individuals rather than general trends). The ICO also clarifies that data subjects must be able to withdraw their consent.

Second, the processing may be necessary for the performance of a contract in which the data subject

is a party. The ICO warns data controllers that this condition may be difficult to satisfy, because by its very nature, big data often goes beyond what is strictly necessary to sell products or deliver a service. The ICO concedes, however, that this condition may be satisfied with respect to emerging payment methods.

Finally, the processing may serve the legitimate interests of the data controller or other parties. Per the ICO, data controllers must balance establishing a legitimate interest (*e.g.*, profiling customers to better focus marketing, or to prevent fraud or misuse of services) against data subjects' privacy rights. If there is another way to meet the legitimate interest that interferes less with people's privacy, then the processing will not be deemed "necessary."

Data Minimization

The report affirms the concept of data minimization, *i.e.*, the principle that organizations should minimize both the volume of data collected and the length of time that it is kept. The ICO recognizes that big data could be seen as excessive by its very nature, since it is often focused on collecting as much information as possible. In order to address this issue, the ICO recommends that organizations clarify from the outset why they are collecting the data and what they intend to do with it, and that they use that context to determine whether the data is relevant and not excessive for such purposes. In addition, while the ICO concedes that it has not seen evidence of organizations keeping data longer than is necessary following advances in digital storage, it suggests that organizations anonymize data if they wish to keep it for a long time.

Security

The ICO suggests that big data may increase the risk of threats to information security, but argues that such risks can be mitigated and controlled if organizations undertake proper risk assessments (often based on their standard risk-management policies) and take appropriate measures to ensure security following such assessments. Where cloud services are used, data controllers must obtain sufficient guarantees from the relevant provider that appropriate security measures are in place.

Response to Critics

The ICO outlines its objections to claims that current data protection principles are not appropriate in the context of big data. It contends that the data protection principles are inherently flexible, apply to big data just as they do to any other data containing personal information, and should not be seen as a barrier to progress. Instead, data protection principles should be viewed as an incentive to develop new approaches and better engage with the public.

Anonymization

The ICO helpfully points out that to the extent personal information in big data is anonymized (*i.e.*, it is not possible to identify the relevant individuals), it will no longer constitute personal information and therefore may be used or shared without further DPA compliance obligations. The ICO gives examples of organizations that anonymize their data for the purposes of analysis and recommends anonymization as a useful step for organizations to consider. At the same time, the ICO warns organizations not to underestimate the difficulty of irreversibly anonymizing data such that individuals can no longer be identified, in particular when such data is viewed in combination with other datasets.

COMMENT

Parties that undertake or intend to undertake big data analytics may take comfort that big data is "not a game played by different rules" and that simple transparency is often the key to achieving compliance with the data protection principles. However, those calling for more prescriptive legislation and certainty in their processing activities are likely to be disheartened by the ICO's continued focus on a risk-based approach.

"Data protection principles should be viewed as an incentive to develop new approaches and better engage with the public."

House of Lords Publishes Inquiry into Right to Be Forgotten

Sharon Tan and Robert Lister

On July 30, 2014, the European Union Committee, a select committee of the House of Lords, published a report on the "right to be forgotten" under the EU Data Protection Directive (95/46/EC) and the relevant UK implementing legislation under the Data Protection Act 1998. The report reviews the status of the right to be forgotten following a 2014 decision on the issue by the Court of Justice of the European

Union (CJEU), analyzes the wider implications of the decision and outlines recommendations for possible future reform.

BACKGROUND

Under Article 6.1(d) and 12 of the Data Protection Directive, data subjects have the right to require data controllers to rectify or erase inaccurate or incomplete personal data. On May 13, 2014, the Spanish Data Protection Agency (SDPA) upheld a complaint from a Spanish citizen relating to online searches of his name. The search results contained a newspaper advertisement from 1998 regarding property owned by him that was being auctioned because of unpaid debts. The SDPA held that the search engine should be required to remove or conceal the personal data in question so that it was no longer included in the search results.

"The committee strongly opposes EU data protection legislation reform that would allow an ever-wider right to be forgotten."

The matter proceeded to the Spanish High Court, which subsequently referred the following questions on the interpretation of the Data Protection Directive to the CJEU:

What is the territorial scope of the Data Protection Directive?

The CJEU held that the Data Protection Directive extends to cover organizations based outside the European Union that have operations in the European Union, even where those operations do not include the processing of data.

Is a search engine a data controller for the purposes of the Data Protection Directive?

The CJEU clarified that an operator of a search engine must be regarded as the controller of the personal data processed by the search engine, despite not strictly having control over such data published on third-party websites.

To what extent is there a right to be forgotten?

The CJEU concluded that web users have the right to directly request search engines to delete the links to websites containing information breaching their rights under the Data Protection Directive, even if the publication of such information was lawful in itself. Furthermore, the CJEU held that this right applies even where the data is not prejudicial to the data subject; the data only needs to be inadequate, irrelevant or excessive for this right to apply.

BURDEN ON SEARCH ENGINES

The European Union Committee's report describes how the CJEU ruling has a binding effect on all search engines. Since the ruling, some search engines have reported receiving high numbers of removal requests, which involve the examination of a greater number of URLs.

In its report, the committee also confirms that the CJEU ruling requires search engines to examine each removal request and decide whether the information in the disputed link is inadequate, irrelevant or excessive in relation to the purposes for which the data is processed. Additionally, search engines must make a value judgment as to whether interference with a subject's fundamental rights would be justified in light of the general public's interests in having access to the information in question. The committee argues that the test outlined by the CJEU is vague, ambiguous and unhelpful, and that such value judgments should not be left to individual search engines, which may reach different conclusions with regard to the same removal request.

In particular, the committee raises concerns that smaller or new search engines might not be able to comply with the CJEU's ruling as easily as larger, more established search engines if they receive a large number of removal requests. Search engines might resort to automatically withdrawing links subject to removal requests if they lack the resources to examine requests on a case-by-case basis—potentially allowing any individual an uncontested right to censorship.

OTHER POTENTIAL EFFECTS OF THE RULING

The report highlights how the definition of "data controller" creates conceptual difficulties—if search engines are to be considered data controllers, then by logical extension, search engine users could be considered to be processing personal data. The notion that search engine users could fall within the definition of a data controller is counterintuitive and could expose shortcomings in the Data Protection Directive, the committee argues.

The CJEU's ruling also will require search engines, national data protection authorities and the CJEU itself to divert resources to respond to the potentially huge number of requests that have been and are

predicted to be received in the future. The committee expresses acute concern about the potential effect on UK businesses, particularly small and medium-sized enterprises and start-ups. In the future, organizations might need to incorporate privacy by design and consider what impact their technology and business methods will have on the privacy of individuals. Such additional costs could hinder many companies from moving beyond the start-up phase.

THE COMMITTEE'S RECOMMENDATIONS

The committee strongly opposes EU data protection legislation reform that would allow an ever-wider right to be forgotten, and argues that the right to privacy should not give data subjects the right to remove links to accurate and lawfully available data. In the committee's view, to allow otherwise would be misguided and unworkable in practice.

While the committee believes there are compelling reasons why search engines should not be classified as data controllers, it stopped short of recommending that search engines be excluded from the upcoming Data Protection Regulation, given the CJEU's interpretation of the Data Protection Directive. Instead, the report recommends that the UK government ensure that the definition of "data controller" accords with reality, and that the new regulation is amended to clarify that the term does not include ordinary users of search engines.

THE ARTICLE 29 WORKING PARTY'S RECOMMENDATIONS

Following the report, the EU Article 29 Working Party acknowledged the high public demand for the right to be forgotten and proposed a more uniform approach to the handling of de-listing complaints. The Working Party proposed the establishment of a network of dedicated contact persons within national data protection authorities to develop common case-handling criteria. Such a network would provide the data protection authorities with a record of decisions on complaints and a dashboard to assist in reviewing similar, new or more difficult cases.

COMMENT

The European Union Committee states that it is critical for data protection law to evolve in a way that achieves a fair balance between the competing fundamental rights of privacy and freedom to seek and impart accurate information lawfully acquired. In the committee's view, neither the Data Protection Directive nor the CJEU's interpretation thereof accurately reflects the current state of

communications service provision, where global access to detailed personal information has become part of everyday life. With radical revision of this area of law expected in the near future, the committee is expected to keep developments in EU data protection legislation under scrutiny.

GPEN Publishes Privacy Sweep Results Following UK Mobile App Guidance

Sharon Tan and Robert Lister

On September 10, 2014, the Global Privacy Enforcement Network (GPEN) published the results of its privacy enforcement survey, or "sweep," carried out earlier in 2014 with respect to popular mobile apps. The sweep aimed to determine the transparency of the privacy practices of 1,211 mobile apps and involved the participation of 26 data protection authorities around the globe. The sweep results indicate that a high proportion of the apps downloaded did not sufficiently explain how consumers' personal information would be collected and used, and likely will lead to future initiatives by national data protection authorities to protect personal information submitted to mobile apps.

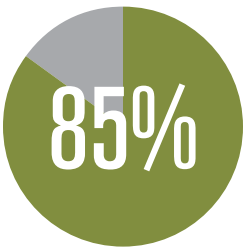
BACKGROUND

GPEN was established in 2010 on the recommendation of the Organisation for Economic Co-operation and Development. GPEN aims to create cooperation among data protection authorities throughout the world in order to strengthen personal privacy globally, and currently includes 51 data protection authorities across 39 jurisdictions.

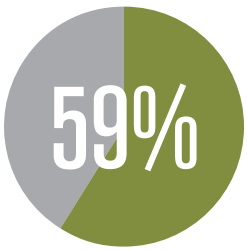
Over the course of a week in May 2014, GPEN's "sweepers"—made up of 26 data protection authorities, including the UK Information Commissioner's Office (ICO), across 19 jurisdictions—participated in the survey by downloading and briefly interacting with the most popular apps released by developers in their respective jurisdictions, in an attempt to recreate a typical consumer's experience. GPEN intended the sweep to increase public and commercial awareness of data protection rights and responsibilities, and to identify specific high-level issues that could become the focus of future enforcement actions and initiatives.

SWEEP RESULTS

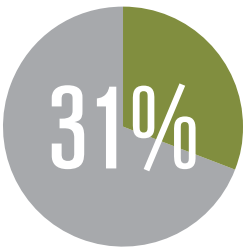
The GPEN sweep's key negative findings include the following:



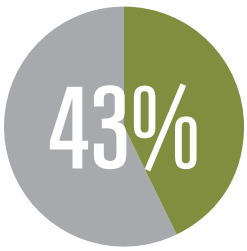
85 percent of apps failed to clearly explain how personal information would be processed.



59 percent of apps did not clearly indicate basic privacy information (with 11 percent failing to include any privacy information whatsoever).



31 percent of apps were excessive in their requests for permission to access personal information.



43 percent of apps had not sufficiently tailored their privacy communications for the mobile app platform, often relying instead on full-version privacy policies found on websites.

The sweep results also highlighted a number of best practices for app developers. Many apps provided clear, easy-to-read and concise explanations of exactly what information would be collected, how and when it would be used, and, in some instances, what would not be done with such information. Some apps also provided links to the privacy policies of their advertising partners and opt-out elections in respect of analytic devices.

The sweep yielded good examples of privacy policies specifically tailored to the app platform by successfully employing just-in-time notifications (warning users when personal information is about to be collected or used), pop-ups and layered information to allow consumers to obtain more detailed information if required.

UK MOBILE APP GUIDANCE

While the GPEN sweep results are useful for developers across Europe, UK developers and those seeking to develop apps for the UK market can obtain further information on compliance with UK data protection legislation from the ICO's privacy in mobile apps guidance, published on December 19, 2013. This guidance was produced after surveys revealed that a majority of UK app users were concerned about how apps used personal information, and that almost half had not downloaded or had deleted an app because of privacy concerns. The ICO guidance aims to give UK developers the best chance of achieving commercial success by explaining the legal requirements for using personal information, including issues of consent and security.

In addition to the best practices identified previously in relation to the GPEN sweep, the ICO recommends that app developers take the following steps:

- Aim to use the least privacy-intrusive data possible.
- Pay special attention to personal information collected for apps targeted at or frequently used by children.
- Implement "privacy by design" throughout development, covering issues such as privacy-friendly defaults and effective user control over privacy settings, allowing users to quickly and easily review and change their decisions or consents.
- Undertake privacy impact assessments throughout development, considering the types of data the app might access, collect or transmit; the potential effect on users of such access, collection or transmission; how important the data is for the purposes of the app; and applicable justifications for collecting such data.
- Do not collect data just in case it might be needed in the future (even where users consent to such collection).
- Ensure that passwords are appropriately salted and hashed when stored on central servers, and use encrypted connections such as SSL/TLS wherever usernames, passwords and sensitive information such as unique IDs are transmitted.
- Establish defined data retention periods, encrypt stored data and ensure permanent deletion of personal information on expiry of the relevant period.
- Properly test and maintain apps to ensure they function as intended and that personal information is not collected or processed in respect of users who do not consent to such processing.
- Consider the requirements of other legislation, such as the Privacy and Electronic Communications Regulations, when apps are designed to send e-mail, SMS or voicemail messages; make phone calls; set cookies or other tracking devices; or engage in viral marketing.

"The sweep yielded good examples of privacy policies specifically tailored to the app platform."

COMMENTS

Many GPEN members are expected to take further action in response to the sweep results. The ICO has commented that it and other GPEN members intend to write to developers identified as deficient. The Belgian Privacy Commission has confirmed that gross violations of data protection law identified in the sweep will be forwarded to and dealt with by the relevant authorities.

UK developers of mobile apps and those intending to develop apps for the UK market should consider closely reviewing the ICO's privacy in mobile apps guidance. The guidance is particularly useful in setting out clear, practical examples of best practices, together with issues to avoid. In addition, consumers generally may find the guidance to be a helpful source of information on their privacy rights.

GERMANY

52.5167° N, 13.3833° E

Video Surveillance in the Workplace

Dr. Paul Melot de Beauregard and Maximilian Baur

In recent years, Germany has seen a number of high-profile cases regarding the use of video surveillance systems (CCTV) in the workplace, including the Lidl case. Lidl, one of Germany's largest supermarkets, was unlawfully monitoring employees via CCTV. Because surveillance took place in unorthodox locations such as bathrooms, the company faced a great deal of media outrage and negative publicity. Cases such as this have made the use of CCTV in the workplace a heavily disputed issue under German labor law.

"Terminations based on illegal recordings are held legally void by German labor courts."

The coalition agreement of December 2013 stipulates possible new legislation if the proposed European data protection law reform does not happen. For now the government has adjourned new legislation on data protection, so the current provisions and rules on the use of CCTV in the workplace continue to apply. If an employer illegally uses video surveillance, the respective recordings may not be admissible in court; an employee's personal rights justify the exclusion of such video recordings. Terminations based on illegal recordings are held legally void by German labor courts. Employers may face criminal prosecution and administrative fines, as well as claims for damages from affected employees.

VIDEO SURVEILLANCE IN PUBLIC AND PRIVATE WORKPLACE SPACES

As a rule of thumb, German law differentiates between video surveillance in public and private areas, and between concealed and overt video surveillance. Surveillance in public spaces (*e.g.*, the service counter area of a bank) is legal as far as it serves precisely defined purposes and is required to pursue an employer's legitimate interests, and as long as an employee's personal rights do not prevail (sect. 6b German Federal Data Protection Act).

The wording of the relevant provision does not include concealed surveillance in public areas; CCTV in public areas is statutorily required to be recognizable. Certain commentators in legal literature therefore argue that concealed surveillance is generally illegal under German law. However, the German Federal Labor Court decided in 2012 that the requirement for CCTV to be recognizable does not call for a general ban on concealed video surveillance in public areas. The court argued that an employer's interests in concealed video surveillance could prevail over an employee's personal rights in certain cases. For example, an employer may use concealed CCTV for protection of proprietary rights. The textbook scenario would be reasonable suspicion of criminal offenses committed by an employee (*e.g.*, theft). Overt video surveillance would not produce evidence in such cases, as a suspect would act accordingly if he or she was aware of video monitoring.

German data privacy law does not explicitly regulate use of CCTV in non-public areas in the workplace (*e.g.*, offices, storage rooms). According to the general clause of sect. 32 German Federal Data Protection Act, an employee's data may be collected, processed or used for employment-related purposes where necessary for hiring decisions or for carrying out or terminating the employment contract.

Whether video surveillance is considered necessary for these purposes must be determined by evaluating the conflicting interests in each specific case. Employees' personal rights usually take priority over an employer's interests, unless legitimate interests justify an exception. Permanent observation is never considered legal under German law. Additional requirements regarding an employer's interests apply when concealed video surveillance is used. The German Federal Labor Court has defined such use as a "last resort" for an employer in cases of possible criminal offenses or other serious breaches of contract. In any case, concealed video surveillance must focus on the suspect and on the relevant areas only (*e.g.*, checkout areas).

INADMISSIBILITY IN COURT

Should the previously mentioned requirements not be met, concealed video recordings may be inadmissible in court. Video recordings violating an employee's basic personal rights (*e.g.*, recordings of bathrooms) never may be used in court. However, inadmissibility of illegal recordings from other areas is not automatic. According to new guidance by the German Federal Labor Court, evidence that has been obtained by illegal means may be used legally in court proceedings

if such use does not constitute or perpetuate a further breach of personal rights.

Breaches of the German Federal Data Protection Act rules of procedure may not lead to inadmissibility. Illegal video recordings, however, are generally inadmissible if an employer unilaterally terminates an employment relationship solely based on such recordings. In the worst-case scenario, a dismissal may be judged legally ineffective even though a breach of contract can be unambiguously identified on video.

COMMENT

Employers should be cautious when using video surveillance in the workplace in Germany, and should consider using overt rather than concealed systems. The data protection officer or relevant data protection authority should be contacted before the required technology is set up. During the whole process, transparency with staff increases an employer's chances of legally using video recordings in court proceedings.

Anti-Stress Legislation and Data Privacy

Dr. Paul Melot de Beauregard and Maximilian Baur

German Employment Minister Andrea Nahles is vocally promoting new "anti-stress" legislation. Such legislation would be aimed at banning employers from contacting their employees outside of working hours. Although German Chancellor Angela Merkel has supposedly rejected these plans for good, the Federal Institute for Occupational Safety and Health is conducting a study on the relationship between constant availability and an increase in mental fatigue and illness among German employees. After the study is completed in 2016, the German Labor Ministry will evaluate possible new legislation.

Certain German employers have already implemented restrictions on contacting employees during their time off. In 2013, the German Labor Ministry banned its managers from contacting employees after hours. Daimler, one of Germany's marquee car manufacturers, has taken a distinctively radical approach. In summer 2014, the company installed new software that allows employees to have incoming e-mails automatically deleted while they are on vacation. Should such a model become statutory law, it could raise certain issues regarding data protection law, in particular relating to private e-mails.

Breaches of German data protection law can be sanctioned with administrative fines and imprisonment. Generally, an employer is not allowed to read an employee's private e-mails. From a data protection standpoint, the implications of new anti-stress approaches such as Daimler's could be substantial. For example, if e-mails are automatically forwarded to a colleague while an employee is on vacation, such forwarding could be deemed an illegal transfer of personal data if personal e-mails are involved. An administrative fine for such a breach could amount up to EUR 300,000. Furthermore, the automatic deletion of e-mails without an employee's consent during his or her vacation could constitute a criminal offense. Under German law, whoever deletes, suppresses, renders unusable or alters data can be punished with imprisonment for up to two years or a fine. Because personal e-mails constitute personal data, employers should implement an option for staff to opt in or out of such automatic deletion processes.

Data privacy issues have not yet played any part in the public discussion regarding anti-stress legislation, and it remains to be seen if new anti-stress regulations will become law. In the meantime, German data protection authorities could evaluate anti-stress restrictions by an employer to provide further clarity on the matter. To date, such evaluation has yet to take place.

"An administrative fine for such a breach could amount up to EUR 300,000."

ITALY

41.9000° N, 12.4833° E

Italian Data Protection Authority Guidelines on Cookies

Veronica Pinotti, Martino Sforza and Nicolò Di Castelnuovo

On May 8, 2014, the Italian Data Protection Authority published its Guidelines to Provide Information and Obtain Consent Regarding Cookies, which set out simplified procedures for providing online information on the use of cookies to users and obtaining their consent, whenever required by law. The guidelines distinguish between technical cookies (including browsing cookies, analytics cookies and functional

cookies) and profiling cookies (*i.e.*, cookies that are aimed at creating users' profiles, and which must be notified to the Authority). Technical cookies do not require any user consent, but do require the provision of certain information to users under Article 13 of Legislative Decree no. 196 of June 30, 2003. Profiling cookies require users to be informed appropriately on the use of such cookies so that users can give their valid consent.

"Publishers and third parties have one year to comply with the guidelines following their June 3, 2014, publication in the *Official Journal*."

The guidelines also distinguish between publishers and third parties, depending on whether the entity is installing cookies on a user's terminal, and clarify why publishers are not required to provide information on, or obtain consent for, the installation of third-party cookies. According to the guidelines, publishers are data controllers with regards to processing carried out by cookies that the publishers installed, but they are mere "technical intermediaries" with regards to processing carried out by third-party cookies. Therefore publishers may not be required to include any notices on their home pages relating to third-party cookies. A similar approach applies to the consent required for profiling cookies. In this scenario, publishers act as data controllers with regards to cookies directly installed by their websites, and as "technical intermediaries" between third parties and users with regards to cookies installed by third parties. In order to keep publishers' responsibilities separate from the responsibilities of third parties, the guidelines require publishers to acquire links to the third parties' information notices and consent forms at the time they enter into the relevant agreements.

Further, the guidelines set out the particular methods for providing privacy notices and obtaining user consent where cookies are used. Similar to guidance issued in other European jurisdictions, the guidelines call for a two-tier privacy notice that includes the following:

- A short privacy notice displayed on a banner that appears on the website homepage (a sample of which has been published on the Authority's website)
- An extended privacy notice, accessible through a link

The guidelines set out in detail the content of both the short privacy notice and the extended privacy notice.

Publishers and third parties have one year to comply with the guidelines following their June 3, 2014, publication in the *Official Journal*. Failure to comply may result in fines ranging from EUR 6,000 to EUR 36,000 (for failure to provide adequate privacy notice), EUR 10,000 to EUR 120,000 (for installing cookies without the user's prior consent), and EUR 20,000 to EUR 120,000 (for failure to submit a complete notification to the Authority).

The guidelines provide useful guidance to publishers regarding their obligations to inform users about the use of cookies, as well as how to obtain users' consent. Furthermore, by distinguishing between publishers and third parties, the guidelines appropriately outline the relevant roles and responsibilities regarding information to and consent from users in relation to third-party cookies.

New Data Privacy Rules on Mobile Payments

Veronica Pinotti, Martino Sforza and Nicolò Di Castelnuovo

On May 22, 2014, the Italian Data Protection Authority published new rules on the processing of personal data for mobile payments (*e.g.*, via smartphone devices and tablets). Mobile payment services include mobile remote payment and mobile proximity payment (*i.e.*, payment through mobile devices incorporating near field communication technology). The new rules only concern mobile remote payment; the Authority will address other types of mobile payment technology in separate rules.

The purpose of the new rules, which follow a public consultation launched in January 2014, is to offer greater protection to users who purchase goods or subscribe to services through new means of e-payment via smartphones, tablets or personal computers. The rules apply to telecoms operators, merchants and technology aggregators, and to other parties involved in the provision of mobile remote payment services, such as app providers that enable users to buy digital content, games or software with phone credit. The rules establish the obligations for information and consent, security measures and data retention for each entity involved in the provision of mobile remote payment services.

Users must receive complete information on how their personal data is processed, in compliance with Legislative Decree no. 196 of June 30, 2003. In particular, the information notice must state all purposes of the data processing, specifically whether users' data will be processed for marketing purposes. Specific consent is required if data is used for marketing or profiling purposes, or if data is communicated to third parties. The requirement to provide information to users applies to both operators and merchants acting as data controllers, and also to aggregators when acting as autonomous data controllers.

Operators, aggregators and merchants must adopt the minimum security measures required under Legislative Decree no. 196 as well as the appropriate security measures provided by the new rules to ensure the confidentiality of personal data. These measures include strong authentication mechanisms for accessing data, procedures for tracking operations and cryptographic systems to protect data.

Personal data processed by operators, aggregators and merchants may be kept for a maximum of six months; once this period has elapsed, data must be erased. Merchants must erase users' IP addresses once the purchase process is complete. Failure to comply with the measures prescribed by the Authority may result in fines under Legislative Decree no. 196. Given the growing use of mobile payments and the potentially far-reaching scope of the new rules, the Authority likely will continue to closely monitor such services and enforce the new rules in case of breach.

New Rules on Biometric Data Use in Italy

Veronica Pinotti, Martino Sforza and Nicolò Di Castelnuovo

On November 26, 2014, the Italian Data Protection Authority announced the adoption of the general decision and guidelines on the processing of biometric data. The general decision and guidelines were under public consultation until June 24, 2014, and their adoption follows the large number of notifications received by the Authority concerning the processing of biometric data and its increased use in various fields, as highlighted at the European level by the Article 29 Working Party in its Opinion 3/2012 on developments in biometric technologies.

Biometric data is defined as data relating to "biological properties, behavioral aspects, physiological characteristics, living traits or repeatable actions

where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability."[1] Biometric systems are closely linked to a person because they can use certain unique properties of an individual for identification or authentication. While a person's biometric data can be deleted or altered, the source from which the data has been extracted in general cannot be altered or deleted.

The development of biometric technologies has helped make many operations more convenient and has made access control systems more reliable, but it also has introduced new threats to fundamental rights, such as genetic discrimination and identity theft. In recent years, the Authority has received an increasing number of requests for prior assessment concerning the processing of biometric data. Under Article 17 of Legislative Decree no. 196 of June 30, 2003, if a processing activity is likely to present specific risks to data subjects' fundamental rights, freedoms and dignity (whether on account of the nature of the data, the arrangements applying to the processing or the effects the latter may produce), the data controller must request a prior assessment by the Authority, which lays down the measures and precautions required to safeguard data subjects' rights.

The general decision identifies the following four categories of biometric data processing that, on the basis of the Authority's experience, are exempt from preliminary assessment under Legislative Decree no. 196:

- Technologies that use fingerprints as credentials for electronic authentication
- Biometric systems based on the processing of fingerprints or the topography of the palm to grant or limit access to sensitive areas or premises (*e.g.*, locations of confidential activities, dangerous manufacturing activities or machinery, or storage of high-value objects)
- Biometric technologies used to facilitate access to public or private premises (*e.g.*, libraries, and gyms or private airport areas, respectively) or services (*e.g.*, opening safe-deposit boxes or accessing bank vaults)
- Advanced signature of electronic documents

1 Opinion 3/2012 on developments in biometric technologies, page 3.

The general decision sets out stringent measures specific to each of these categories that must be implemented in order for the categories to be exempted. These measures include supplementary security measures, strong encryption methods, recording of access logs and compliance with International Organization for Standardization standards.

The guidelines address the various types of biometric processing that currently exist, including those that continue to require the prior assessment of the Authority (*e.g.*, retina scans and facial recognition), and set out specific security measures and processing methods in addition to those already envisaged by Legislative Decree no. 196. The guidelines stress that the Authority will pay particular attention to the security measures of mobile technologies, such as tablets and laptops.

FRANCE

47.0000° N, 2.0000° E

Data Protection Authority's Investigative Powers Strengthened by Online Control

Myrtille Lapuelle and Jilali Maazouz

In order to ensure compliance with data protection legislation, the French Data Protection Authority (CNIL) has been given investigative powers. Until recently, such investigative powers were limited to three main procedures:

- Onsite inspections, during which CNIL can access business premises and inspect hardware and software on which personal data is stored
- Offsite controls that allow CNIL to send written injunctions asking for specific documents and files to verify that data processing practices are compliant
- Hearing procedures allowing CNIL to summon people involved in data processing to a hearing at its offices in order to obtain any relevant information

The Consumer Protection Act that came into force on March 17, 2014, gave CNIL the power to conduct online

controls designed to remotely detect infringements of the French Data Protection Act. This power is limited to freely accessible online data, including information accidentally or negligently made available, and information disclosed by a third party. CNIL has specified that this power cannot be used to bypass security measures implemented to protect websites.

Infringement findings are listed in an official report, sent to the entities or individuals involved, and are enforceable against them. Unlike reports adopted after onsite and offsite inspections, which must be drafted in a contradictive way, reports following an online control are not subject to such an obligation.

CNIL's new investigative powers are designed to help it adapt to digital development, and should improve its efficiency and responsiveness in what is a fast-changing environment. This new power likely will significantly increase the number of investigations carried out. While CNIL conducted 414 controls in 2013, it aims to conduct 550 controls by the end of 2014. CNIL intends that 200 of these will involve online investigations. It is clear that CNIL's new powers represent a significant step forward in the protection of French citizens' personal data.

Number and Seriousness of Sanctions on the Rise

Myrtille Lapuelle and Jilali Maazouz

During recent years, the sanctions imposed by the Data Protection Authority (CNIL) for violations of the Data Protection Act have increased, both in number and in severity. In 2011, all eight sanctions imposed by CNIL were warnings. In contrast, in 2012 CNIL imposed 15 sanctions, including four fines of more than EUR 1,000, and in 2013 it imposed 13 sanctions, including five fines of more than EUR 3,000. Of the 12 sanctions that have been imposed so far in 2014, only three were warnings, and six were fines of more than EUR 3,000.

The most severe of these fines was a EUR 150,000 monetary penalty imposed by CNIL's Sanctions Committee on a major search engine following a finding that its privacy policy failed to comply with the French Data Protection Act. Specifically, the search engine did not sufficiently inform its users of the conditions in which their personal data was processed, nor of such processing's purpose. Consequently, data subjects were not able to exercise their rights, particular those of access, objection and deletion.

"Cookies Sweep Day" – a European Coordinated Action for Cookies Controls

Myrtille Lapuelle and Jilali Maazouz

In 2014, the Data Protection Authority (CNIL) continued its work on international cooperation between data protection authorities and participated in the international controls campaign. The campaign was organized by the G29 and sought to harmonize European authorities' current practices regarding cookies.

Cookies are tracers placed on internet users' hard drives by website hosts. They allow websites to identify a single user across multiple visits with a unique identifier. EU Directive 2002/58/EC on privacy and electronic communication imposes an obligation to obtain users' prior consent before placing or assessing cookies and similar technologies on users' devices—an obligation transposed into French law by Article 32-II of the French Data Protection Act. Not all cookies require prior consent; some tracers, such as functional cookies, are exempt from the consent obligation.

Website owners can rely on tools made available by CNIL to ensure their compliance with cookie requirements. In December 2013, CNIL released guidelines explaining which cookies are subject to the consent requirement and how consent can be obtained for the use of cookies and other online trackers in compliance with EU and French data protection requirements.

From September 15 to 19, 2014, CNIL organized a "cookies sweep day" to examine compliance with its guidelines. Other data protection authorities across the European Union undertook parallel sweeps simultaneously. The purpose of the coordinated action was to compare practices on the information that websites must give to internet users and the methods implemented to obtain consent for cookies.

"In October 2014, CNIL also began conducting onsite and remote controls to verify compliance with its guidelines on cookies."

In October 2014, CNIL also began conducting onsite and remote controls to verify compliance with its guidelines on cookies. Depending on the findings of the sweep and inspections, CNIL may issue warnings or financial sanctions to non-compliant websites and applications. Such initiatives reflect CNIL's aim to modernize its approach and introduce more effective personal data protection.

SPAIN

40.4333° N, 3.7000° W

SPDA Clarifies Content and Structure of Cookie Policies

Rohan Massey and Robert Lister

In 2014, the Spanish Data Protection Agency (SDPA) published a report that clarifies the definition of the term "cookie" and outlines in detail the information that must be provided in the second layer of Spanish cookie policies.

"The Convention seeks to establish a legal framework for ensuring privacy and data security throughout the African continent."

BACKGROUND

Article 5(3) of the EU E-Privacy Directive (2002/58/EC) obliges Member States to ensure that the use of electronic communication networks to store information in a user's browser is only allowed if the user is provided with, or given access to, "clear and comprehensive information" about the purpose of the storage, and has given his or her consent. The Directive is implemented into Spanish law by Article 22 of Law 34/2002 on Information Society Services and E-Commerce (as amended in March 2012).

Similar to other national implementing legislation in Europe, Spanish legislation allows a user's consent in relation to the use of cookies to be express or implied. Implied consent can be obtained through browser or application settings provided that a positive action by the user is required. Consent is only valid if the user has been fully and duly informed. For that reason, the SDPA recommends using a two-layer information system to inform users and ensure that their valid consent is obtained.

In previous reports, the SDPA has stated that the first layer of information must be provided to users on their first visit to the service provider's website through a header, footer or pop-up window. Broadly, this first layer must warn users (1) whether cookies (including third-party cookies) are used and for what purposes, and (2) that performing a certain action (*e.g.*, continued use of the website) implies acceptance of the cookies. In addition, the first layer must provide the opportunity to refuse the use of cookies and provide a link to the second layer of information. According to the SDPA, this first layer must appear prominently upon first viewing of the website and should not simply set out the service provider's full privacy or cookie policy.

The SDPA's 2014 report focuses on the additional information to be provided in the second layer of cookie policies. The report also clarifies that the term "cookie" includes all mechanisms that allow the storage and recovery of data from users' devices.

COOKIE POLICIES

According to the SDPA, the second layer must contain additional information about cookies, and in particular must explain the following:

- What cookies are and for what purposes they are generally used
- What types of cookies are used on the relevant website and the particular purpose(s) for which they are used
- Whether any third-party cookies are used, and if so, identification of the relevant third party and a link to additional information
- Which entities intend to use the data collected by cookies, including third parties where relevant
- How to disable or delete cookies through specific website or application functionality, browser settings or common platforms that exist for such purposes
- How to withdraw consent to the use of cookies, and an opportunity to do so

Regarding the second point above, the SDPA comments that a general description categorizing cookies into broad groups based on functionality generally will be sufficient, provided it does not cause ambiguity for users and the purposes, uses and owners of the relevant cookies are sufficiently explained.

Detailed tables of information on all cookies used are not required, but there is nothing to prevent entities from providing them. Service providers also can provide links to third-party websites in order to provide additional information as long as the links function properly, provide accurate and up-to-date information, and refer users to information in Castilian Spanish or one of Spain's other official languages. The SDPA specifically warns service providers that links to information in English or any other non-official language will not be admissible.

COMMENT

While the SDPA's report is unlikely to surprise those well versed in the E-Privacy Directive, the guidance is nonetheless useful for providers considering whether existing or new cookie policies are sufficient to comply with Spanish legislation. Service providers in other jurisdictions also may find the report a useful reminder of their own obligations, since many European jurisdictions provide for very similar, if not identical, requirements.

AFRICA

African Union Adopts Convention on Cybersecurity and Personal Data Protection

Heather Egan Sussman

On June 27, 2014, the Convention on Cybersecurity and Personal Data Protection was adopted during the 23rd Ordinary Session of the Summit of the African Union. The Convention seeks to establish a legal framework for ensuring privacy and data security throughout the African continent, and is divided into three substantive parts. The first part addresses electronic commerce, including security of electronic transactions and basic rules for electronic contracting and advertising. The second part seeks to establish a framework for ensuring privacy and protection of personal data, including the establishment of national data protection authorities and fair information practice principles that reflect similar concepts in European data protection law. The third and final substantive section of the Convention addresses issues of cybersecurity and protection against cybercrime.

Like the EU Data Protection Directive, the Convention directs African Union member countries to establish national laws to implement the provisions of the Convention. According to its terms, however, the Convention does not become effective until 15 of the 54 African Union member countries have ratified the Convention pursuant to their national constitutions. In the meantime, member countries may submit proposals to amend or modify the Convention.

While the Convention does not yet have the force of law, its adoption at the Summit demonstrates that these issues are on the agenda at the highest levels of African government. Looking ahead to 2015, one can expect continued examination of the Convention by the member countries, and continued debate as to the most effective way to ensure a broad privacy and data protection regime in Africa.

SOUTH AFRICA

30.0000° S, 25.0000° E

Protection of Personal Information Act

Rohan Massey and Robert Lister

On April 11, 2014, the first sections of the Protection of Personal Information Act (POPI) came into effect. These sections relate to the establishment of the Information Regulator and the procedure for making regulations. They also determine the nature of the regulations that the Information Regulator may make with regards to POPI in areas such as complaint submission, investigations, administrative fines and the responsibilities of an organization's information officer. To date, there are no obligations on organizations arising from these sections.

BACKGROUND

The aim of POPI is to provide consumers with their constitutional right to privacy by introducing measures that ensure organizations process personal information in a fair, responsible and secure manner. POPI establishes why and how organizations may collect, use, disclose and store personal information. All companies that process personal information must comply with POPI. The consequences of non-compliance include fines up to R10 million

and potential imprisonment for up to 10 years. Organizations also should recognize the potential reputational risk, which may be the most damaging consequence of non-compliance.

The establishment of the Information Regulator before all POPI provisions are in effect underlines the speed at which this legislation is being implemented. POPI will be fully implemented when the president publishes the enactment date in the *South African Government Gazette*. Once the enactment date is published, organizations in South Africa will have 12 months to ensure that all their practices and processes are in line with the requirements of POPI.

In the past, organizations might have assumed that the establishment of a regulator would cause additional delays and therefore provide organizations with a longer grace period before any legislation fully came into force. The partial enactment of POPI to first establish the Information Regulator shows that this will not be the case. Organizations therefore should take this opportunity to review their internal framework regarding personal information and prepare for the full enactment of POPI.

GUIDANCE

In preparation for POPI's full implementation, organizations should conduct an analysis of their current internal framework regarding privacy. Any analysis is likely to require involvement of the legal, risk and technology departments. Of primary importance is establishing what personal information the organization has and how this personal information is processed.

Personal information should be arranged in two categories: internal information that belongs to the workforce and for which the organization is the responsible party, and personal information that belongs to third parties and for which the organization may or may not be the responsible party. Organizations must be aware of how they process these categories of information under POPI, because different considerations and limitations will apply across and within the two categories. Personal information relating to the workforce will have different considerations and limitations depending on its type—for example, information about salaries will differ from information about internal performance reviews. Equally, customer information relating to the delivery of a product will differ from information used for direct marketing purposes.

Once the initial analysis is complete, organizations can identify the areas in which they might fall short of POPI's requirements. They then can identify next steps and strategies to ensure compliance with POPI once it comes into force.

COMMENT

The appointment of the Information Regulator's chairperson and members will be based on the recommendation of the National Assembly to the President, and it has been suggested that these appointments will take place shortly. There is a possibility that the government will delay the full enactment of POPI to give the Information Regulator time to establish its procedures and views of the regulations, but it would be unwise to rely on this possibility given the potential consequences of non-compliance. Organizations should instead consider this period an opportunity to begin working towards compliance with POPI.

Given the level of personal information that many organizations hold, 12 months is a very short time to ensure all practices and processes are in line with POPI's requirements. Undertaking an analysis of an organization's existing internal framework for privacy is likely to be time consuming and labor intensive. Furthermore, this analysis will only be the first step in seeking compliance; once organizations have completed their assessment, they will still need to address areas in which they fall short of the requirements. Organizations therefore should begin reviewing their internal procedures as soon as possible and establish a timeline for making amendments to ensure that they are compliant with POPI once it is fully enacted.

"In preparation for POPI's full implementation, organizations should conduct an analysis of their current internal framework regarding privacy."

Spring 2014 saw the enactment of several data security measures in China, improving the protection of individuals' personal data in various settings and transaction types. Meanwhile, Malaysia's landmark Personal Data Protection Act has reached the implementation stage, and Australia continues its debate over the necessity of a statutory tort of privacy.

PAKISTAN

33.6667° N, 73.1667° E

Electronic Surveillance and Interception in Pakistan – Is It Constitutional?

Faisal Daudpota | Daudpota International

On November 14, 2014, a local nonprofit organization hosted Pakistan's first national conference on privacy. One of the conference's discussion themes was surveillance laws, particularly the Investigation for Fair Trial Act, 2012 (IFTA), which establishes a compliance regime for the issuance of two kinds of warrants: warrants of surveillance and warrants of interception. These warrants may be issued by a judge of the High Court upon request by select law enforcement agencies to carry out the following actions, among others:

- Intercepting and recording a suspect's telephonic communications with any person
- Video recording any person, persons, premises, event, situation, *etc.*
- Intercepting, recording or obtaining any electronic transaction including but not limited to e-mails and SMS

In light of the potential intrusiveness of the warrant regime, the IFTA attempts to ensure the privacy of Pakistan's citizens through the following safeguards:

- The law enforcement agency requesting the issuance of a warrant of surveillance or a warrant of interception must provide a High Court judge with a signed statement confirming that the warrant shall be not be used to interfere with the privacy of any person.
- The High Court judge, while passing an order for the issuance of a warrant, must ensure that it does not unduly interfere in the privacy of any person or property.
- The High Court judge must recommend departmental action against the authorized officer of the relevant law enforcement agency if the judge believes that the issuance of a warrant has resulted in undue and inappropriate interference in the privacy of any person.

Unfortunately, however, these safeguards appear insufficient to meet the privacy guarantees required by the Constitution and laws of Pakistan.

CONSTITUTIONAL PROTECTIONS OF PRIVACY

In particular, under Article 14 of the Constitution (relating to protection of privacy), the federal and provincial governments have an obligation to protect the privacy of Pakistan's citizens.

In *Riaz v. Station House Officer, Police Station Jhang City & Others* (PLD 1998 Lahore 35), Pakistan's superior courts acknowledged that the issuance of a house search warrant potentially infringes the constitutional guarantee of the fundamental right to privacy in the home. Enjoyment of this right has been made subject to law but at the same time has been described as inviolable. For this right to be truly inviolable, the laws relating to it must be given a strict construction rather than a loose and liberal interpretation, so that the right is preserved rather than eroded. The IFTA's provisions therefore must be read with Article 14 of the Constitution in mind and, accordingly, cannot frustrate the absolute guarantee to privacy as provided by Article 14. The IFTA safeguards, however, merely require that the warrant "not unduly interfere" with personal privacy. This would appear to be a much less stringent standard that what is required by Article 14.

SEPARATION OF JUDICIARY DOCTRINE

Moreover, IFTA may also contravene Article 175 (concerning separation of the judiciary) of the Constitution, because IFTA mandates the performance of administrative functions by judicial persons, *i.e.*, High Court judges. By conferring these duties, a High Court judge becomes a *persona designata* under IFTA.

This identification of specific judicial persons as *persona designata* raises several constitutional difficulties. First, under IFTA the consent of a High Court judge is not in fact being sought; rather, a mandatory administrative duty is being imposed upon the judge as a *persona designata*. Since administrative duties are not pure judicial functions, such duties may be conferred on judges only as *persona designata* rather than as members of courts, and should be subject to the consent of the judge. This is particularly the case with respect to the issue of administrative warrants.

Second, by establishing *persona designata*, IFTA may frustrate the doctrine of separation of the judiciary and executive functions, because, according to Pakistan's superior courts, "any provision in an Act or any rule or a notification empowering any executive functionary to have administrative supervision and control over the subordinate judiciary will violate Article 203 of the Constitution and militate against the concept of separation and independence of judiciary as envisaged by Article 175 of the Constitution and the Objectives Resolution."

COMMENT

The authors and proponents of IFTA appear to have disregarded the constitutional limitations on the criminal justice system, the constitutional safeguards of citizens' privacy and the jurisprudence regarding criminal procedure. Given that privacy issues are increasingly an area of debate in today's information-focused society, it likely will be only a matter of time before the provisions of IFTA are subjected to judicial scrutiny.

INDIA

21.0000° N, 78.0000° E

Privacy and Data Protection Developments

Sajai Singh and Vishnu Nair | J. Sagar Associates

"The draft bill and its proposed provisions promise to provide greater protection of individuals' privacy rights."

The Supreme Court of India has recognized the right to privacy as a fundamental right that is implicit in the right to life and liberty guaranteed by Article 21 of the Constitution. At present, such right may only be enforced against the state, however, and not necessarily vis-à-vis private parties. The Information Technology Privacy Rules of 2011, issued under the Information Act of 2000, regulate the collection and use of personal information and sensitive personal data by corporate entities. Among other things, the Information Technology Rules require entities to have a privacy policy in place, obtain consent from providers of sensitive personal data and follow reasonable security practices.

Various parties consider these existing regulations to be inadequate and have called for a more robust regulatory landscape governing privacy and data protection. In 2014, two legislative developments made progress toward that goal.

DRAFT PRIVACY BILL

Prior attempts to establish comprehensive data privacy legislation have stalled. In 2011, the Department of Personnel and Training under the Ministry of Personnel, Public Grievances and Pensions submitted a draft privacy bill to the Ministry of Law and Justice, but the bill was neither ratified nor taken to the Indian legislature to be passed as a statute.

In 2012, a government-appointed group of experts headed by Justice A.P. Shah submitted a report on privacy regulation reforms in India. In February 2014, a revised draft privacy bill was submitted to the Ministry of Law and Justice. While the draft bill has not been released to the public, it reportedly takes into account the recommendations of the 2012 committee report and includes the following points:

- The rights under the bill would apply to all residents of India, including non-citizens.
- Data controllers—entities that control personal data obtained from a data subject—would be obligated to comply with the bill's provisions.
- The bill proposes the establishment of a Data Protection Authority (DPA) to investigate breaches of the bill's obligations and issue appropriate directions and orders. The DPA would appoint adjudicating officers to investigate complaints from data subjects and impose penalties.
- The bill proposes to introduce privacy principles and provide regulations surrounding the same. These principles include notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security, openness and accountability.

The draft bill and its proposed provisions promise to provide greater protection of individuals' privacy rights. The bill attempts to bring India's data protection regime up to par with some of the stronger data protection jurisdictions in Asia and beyond. Further clarity can be expected on these points once the draft bill is accepted by the government and taken up for legislation.

ADDITIONAL POWERS FOR CERT-IN

On January 16, 2014, the central government issued the Information Technology Cert-In Rules of 2013, which grant the Indian Computer Emergency Response Team (CERT-In) functioning under the Ministry of Communications and Technology additional powers to investigate cybersecurity incidents and breaches, including any real or suspected adverse event in relation to cybersecurity that violates an applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information, or changes to data without authorization. In addition to responding to cybersecurity incidents, the CERT-In is responsible for predicting and preventing such incidents, analyzing and undertaking forensics on incidents, and scanning cyberspace for vulnerabilities.

Any individual, organization or corporation affected by a cybersecurity incident may report the incident to CERT-In. Service providers, intermediaries, data centers and corporations are required to report cybersecurity incidents to CERT-In within a reasonable timeframe. Incidents that must be reported to CERT-In as early as possible include the following:

- Targeted scanning or probing of critical networks or systems
- Actions that compromise critical information
- Unauthorized access to IT systems or data
- Defacement of websites or unauthorized changes to websites, such as the insertion of malicious codes or links to external websites
- Attacks on servers, databases, e-mail and network devices, such as routers
- Identity theft, spoofing and phishing attacks
- Attacks on critical infrastructure and wireless networks

With its new powers, the CERT-In should provide the basis for stronger regulatory and enforcement mechanisms in the future.

CHINA

35.0000° N, 103.0000° E

China's New Consumer Protection Law

Jared T. Nelson and William Zhou

On March 15, 2014, the Decision of the Standing Committee of the National People's Congress on Amendments to the Consumer Rights and Interests Protection Law came into effect, instituting several important revisions to China's consumer rights law.

PROTECTION OF CONSUMERS' PERSONAL INFORMATION

The newly amended Article 14 explicitly stipulates that consumers have the right to request legal protection of personal information when purchasing or using goods, or receiving services. Specific rules for the protection of consumers' personal information are provided under the newly added Article 29 and include three key points:

- Where business operators collect or use consumers' personal information, the operators must abide by the principles of legitimacy, fairness and necessity; expressly inform consumers of the purpose, method and scope of the collection and use; publish the company's policy on collection and use; and abide by all laws and regulations, as well as any mutual agreements between the company and the consumers.
- Business operators must keep information collected from consumers confidential and must not disclose, sell or illegally provide others with that information. Business operators also must take technical and other necessary measures to secure consumers' personal information and to prevent the disclosure or loss of that information. If the personal information becomes or might become divulged or lost, the business operator must take remedial measures immediately.
- Business operators must not send commercial messages to consumers without consent or request, and must immediately cease any messages if a consumer explicitly refuses to receive such commercial messages.

"The Chinese government has begun to address the protection of personal information more comprehensively."

The newly added Article 29 largely echoes the provisions of the Decision on Strengthening Protection of Online Information, which was adopted by the Standing Committee of the National People's Congress on December 28, 2012. There are important differences between the two laws, however. The Decision on Strengthening Protection of Online Information primarily focuses on the protection of citizens' digital personal information, regardless of whether that data is related to consumers or non-consumers, while the provisions of the newly amended Consumer Rights and Interests Protection Law concentrate on the protection of consumers' personal information, regardless of whether such information is digital. These two laws now complement each other to provide broader protection for individuals and more regulation of entities collecting or using personal data.

CIVIL AND ADMINISTRATIVE LIABILITIES

According to the amended Article 50, business operators that infringe on consumers' rights regarding the protection of personal information will be ordered to cease the infringement, restore any damages to the consumers' reputation, eliminate the violation's negative effects, make apologies and compensate the victims for any losses. Additionally, according to the amended Article 56, such business operators may receive a variety of punishments, including a warning, confiscation of unlawful earnings, a fine up to either RMB 500,000 or 10 times the value of the unlawful earnings, and possible business license suspension or revocation.

COMMENT

The Chinese government has begun to address the protection of personal information more comprehensively, and provisions similar to those in the amended Law on the Protection of Consumer Rights should be expected in future laws and regulations. These data protection measures are intended to increase trust and accountability in the broader retail market, and are likely to contribute to an increase in China's consumption in the future.

Measures on the Administration of Online Transactions

Samon Sun and William Zhou

On January 26, 2014, China's State Administration for Industry and Commerce (SAIC) passed the Measures on the Administration of Online Transactions, which became effective on March 15, 2014. The Measures were enacted to regulate online product transactions and related services.

COLLECTION OF INFORMATION

According to Article 18 of the Measures, online retailers and related service operators may collect or use the information of consumers or business operators during business activities, but should comply with the following principles:

- The collection and use must be legal, rightful and necessary.
- The data collector must indicate the purposes, methods and scope of information collection and use.
- The data collector must obtain the consent of parties whose information is to be collected.
- The data collector must disclose its information collection and use rules.
- The data collector's collection and use of information must not violate any laws and regulations, or breach any agreements between the parties.

To further clarify the Measures, the SAIC issued the Guidelines for the Performance of Social Responsibilities by Online Transaction Platform Operators, which came into effect on May 28, 2014.

PROTECTION OF INFORMATION

Under Article 18 of the Measures, online retailers, related service operators and their employees shall keep consumers' personal information, along with trade secrets or other sensitive information from business operators, strictly confidential, and shall not disclose, sell or illegally offer that information to others. Online retailers and related service operators also are required to take technical and other necessary measures to ensure information security and prevent information leakage or loss. Such retailers or operators must take immediate remedial measures if information disclosure or loss occurs or may occur.

Article 36 of the Measures stipulates special obligations for service operators that provide credit-rating services for online product transactions. These entities are required to collect credit information legally; to be neutral, fair and objective; and to refrain from adjusting users' credit ratings or related information arbitrarily, and from using the collected credit information for any illegal purposes.

LIABILITIES

Any party that violates Article 36 of the Measures will receive a warning and be requested to make a correction. If the party refuses to make a correction, it shall be subject to a fine ranging from RMB 10,000 to RMB 30,000.

Provisions on Users' Personal Information Security Management for Postal and Delivery Services

Jared T. Nelson, Samon Sun and William Zhou

On March 26, 2014, the Provisions on Users' Personal Information Security Management of Postal and Delivery Services came into effect. The Provisions focus on improving the security of personal data handling by postal and delivery services. Given the recent explosion of e-commerce-related deliveries in China, the Provisions likely will play an important role in protecting information that was previously at risk of disclosure.

The Provisions define users' personal information as personal information used in the process of postal and delivery services, including the data subject's name, address, national identification number, telephone number and company name, as well as the delivery number, time and package contents.

MANAGEMENT OF USERS' PERSONAL INFORMATION

Per Article 36 of the Provisions, postal and express enterprises must improve the security of their storage and management of users' electronic information by taking the following actions:

- Storing users' personal information in a separate physical area and prohibiting unauthorized personnel from accessing the area
- Using encryption techniques when electronically storing users' personal information
- Ensuring proper use, storage and disposal of devices that contain users' personal information
- Appointing a person responsible for the management of data storage devices, and establishing a registration system to limit the use of output interfaces for those devices
- Deleting users' personal information and destroying any defunct hardware devices

PROTECTION OF USERS' PERSONAL INFORMATION

Postal enterprises, express enterprises and postal administrative departments now have an obligation to keep users' personal information confidential under Article 15 and Article 51 of the Provisions. Without

"Postal enterprises, express enterprises and postal administrative departments now have an obligation to keep users' personal information confidential."

express permission in laws and regulations, or written consent from users, protected personal information cannot be sold or provided to any other entities or individuals.

LIABILITIES

Pursuant to Article 47, postal enterprises and express companies must compensate users for losses caused by unlawful disclosure of personal information. Such unlawful disclosure also may lead to administrative liabilities, or even criminal liabilities in severe situations.

Shanghai's Pilot Free-Trade Zone: Rules for Telecommunications Enterprises

Jared T. Nelson and William Zhou

On April 15, 2014, China's Ministry of Industry and Information Technology published the Administrative Measures of the China (Shanghai) Pilot Free-Trade Zone for Pilot Foreign Investment in the Operations of Value-Added Telecommunications Services. The new Measures were a welcome clarification of the role and impact of the new free-trade zone, which has been largely undefined and lacking in any clear explanation despite promising initial statements concerning deregulation and access for foreign businesses. The value-added telecommunications industry in particular has been a coveted opportunity for foreign companies and investors in China, and while the Measures do not open the industry without significant reservations, new businesses are likely to greet the changes enthusiastically. Along with the new opportunities for foreign businesses, however, come clear signals that Chinese citizens' privacy rights will be protected with special diligence. The Shanghai Communications Administration will conduct annual inspections in accordance with the Measures for all foreign-invested telecommunications enterprises to ensure their compliance with all laws and regulations relevant to the protection of users' personal information.

Notable 2014 Enforcement Activities

Jared T. Nelson and William Zhou

In August 2014, the founders of ChinaWhys Co., a China-based business intelligence company, were found guilty by the Shanghai No. 1 Intermediate People's Court for buying and selling 256 records of Chinese citizens' personal information during the course of due diligence and other investigations. UK citizen Peter Humphrey received a sentence of 30

months in prison, a fine of RMB 200,000 and an order of deportation. U.S. citizen Yu Yingzeng received a two-year prison term and a fine of RMB 15,000. This was the first case in China in which foreigners were sentenced for illegally obtaining citizens' personal information, and it demonstrates the uncertain legal environment for private investigation firms and due diligence consultants in China.

The year 2014 also has been marked by a series of significant cases related to data leaks from technology companies, device manufacturers and internet service companies. One notable example is a January 2014 case dealing with the leak of data related to 20 million hotel guests. The leaked information contained names, gender, nationality, mobile phone numbers and other personal details, exposing some of the victims to harassment, especially by telemarketers.

HONG KONG, CHINA

22.2670° N, 114.1880° E

Data Privacy Guidance for the Banking Industry

Samon Sun and Jenny Chen

On October 6, 2014, Hong Kong's Office of the Privacy Commissioner for Personal Data issued the Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry to assist the banking industry in complying with the Personal Data Privacy Ordinance when dealing with data collection, data storage, use of personal data and customers' data access requests. This guidance is an important roadmap for banks and other banking-related entities, providing a variety of practical recommendations and suggestions based on real cases and experiences within the banking community.

Hong Kong's Privacy Management Program

Jared T. Nelson and Jenny Chen

On February 18, 2014, Hong Kong's Office of the Privacy Commissioner for Personal Data (PCPD) published the Privacy Management Program: A Best Practice Guide. The guide is another encouragement for organizations in Hong Kong to proactively implement data protection and management schemes through effective corporate governance, rather than merely being in compliance with the law. Although the guide does not have a legally binding effect and is intended only as an interim measure before the Data User Return Scheme set out in Part IV of the Personal Data Privacy Ordinance takes effect, it shows the PCPD's determination to enhance corporations' awareness of matters related to personal data protection.

Corporations that wish to implement the Privacy Management Program should consider the following recommendations:

- Establish a governance and management structure compatible with the volume of personal data held.
- Review and update internal data privacy protection policies regularly.
- Provide internal trainings to enhance employees' awareness of the importance of proper data handling procedures.
- Maintain a proper record of all personal data and develop an appropriate database.
- Develop or adopt risk-assessment tools for all relevant projects.
- Review and adjust the Privacy Management Program on a regular basis to ensure its effectiveness and sustainability.

"The guide is another encouragement for organizations in Hong Kong to proactively implement data protection and management schemes."

SOUTH KOREA

37.5500° N, 126.9667° E

South Korea Data Privacy Law Developments

Paul J. Kim and Solyn J. Lee

Since the enactment of the Personal Information Protection Act (as amended) (PIPA) in 2011, South Korea has enforced restrictions on the collection and use of personal information. Despite such efforts, data breach incidents have occurred occasionally. As a result, an amendment to PIPA came into force on

August 7, 2014, to prevent companies from collecting and processing resident registration numbers (RRNs), the key item of information necessary to verify a person's details.

Under Article 24 of PIPA, personal information processors are prevented from collecting and using RRNs based solely on the consent of a data subject. Prior to the amendment, this prohibition was applicable only to website operators. The current version of PIPA, however, requires all sectors handling personal information in South Korea to comply with this regulation. Violations could result in fines up to KRW 30 million (approximately U.S.$30,000) except under certain limited circumstances.

PIPA also imposes stricter penalties on companies that fail to protect personal information. Fines can reach up to KRW 500 million (approximately U.S.$500,000) unless the company in question proves that all measures necessary for securing the safety of personal information, as defined in Article 29 of PIPA, were properly taken. Companies operating in South Korea therefore should take all necessary steps to comply with PIPA's new amendment.

JAPAN

35.6833° N, 139.7667° E

Proposed Amendments to the Personal Information Protection Act

Jared T. Nelson and William Zhou

"While not mandatory, the code offers useful guidelines for companies operating in Japan."

Japan enacted its Personal Information Protection Act (PIPA) in 2005. Since then, some public critics of PIPA have asserted that limitations and ambiguities fail to reconcile and properly balance individuals' privacy rights with the potential for big data and other data-related industries. In response, in 2014 the Japanese government released a basic outline of possible amendments to PIPA for public comments, with the intention of revising the law in 2015. Potential amendments would alter the law and include the establishment of an independent third-party organization that would be responsible for enforcing the laws and creating additional self-regulation compliance rules.

One of the most significant potential amendments put forth for comments is to allow organizations to transfer personal data to third parties without the consent of the data subject if the data is anonymized or otherwise processed so that there is a reduced risk that such data may be used to identify the data subject. The amendments also propose a clarified definition of personal data and sensitive data that would include any information that might cause social discrimination, such as race, social status, belief system or criminal history.

BEST PRACTICES ADVISORY

In April 2014, Japan's Ministry of Economy, Trade and Industry issued a code of practice for notifying customers about the collection and use of data. While not mandatory, the code offers useful guidelines for companies operating in Japan and creates recommended standards and best practices for businesses.

JOINING THE APEC CROSS BORDER PRIVACY RULES SYSTEM

In May 2014, the Asia-Pacific Economic Cooperation (APEC) announced that Japan was approved as a participant in the Cross Border Privacy Rules System. This significant step shows Japan's commitment to improving its information privacy and protection system, as well as its concern for global solutions.

MALAYSIA

3.1333° N, 101.7000° E

Implementing the New Personal Data Protection Act

Jared T. Nelson

Malaysia's Personal Data Protection Act (PDPA) was promulgated in 2010 but only came into effect at the end of 2013. In 2014, the first full year of the PDPA, the government has issued a series of new codes of conduct and other statements to assist businesses with compliance and raise public awareness of the new rules.

The codes of conduct, issued by the Personal Data Protection Commission, address topics such as the form of consent necessary for collection of data and

the type of consent required for direct marketing. These codes and other policy statements by the commission supplement and enhance the PDPA, sending a clear message that the legislative and enforcement authorities are seeking to create a robust, transparent and compliant system.

Implementation of the PDPA is ongoing. Currently the implementation plan is in its second phase, which began in April 2014. This phase emphasizes compliance and evaluations to assess the readiness of affected entities in developing best practices and protocols.

February 2014 marked the end of the PDPA transitional period, which allowed organizations to conduct an initial review of policies, procedures and practices. The end of the transitional period and the beginning of the implementation phase are significant steps towards the full realization of the landmark PDPA in Malaysia.

SINGAPORE

1.3000° N, 103.8000° E

Singapore's Personal Data Protection Act Now in Force

Samon Sun, Jared T. Nelson and Jenny Chen

Singapore's Personal Data Protection Act (PDPA) was promulgated in 2012 but only came into force on July 2, 2014. The PDPA protects individuals' privacy rights while recognizing organizations' need to collect, use and disclose personal data for legitimate and reasonable purposes. It creates a minimum standard of protection for personal data and supplements a patchwork of sector-specific legislation to create a more robust data privacy environment. Non-compliance with the PDPA may result in sanctions, including criminal liabilities and financial penalties up to S$1 million.

In order to assist companies in meeting the requirements of the PDPA, the Personal Data Protection Commission issued the Personal Protection Regulations of 2014. These regulations provide additional clarity on some of the main PDPA provisions, including an individual's right to access and correct data held by a company, and restrictions on the transfer of personal data outside of Singapore.

Do Not Call Provisions

Jared T. Nelson and Jenny Chen

On January 2, 2014, the Do Not Call Provisions of Singapore's Personal Data Protection Act came into effect and established Singapore's Do Not Call Registry. The provisions prohibit organizations from sending marketing messages via voice call, text or fax to any Singapore telephone number in the Do Not Call Registry. E-mails and other electronic messages that do not use telephone numbers as identifiers do not fall under the scope of the Registry. Breach of the Do Not Call Provisions may result in fines up to S$10,000 per offense.

"Breach of the Do Not Call Provisions may result in fines up to S$10,000 per offense."

Advisory Guidelines for Implementation of the Personal Data Protection Act

Jared T. Nelson and Jenny Chen

Since 2013, the Personal Data Protection Commission has been issuing advisory guidelines for the implementation of the Personal Data Protection Act (PDPA). Although these guidelines are not legally binding, they indicate trends in the interpretation of the PDPA's provisions.

On May 16, 2014, the Commission published advisory PDPA implementation guidelines for the telecommunications and real estate sectors. The telecommunications sector guidelines were developed in consultation with the Information-Communications Development Authority of Singapore to address the unique circumstances the telecommunication sector faces in complying with the PDPA, such as the need to obtain consent from pre-paid mobile subscribers. The real estate sector guidelines were developed in consultation with the Council for Estate Agencies to address issues that real estate agencies must address in complying with the PDPA, such as the disclosure of a client's personal data in a co-broking situation.

NEW ZEALAND

42.0000° S, 174.0000° E

Harmful Digital Communications Bill

Richard Wells and Libby Conole | Minter Ellison Lawyers

In New Zealand, harmful digital communications, like harmful communications in general, are governed by a range of existing laws addressing behaviors such as harassment, criminal incitement of suicide, defamation and invasion of privacy. Several disturbing cases have demonstrated that the existing laws covering harmful digital communications do not meet the current thresholds for criminality, in particular around cyber-bullying and harassment.

"The HDCB as drafted would make wide-ranging alterations to existing legislation in order to better apply current harassment and anti-bullying laws to electronic environments."

The Harmful Digital Communications Bill (HDCB) seeks to address this concern by creating new criminal offenses for the most serious harmful digital communications and providing a new civil enforcement regime to deal with minor harmful behavior. The HDCB was introduced to Parliament in November 2013 following a ministerial briefing by the Law Commission and is currently awaiting its second reading. The HDCB as drafted would make wide-ranging alterations to existing legislation in order to better apply current harassment and anti-bullying laws to electronic environments. The Privacy Act 1993 (and the Information Privacy Principles contained therein) also is slated to undergo amendment in pursuit of this objective.

DEFINITION OF DIGITAL COMMUNICATIONS

The HDCB defines "digital communications" as any form of electronic communication, including text messages, writing, photographs, pictures, recordings and other content that is communicated electronically. Digital communications therefore would encompass communication via e-mails, blogs and social media platforms.

In order to be caught by the HDCB, the digital communication must be harmful. The HDCB defines "harm" as serious emotional distress.

USE OF PUBLICLY AVAILABLE INFORMATION

According to the Privacy Act Information Privacy Principles 10 and 11, an agency that holds personal information shall not use the information for any purpose other than that for which it was collected, and shall not disclose it to a person, body or agency unless one of the given exceptions applies. One of these exceptions is where the source of the information is publicly available. As a result, personal information may be used for purposes other than that for which it was collected or may be disclosed to another party if that information is already publicly available. This exception allows information of a sensitive nature that is not secret to be posted or communicated online, which may be profoundly upsetting to the data subject. The exception also allows for the perpetual redistribution of information without breach of the Privacy Act. In fact, the more the information is disseminated, the stronger the argument becomes that the information is "publicly available" and that the disclosure is accordingly not in breach.

The HDCB proposes to limit this exception by allowing use or disclosure of publicly available personal information only in circumstances where it would not be unfair or unreasonable to so use or disclose. This change would in effect create a new category of Privacy Act breach, whereby redistribution of personal information in unreasonable or unfair circumstances would be an offense regardless of whether the information is publicly available. Because the proposed amendment is not limited to information used or disclosed online, this change could have effects beyond the HDCB's target of digital communications.

USE OF PERSONAL INFORMATION RELATING TO DOMESTIC AFFAIRS

Currently, nothing in the Privacy Act's Information Privacy Principles applies to information collected by an individual principally in connection with that individual's personal, family or household affairs. The purpose of this exception is to provide a "safe zone" whereby individuals may conduct themselves socially in connection with matters of which they have personal knowledge, without fear of breaching the Privacy Act.

In an online environment, however, this exception allows sensitive personal information collected in the context of a personal relationship to be widely disseminated over the internet without liability arising under the Privacy Act. The Law Commission highlighted the particular concern of intimate photos posted online following relationship breakdowns; such information originally was collected in a

personal context but later was used to destructive and emotionally harmful ends.

The HDCB as drafted removes this exception where personal information is collected, disclosed or used in circumstances that would be highly offensive to an ordinary reasonable person. This places an outer boundary on the exception while preserving the integrity of its core purpose.

UNINTENDED CONSEQUENCES OF THE HDCB

Commentators have noted that the HDCB may have the unintended consequence of bolstering a "right to be forgotten," similar to recent European case law. The right to be forgotten, which is conceptually close to other privacy rights, is not well recognized or established in New Zealand, but some argue that existing laws provide for this right in particular circumstances. For example, the right to be forgotten already exists in the sense that New Zealand uses discharges without conviction, non-publication or suppression orders, and allows for minor criminal offenses to be "wiped clean" after seven years under the Criminal Records (Clean Slate) Act 2004.

The HDCB would support the right to be forgotten in online contexts by providing a mechanism for content to be removed or disabled, and for an individual to be "forgotten" if the complainant can prove that the availability of links and search engine results causes serious emotional distress.

AUSTRALIA

35.3080° S, 149.1245° E

ALRC Report on Serious Invasions of Privacy in the Digital Era

Tarryn Ryan and Veronica Scott | Minter Ellison Lawyers

In September 2014, the Australian Law Reform Commission (ALRC) released its Report on Serious Invasions of Privacy in the Digital Era. Following several earlier ALRC reports and privacy-related inquiries, the ALRC had been tasked to design a statutory tort of privacy addressing the challenges posed by modern technology, and to propose other innovative ways to respond to privacy challenges.

DESIGNING A STATUTORY TORT

The ALRC ultimately recommended a cause of action with the following essential elements:

- The invasion of privacy must be either by "intrusion into seclusion" (*i.e.*, physically intruding into a person's private space or recording private activities or private affairs) or by "misuse of private information" (such as collecting or disclosing private information about an individual).
- The plaintiff must have a reasonable expectation of privacy in all the relevant circumstances.

- The invasion must have been committed intentionally or recklessly (negligence is not sufficient).
- The invasion must be serious.
- The invasion need not cause actual damage, and damages for emotional distress may be awarded.

Additionally, the court must be satisfied that the public interest in privacy outweighs any countervailing public interests. A non-exhaustive list is provided, including interests such as freedom of expression, freedom of the media, public health and safety, and national security. The court must consider the public interest as an element of the tort when determining if the plaintiff has a cause of action, rather than as an available defense. There has been much discussion about this issue, with the ALRC favoring a threshold question that would prevent a claim from proceeding where strong public interest grounds justify the invasion of privacy.

A number of defenses also were recommended, including lawful authority, consent, necessity, absolute privilege, publication of public documents and fair reporting of public proceedings, along with situations where the conduct was incidental to defense of persons or property.

The remedies that would be available to a successful plaintiff are wide ranging and include damages, accounts of profits, injunctions, delivery up or destruction and removal of material, correction and apology orders, and declarations.

OTHER WAYS TO PROTECT PRIVACY

As an alternative to the new tort, the ALRC explored and recommended reforms to existing laws aimed at preventing or redressing serious invasions of privacy. One of these recommendations was to enact legislation to enable courts to award compensation for emotional distress in actions for breach of confidence. Currently such compensation is not generally available unless the emotional distress reaches the level of a recognized psychiatric illness.

This recommendation, however, assumes that the Australian common law will move in the same direction as UK law and extend the equitable action for breach of confidence to protect personal privacy. While the Australian High Court opened the door to such a development in the 2001 case *Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd*, there has been limited development since then. Two lower court decisions have embraced the idea of a common law tort for invasion of privacy, but both cases

settled before appeals instituted by the respective defendants had been heard. Consequently, whether such a cause of action exists in Australian common law has yet to be determined by an appellate court.

Another recommendation was to unify and strengthen the existing regulation of surveillance device use. Current state- and territory-based surveillance laws, where they exist, often are inconsistent and incompatible with emerging technologies. Harmonization would not only make the laws more effective but would cut red tape, particularly in the area of workplace surveillance, where national businesses currently are required to grapple with requirements that vary from state to state.

Other recommendations included a "responsible journalism" defense, as well as a statutory tort of harassment, similar to current laws in jurisdictions such as the United Kingdom and New Zealand, to combat some of the most serious invasions of privacy, in the event the statutory tort of privacy does not proceed. Finally, the ALRC recommended that the Australian privacy commissioner be given additional powers in the Privacy Act 1988 to investigate complaints about serious invasions of privacy more generally. It also was suggested that the privacy commissioner be given the ability to act as *amicus curiae* or intervener in relevant court proceedings. For these suggestions, the practicalities of funding would need to be addressed.

WILL AUSTRALIA FINALLY GET A STATUTORY TORT OF PRIVACY?

There has been a long debate in Australia over whether a statutory tort of privacy is necessary, and that debate looks set to continue. The ALRC released its first report on the subject in 1979; this year's report is the third to address this issue. The ALRC's task was not to decide whether there should be a tort but to design it. When the inquiry started in 2013, it appeared that the then-current federal Labor government would support the introduction of a statutory tort. Since then, there has been a change in government, and it seems unlikely that the ALRC's design for a statutory tort will become part of the Australian regulatory landscape in the foreseeable future. The commonwealth attorney general has made it clear that the current Liberal government does not support the introduction of a tort of privacy.

The government's attitude to privacy reform has been further illustrated by its opposition to mandatory data-breach notification legislation, and the attorney general's recommendation of a "light-touch" approach to enforcement of recent reforms in Australian data protection legislation. The proposed introduction of new data retention laws and counter-terrorism laws also suggests that the privacy pendulum is swinging in the opposite direction for now.

"There has been a long debate in Australia over whether a statutory tort of privacy is necessary, and that debate looks set to continue."

Latin America's country-specific data privacy laws continued to evolve in 2014. For example, Brazil heightened its commitment to penalizing data privacy violations, and Chile issued a draft law to overhaul its existing privacy regime.

LATIN AMERICA

Data Privacy in Latin America

Effie D. Silva

Multinational companies continue to flood the Latin American marketplace seeking to take advantage of globally competitive sectors, such as manufacturing and industrial development. This influx of new business has increased concerns about the security and privacy of personal data flowing between countries, and has led to the enactment of numerous data privacy laws in the United States and Europe over the last few years. However, unlike the European Union and the United States, Latin America has no uniform directives governing the regulation, enforcement and procedure of data privacy laws. This lack of uniformity has created staggering differences between each country's data privacy laws. As a result, it is imperative that companies conducting business in Latin America stay apprised of country-specific data privacy laws, which frequently change and evolve.

COSTA RICA

9.9333° N, 84.0833° W

Increased Enforcement of Data Protection Law Expected

Effie D. Silva

Costa Rica's data protection law, Ley Protección De La Persona Frente Al Tratamiento De Sus Datos Personales, Law 8968, which came into effect on March 5, 2013, is modeled after the EU Data Protection Directive in that it requires each member state to pass a privacy law, called a data protection law, that reaches both government and private entities, including businesses that process employee and consumer data. While the United States' sectoral privacy laws target discrete categories of data (such as medical and credit records, and children online), the EU Directive mandates omnibus laws that cover all processing, defined to include even collection and storage of data about personally identifiable individuals. Costa Rica's data protection law, like the EU Directive, is not limited to electronic (computerized) data and therefore reaches written, internet and even oral communications. Its breadth also goes well beyond business data. The data protection law requires explicit data subject consent for any processing of data, and implements notice and consent requirements; limits on data transfers; and appropriate security measures that protect against unauthorized use, access, disclosure and destruction of personal data. Pursuant to the regulations implementing the law, companies must notify data subjects within five days of any "irregularity in the processing or storage of their data," such as a data breach or theft. Companies also must notify the Data Protection Agency of the People (Agencia De Protección De Datos De Los Habitants) of any data breach.

The data protection law has seemingly limitless jurisdictional reach, and businesses based outside of Costa Rica should be aware of the origins of the data that they process. To prevent Costa Rican businesses from circumventing the data protection law by transmitting regulated data outside of Costa Rica for processing offshore, the data protection law specifically prohibits the transmission of personal data to any country without a level of data protection considered adequate by EU standards. Concerns have been expressed over the scope of the law to deal with cloud computing, the management of remote databases (including international transfers of personal data) and the processing of personal information on the internet. It is expected that the Costa Rican Data Protection Authority will move rapidly towards enforcing its new law in late 2014 and into early 2015, and therefore it is imperative for multinationals in Costa Rica to quickly get up to speed and comply with the data protection law's strict EU-like requirements.

"The data protection law has seemingly limitless jurisdictional reach."

COLOMBIA

34.0008° N, 81.0353° W

Update on the Data Protection Act

Effie D. Silva

On April 18, 2013, Colombia's Data Protection Act (Ley 1581 del 17 de Octubre de 2012 por el cual se Dictan Disposiciones Generales para la Protección de

Datos Personales) took effect. Two months later, in June 2013, the Colombian government implemented regulations for the law in a decree. Colombia was the sixth country in Latin America to enact a data privacy law, behind only Argentina, Costa Rica, Mexico, Peru and Uruguay. The regulations set forth applicable consent requirements, limits on cross-border transfers, and the information that must be given to data subjects. The regulations also require registration of all automatic or manual private- or public-sector personal data databases in the National Registration Database. One of the most important aspects regulated by the decree is the international transfer and transmission of data, since most companies have their head office or subsidiaries outside of Colombia, and some have hired data processors outside the country in jurisdictions where technical capacity is not an issue. The law requires that, in order to transfer or perform international transmission of personal data, the data controller must either obtain an express authorization from the subject to do so, or require the data controller and the processor to subscribe to a data transmission agreement in which the purposes of the processes are clearly established.

For non-compliance, the implementing regulations impose fines of more than $600,000, suspension of activities for a period of up to six months, and the temporary or permanent closure of operations. As a result, companies are starting to implement compliance measures in order to avoid sanctions that will inevitably be handed out by the enforcement authorities in 2015.

"As in the European Union, individuals may revoke consent at any time, without justification and with no retroactive or punitive effects."

PERU

12.0433° S, 77.0283° W

Breach of Law for Personal Data Protection Can Result in Penalties, Fines

Effie D. Silva

On March 22, 2013, approximately two years after it was enacted, Peru's Law for Personal Data Protection took effect. While the law does not require notification to any central authority or data subject in the event of a breach, it generally requires data subject consent to process data. As in the European Union, individuals may revoke consent at any time, without justification and with no retroactive or punitive effects. In 2014, the Data Protection Authority clarified that Article 14 of the law (conditions under which data subject consent is not required for personal data processing) applies to both personal data and sensitive personal data, without making a distinction between the two types of data. The law also provides that the purposes of processing data must be clearly and objectively conveyed to individuals by the data controller. Further, the law provides individuals with various rights to access, update or eliminate personal data held by a company. Cross-border transfers of personal data are permitted only if the entity receiving the data assumes the transferor's obligations in a written agreement, similar to the requirements under the European model. Any cross-border data transfers must be reported to the Peruvian Data Protection Authority.

As in other Latin American countries, businesses that breach these regulations will be subject to criminal penalties or monetary fines that can range from $7,150 to $142,000. In late 2014, the Data Protection Authority issued a $20,000 fine against a Peruvian website housed offshore for violating the law by not providing an individual with his access and recertification rights. Although Peruvian authorities have not reported any larger fines issued to date, fines against non-compliant multinationals are anticipated in 2015.

BRAZIL

15.7833° S, 47.8667° W

Increased Focus on the Marco Civil da Internet

Effie D. Silva

The Civil Internet Bill (Marco Civil da Internet) has become a priority for the Brazilian government in late 2014. The Marco Civil is aimed at defining core internet rights, which include data protection, freedom of access and expression, and privacy. Recent amendments to the Marco Civil could have serious implications for companies doing business in Brazil, by requiring them to use local data storage centers to store data collected from Brazilian users. Companies

could not transfer personal information of Brazilians outside of Brazil for storage or processing. Google recently spoke out against the proposed changes to the Marco Civil, stating: "[t]he proposed amendment requiring internet companies to store Brazilian user data in Brazil risks denying Brazilian users access to great services that are provided by U.S. and other international companies." In the remainder of 2014, the Brazilian government also may focus on the Data Protection Bill of 2011 in addition to the Marco Civil. This draft legislation would establish a data protection authority, require data subject consent prior to transfers of data and require data breach notification. The proposed law would replace Brazil's current sector-specific privacy framework.

Brazil is the fifth largest country in the world, and the number of Brazilian internet and smartphone users continues to grow rapidly. The new laws therefore will have a significant impact on organizations offering digital products or services to Brazilian consumers. The proposed privacy requirements would broadly restrict companies from sharing users' personal information, communications and certain online logging data. The Marco Civil also incorporates an approach to liability for internet companies hosting third-party user-generated content that is analogous to section 230 of the U.S. Communications Decency Act. Specifically, under the Brazilian Internet Law, an internet company will not be liable for user-generated content posted on its service unless it ignores a judicial order to remove content. Notably, the Brazilian Internet Law does not include the original proposal of a mandatory Brazilian cloud for storage of Brazilian users' data. However, the Marco Civil does embrace a broad concept of Brazilian government jurisdiction over online companies that collect or use Brazilian users' data, even for companies located outside of Brazil.

In July 2014, the Brazilian Consumer Protection and Defence Department sent a message to all corporations dealing with internet users by issuing a $1.59 million fine against Oi, the country's largest telecommunications company, for failing to notify internet users that their browsing activities had been tracked and sold to third-party advertisers. Although the fine was based on the telecom giant's violation of Brazil's Consumer Law, it demonstrates Brazil's new commitment to cracking down on data privacy violations.

ARGENTINA

34.6000° S, 58.3833° W

Legislative and Enforcement Developments

Effie D. Silva

On August 14, 2014, Argentina's Law Number 26.951, which created the National Do Not Call Registry (NDNCR), became effective. The law allows users to register landline and mobile telephone numbers, and the law's prohibitions become effective immediately at the time of registration. In particular, once a number is registered, the law prohibits unsolicited calls for advertising, marketing or selling, and persons wishing to call numbers for those purposes must consult the NDNCR every 30 days. The law exempts calls made to numbers with an existing business relationship (as long as the calls are made at a "reasonable time"), calls based on express consent and emergency calls, among a few other narrow exemptions. Like Argentina's Personal Data Protection Act, the law will be enforced by the National Directorate for the Protection of Personal Data (DPA) and the Ministry of Justice and Human Rights. Violators are subject to penalties pursuant to the Personal Data Protection Act.

"Argentina has become the main recipient of personal data transferred from Spain to other Latin American countries."

The Personal Data Protection Act, which is based on the EU Data Protection Directive, provides general principles of data protection, rights of data holders, sanctions for violations and rules governing personal data protection actions. Argentina's proactive approach to safeguard personal data through legislation has led to the country's classification by the European Commission as a country with an "adequate" level of protection. As a result of earning this classification, Argentina has become the main recipient of personal data transferred from Spain to other Latin American countries. Section 33 of the Personal Data Protection Act includes a private right referred to as a data protection right. This right allows a court to consider private action by any individual seeking enforcement of the right to access, rectify, update or suppress personal information. Argentina's laws, however, provide no special provisions or rules on the right to privacy when it comes to the internet. Argentinian courts regard privacy on the internet as similar to privacy in other media, such as TV and print. Under these laws, the internet and internet-related services are considered as files, databases or other technical media for data processing.

In 2014, data privacy enforcement has been relatively infrequent. In the past there have been cases in which criminal complaints have been filed—for example, against ChoicePoint for selling information about Argentinean citizens to the U.S. government—and some multinationals have received sanctions for not renewing a database at the proper time. By contrast, the few opinions issued by the DPA in 2014 have involved the legitimacy of data transfers by businesses to other countries. For example, in March 2014, the DPA issued Opinion No. 16/13, in which it concluded that in order for employee data to be transferred to a third-party processor in a country without adequate data protection, the transferee must include appropriate contractual provisions to ensure that the Personal Data Protection Act is followed. These provisions include the following:

- The transferor must obtain a guarantee from the third party that its local laws will not circumvent the provisions of the Personal Data Protection Act.
- The third party must agree to comply with any requirements imposed by the DPA.
- Data owners must be provided with the rights of access, rectification, deletion and confidentiality.
- Data must be destroyed at the end of processing.
- Any disputes must be resolved in Argentinean courts.

The DPA issued similar opinions regarding financial data, insurance data and responses to government requests.

CHILE

33.4333° S, 70.6667° W

Proposed Amendment Would Overhaul Personal Data Law

Amy C. Pimentel and Heather Egan Sussman

Chile's Personal Data Law (Protección de la Vida Privada y Protección de Datos de Carácter Personal), adopted in 1999, protects an individual's personal data, including data found in commercial, financial and banking records. The law makes it a crime to destroy, disable, intercept or

interfere with databases, and to illegally access, destroy or change information contained in such databases. Additionally, the law forbids the malicious disclosure or publication of data contained in information systems.

In October 2014, the Chilean government released a new draft law that would amend the existing law, aiming to bring privacy protection in Chile up to international standards. The law, if passed, would create a public entity to oversee privacy in Chile (with powers to impose penalties, resolve claims for breaches of the law and create a registry of national databases), recognize the principle of legitimacy (including proportionality, quality, transparency, accountability and security), require special treatment for sensitive data and the international transfer of personal data, and establish penalties for violations of the law. The Chilean government is also considering bill No. 9.388-03, which would introduce the "right to be forgotten" into Chilean data privacy law.

HONDURAS

14.1000° N, 87.2167° W

Draft Law on the Protection of Personal Data and Action of *Habeas* Data

Amy C. Pimentel and Heather Egan Sussman

Currently, Honduras recognizes *habeas* data as a constitutional right, authorizing individuals to file complaints with the Constitutional Court against any entity possessing a database to determine what information is held about an individual and to request correction, disclosure or destruction of that personal data. In early 2014, a draft Law on the Protection of Personal Data and Action of *Habeas* Data was introduced in the National Congress of Honduras. This draft was based on the EU Data Protection Directive and the data protection laws of other Latin American countries. If it passes, the law would apply to personal data transfers and records in automated and manual databases in the public and private sector, with some exceptions. Much like the EU Directive, the draft outlines the requirements for notice to data subjects, restricts the types of use and processing of personal data, and creates a monitoring and enforcement mechanism. The law invests authority in the Institute of Access to Public Information, which may impose sanctions for misconduct. If this law passes, Honduras will see a major increase in its data privacy protection.

DOMINICAN REPUBLIC

19.0000° N, 70.6667° W

Further Clarification of New Personal Data Protection Law Likely in 2015

Amy C. Pimentel and Heather Egan Sussman

In late 2013, the National Congress of the Dominican Republic enacted the Personal Data Protection Law (Ley No. 172-13), which provides a framework for the handling of personal and specially protected data, credit information and credit reports. Although the law incorporates many aspects of the EU Data Privacy Directive, it is not nearly as comprehensive. The law requires that the collection and processing of personal data be purposeful, relevant and not excessive to its specific and legitimate stated purpose. It creates a personal right of action for data subjects to enforce their right to access, rectify, update and delete their personal data. Processors of personal data must ensure confidentiality, accuracy and a data subject's right of access to the data, and must implement security measures to safeguard collected information. The law further requires processors to obtain consent prior to treating and transferring personal data within and outside the Dominican Republic. However, there is no obligation under Dominican law to give notice in the event of a data security breach.

"Processors of personal data must ensure confidentiality, accuracy and a data subject's right of access to the data."

The law does not create a data protection authority, but the Superintendency of Banks is authorized to regulate credit information agencies. The law allows for criminal penalties, which may range from six months to two years imprisonment and monetary fines. In 2015, the law is likely to face continuing criticism concerning its narrow application and rigorous regulation of credit information and other data coming from economic or commercial relationships. It is also likely that the government will interpret and clarify the law as it implements the law's provisions in the coming year.

FOR MORE INFORMATION

CO-CHAIRS, PRIVACY AND DATA PROTECTION GROUP

Heather Egan Sussman
+1 617 535 4177
hsussman@mwe.com

Daniel F. Gottlieb
+1 312 984 6471
dgottlieb@mwe.com

Rohan Massey
+44 20 7577 6929
rmassey@mwe.com

McDERMOTT WILL & EMERY

Maximilian Baur
+49 89 12712 332
mbaur@mwe.com

Anthony A. Bongiorno
+1 617 535 4044
abongiorno@mwe.com

Sarah Bro
+1 949 757 6001
sbro@mwe.com

A. Marisa Chun
+1 650 815 7668
mchun@mwe.com

Devin Cohen
+1 617 535 3867
decohen@mwe.com

Nicolò Di Castelnuovo
+39 02 7862 7305
ndicastelnuovo@mwe.com

Jennifer S. Geetter
+1 202 756 8205
jgeetter@mwe.com

Kate Hammond
+1 310 284 6114
khammond@mwe.com

Julia Jacobson
+1 617 535 3881
jjacobson@mwe.com

Marcos Daniel Jiménez
+1 305 329 4458
mjimenez@mwe.com

Manoj Khandekar
+1 312 984 2092
mkhandekar@mwe.com

Ann Killilea
+1 617 535 3933
akillilea@mwe.com

Paul J. Kim
+82 2 6030 3602
pkim@mwe.com

Robert M. Kline
+1 305 347 6537
rkline@mwe.com

Matthew L. Knowles
+1 617 535 3885
mknowles@mwe.com

Myrtille Lapuelle
+33 1 81 69 14 84
mlapuelle@mwe.com

Solyn J. Lee
+82 2 6030 3607
sjlee@mwe.com

Robert Lister
+44 020 7577 3481
rlister@mwe.com

Jilali Maazouz
+33 1 81 69 15 04
jmaazouz@mwe.com

Dr. Paul Melot de Beauregard
+49 89 12712 330
pbeauregard@mwe.com

Bridget K. O'Connell
+1 617 535 4091
boconnell@mwe.com

Amy C. Pimentel
+1 617 535 3948
apimentel@mwe.com

Veronica Pinotti
+39 02 7862 7302
vpinotti@mwe.com

Audrey Pumariega
+1 305 329 4421
apumariega@mwe.com

David Quinn Gacioch
+1 617 535 4478
dgacioch@mwe.com

David A. Roller
+1 305 329 4482
droller@mwe.com

Martino Sforza
+39 02 78627300
msforza@mwe.com

Effie D. Silva
+1 305 329 4452
esilva@mwe.com

Sharon Tan
+44 20 7577 3488
stan@mwe.com

Matthew R. Turnell
+1 617 535 4019
mturnell@mwe.com

Scott Weinstein
+1 202 756 8671
sweinstein@mwe.com

Han (Jason) Yu
+1 310 788 1539
hyu@mwe.com

Edward G. Zacharias
+1 617 535 4018
ezacharias@mwe.com

MWE CHINA LAW OFFICES

Jenny Chen
+86 21 6105 0916
jnchen@mwechinalaw.com

Samon Sun
+86 21 6105 0558
ssun@mwechinalaw.com

William Zhou
+86 021 6105 0540
wzhou@mwechinalaw.com

Jared T. Nelson
+86 21 6105 0513
jtnelson@mwechinalaw.com

DAUDPOTA INTERNATIONAL

Faisal Daudpota
+971 55 951 9972
faisal@daudpota.com

J. SAGAR ASSOCIATES

Vishnu Nair
+91 80 435 03611
vishnu.nair@jsalaw.com

Sajai Singh
+91 98 450 78666
sajai@jsalaw.com

MINTER ELLISON LAWYERS

Libby Conole
+64 9 353 9783
libby.conole@minterellison.co.nz

Veronica Scott
+61 3 8608 2126
veronica.scott@minterellison.com

Richard Wells
+64 9 353 9908
richard.wells@minterellison.co.nz

Tarryn Ryan
+61 3 8608 2000
tarryn.ryan@minterellison.com

McDERMOTT'S PRIVACY AND DATA PROTECTION GROUP

McDermott Will & Emery's Privacy and Data Protection Group comprises more than 50 lawyers who are dedicated to helping companies manage information and related risks throughout the data lifecycle. We represent large and small companies from nearly every industry and sector. We have experience across the full range of privacy and data protection laws. This deep industry experience and our global, multi-disciplinary approach to data management uniquely position us to provide practical, efficient solutions to our clients.

For more information about McDermott Will & Emery visit www.mwe.com.

www.ofdigitalinterest.com

Insightful. Global. Connected.

Privacy, data security, digital advertising and online consumer protection are some of the fastest growing areas of the law around the world. In the digital realm, jurisdictional lines can be crossed in nanoseconds, and this compounds compliance challenges. Follow ofdigitalinterest.com, a blog dedicated to sharing insights into regulatory developments, industry trends and current issues affecting the digital environment.

McDermott
Will & Emery

@McDermottLaw | McDermott Will & Emery | www.mwe.com

McDermott
Will & Emery

www.mwe.com