Skadden

PRIVACY & CYBERSECURITY UPDATE

JANUARY 2014

CONTENTS

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 14, or your regular Skadden contact.

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

Four Times Square
New York, NY 10036
212.735.3000

We thought it appropriate to release the January edition of our *Privacy & Cybersecurity Update* on January 28, 2014 — the sixth international **Data Privacy Day**. January 28 commemorates the January 28, 1981, signing of Convention 108 — the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Enacted by the Council of Europe, Convention 108 was the first legally binding international treaty dealing with privacy and data protection. Today, Data Privacy Day is used by many organizations to remind employees of their data privacy and security obligations.

The data privacy and security industry got off to a roaring start in 2014 with important developments on multiple fronts, including data breaches at Target and other retailers, FTC activity on Safe Harbor certifications, executive branch activity on "big data" and data breach class actions. We review these important developments, and others, below.

RAMIFICATIONS OF THE TARGET DATA BREACH

The cybersecurity attack on Target is undoubtedly one of the highest profile data breaches in history. The number of people impacted (possibly 70 million); the type of data taken (in many cases, encrypted PIN data, customer names, credit and debit card numbers, card expiration dates and the embedded code on the magnetic strip on the back of cards); and the time period of the attack (the critical pre-Christmas shopping season) catapulted the Target data breach onto the front page. The full extent of the breach is not yet known. In addition to similar attacks at Neiman Marcus and Michaels Stores, recent reports indicate that other retailers may have been compromised as well.

Not surprisingly, these data breaches, particularly Target's, have reopened or accelerated debates on a number of legislative, regulatory and legal issues. We discuss below some of these ramifications and how the Target breach may have been a watershed moment in the area of privacy and data security.

CYBERSECURITY REGULATION. As soon as news of the Target data breach broke, a number of legislators and privacy and security pundits asserted that these types of breaches prove that cybersecurity regulation is required. However, it remains unclear what sort of legislation could have been in place to stop the attack. As companies have learned, hackers routinely find ways to exploit what most would consider "industry standard" security. The Target breach is therefore unlikely to result in the enactment of cybersecurity legislation. However, if it is subsequently determined that other companies, or the government, had advanced warning of the malware that struck the retailers, but were reluctant to disclose it, there may be a strong push for "information sharing" legislation that would encourage companies to share such critical information.

The breach also dramatically highlighted Congress' disjointed approach to privacy and cybersecurity legislation. Within days of the breach announcement, a diverse group of House and Senate committees announced hearings, including: the

House Subcommittee on Commerce, Manufacturing and Trade; the Senate Commerce Subcommittee on Consumer Protection; the Senate Banking Subcommittee on Security; and the Senate Judiciary Committee. Senate Commerce Committee Chairman Jay Rockefeller (D-W.Va.), who has been at the forefront of this issue for the last few years, stated in a letter to Target that the Senate Commerce Committee "has jurisdiction over commercial data practices and data security." While some view this as a turf war, others note that data security simply touches on multiple issues and industries, and hence comes under the jurisdiction of multiple Congressional committees. With no single committee spearheading the cybersecurity effort, the issue has become somewhat diluted, further hampering the possibility of any meaningful legislation being enacted.

The Target breach also spurred the reintroduction of specific legislative proposals. For example, Sen. Patrick Leahy (D. Vt.) reintroduced — for the fifth time — the Personal Data Privacy and Security Act, a bill he first introduced in 2005. The bill would, among other things:

- add violations of the Computer Fraud and Abuse Act to the definition of racketeering activity. This change would increase certain penalties for violating the Act and make it easier for the government to prosecute certain organized criminal groups who engage in computer network attacks;
- make it a crime to intentionally and willfully conceal a data breach;
- make it a felony to damage a computer that manages or controls national defense, national security, transportation, public health and safety, or other critical infrastructure systems or information;
- require businesses to create a data privacy and security program to protect and secure sensitive data, including by (1) regularly assessing, managing and controlling risks; (2) providing employee training; and (3) conducting tests to identify system vulnerabilities; and
- Create a federal data breach notification standard (discussed below).

DATA BREACH NOTIFICATION: Any company that has experienced a data breach that required nationwide consumer notification is all too aware of the patchwork of state notification statutes that exist. Statutes are in place in 46 states and the District of Columbia requiring that citizens of their state be notified in the event of certain data breaches. While there is clearly some overlap between the statutes, there are enough differences to frustrate any in-house counsel dealing with this issue. Therefore it is not surprising that the Target breach resulted in calls once again for a single omnibus data breach notification law.[1] For example, Sen. Leahy's Personal Data Privacy and Security Act includes a data breach notification requirement as does the Data Security Act of 2014 introduced by Sens. Tom Carper (D-Del.) and Roy Blunt (R-Mo.).

The fact that a single data breach notification law has not yet been passed is somewhat surprising. Many attribute it to a lack of consensus as to what type of event should trigger the notification requirement. Others feel that since some data breaches only impact residents of certain states, a federal law is not appropriate. Nonetheless, the Target data breach may spur more serious discussions about the establishment of a federal data breach notification requirement.

SEC DISCLOSURES. The Target data breach highlights the importance of disclosing data security risks. For example, Target's 2013 10-K cautioned, in pertinent part:

---

[1] A single notification law exists with respect to health information (under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et 5 seq.) and financial information (under the Gramm-Leach-Bliley Act (15 U.S.C. 22 6801(b)).

> *We have a program in place to detect and respond to data security incidents … If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. … The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.*

In 2011, the SEC issued guidance on cybersecurity risks noting that "although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."[2] To that end, the SEC specified that registrants should disclose the risk of cyber attacks if they are among the most significant factors that make an investment in the company speculative or risky. As part of this evaluation, "registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."

In the current cybersecurity environment, one could argue that the probability of a cyber attack is far greater today than in 2011 when the SEC guidance was issued. The SEC also addressed disclosures that should be made after a cybersecurity breach.

Overall, the Target breach serves as an important reminder to companies to review the October 2011 guidance from the SEC and their own disclosures regarding cybersecurity.

ACTIVE DEFENSE AND THE COMPUTER FRAUD AND ABUSE ACT (CFAA). In some situations, security experts believe that they could contain the damage caused by a security breach if they remotely accessed the third-party computers from where the breach was launched. What is hampering their efforts in these cases is not technological limitations, but rather the restrictions imposed by the CFAA.[3] Although there is no evidence that the security experts working on the Target breach had information that would have even made this option viable, the breach has highlighted the debate over whether the CFAA needs to be amended to allow this type of "self help" impact mitigation, also known as "active defense."

Under the CFAA, one is subject to civil and even criminal penalties if one "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer"[4] or "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage."[5] A company — whose intentions might be nothing more than to stop the damage caused by the data breach — would nonetheless be in violation of the CFAA. While one might feel that hackers should lose the right to privacy regarding their own computers, the reality is that "active defense" strategies might also require accessing innocent third-party computers that were unknowingly taken over by the hacker.

---

[2] SEC Disclosure Guidance: Cybersecurity. October 13, 2011.
[3] 18 U.S.C. § 1030.
[4] 18 U.S.C. § 1030(a)(2)(C).
[5] 18 U.S.C. § 1030(a)(5)(B).

Those who advocate for modifications to the CFAA argue that there should be an exception added for companies engaged in active defense. Some acknowledge that if an innocent third-party system is damaged in the process, the party engaged in the active defense should be liable for paying for such damage, but should not be liable for criminal activity.

Those opposing such changes to the CFAA express concern over making "active defense" (or "back hacking" as they sometimes call it) too readily accessible. Their concern is that companies, anxious to see retribution, might not limit their active defense to stopping the damage, but may seek to wreak havoc on the hacker. In addition, they argue that even if the "back hacker" is willing to pay for any damage they cause to an innocent third-party computer, the damage might negatively impact the third party's business in ways that are not compensable through monetary damages. Overall, they see no benefit — only the potential for great harm — in allowing companies to take these matters into their own hands.

LIABILITY FOR REISSUING CARDS. The Target data breach also reignited the long-simmering debate as to who should bear the expense for reissuing cards in the event of a data breach — issuing banks or retailers who suffered the breach. Banks typically argue that retailers should bear this expense, since it was a failure of their security that allowed the breach to occur. Retailers, on the other hand, maintain that since banks are not issuing cards with appropriate levels of security protection, they should bear the cost. In addition, Visa and MasterCard have imposed an October 15, 2014 deadline by when U.S. banks must issue, and retailers must accept, cards that use computer chips to store information — the prevalent form of card in Europe where credit card theft is less rampant. Banks and retailers have battled over who should bear the expense of this upgrade.

The Senate Banking Committee will likely consider this issue in its upcoming hearings on data security. Sen. Robert Menendez (D-NJ) has said that retailers should bear these costs and has pushed for supporting legislation, including a measure that would allow the Federal Trade Commission to impose fines or penalties on companies at fault. To date, the banking and retail industries each have pushed for legislation that would hold the other side liable for these reissuing costs, with the result that no legislation has moved forward.

CALIFORNIA FEDERAL JUDGE WINNOWS DOWN MASSIVE PRIVACY CLASS ACTION

When a company experiences a data breach resulting in the unauthorized access of personal information, a barrage of class action lawsuits undoubtedly follows. The key hurdle for the plaintiffs in most of these cases is that they have not suffered any actual harm or damage from the breach, and therefore may lack standing to bring an action. One federal judge in California recently issued a voluminous judicial ruling that sheds some light on the types of claims that may be viable in privacy class actions.

On January 21, 2014, California District Court Judge Anthony J. Battaglia dismissed the vast majority of claims asserted by plaintiffs in a putative nationwide privacy class action arising from a 2011 data breach that compromised the personal information of 31 million users of Sony's online gaming services.[6] Nonetheless, the court did allow several claims under various states' consumer-fraud laws to proceed.

---

[6] *See In re Sony Gaming Networks & Customer Data Security Breach Litig.*, No. MDL 11-2258, 2014 U.S. Dist. LEXIS 7353 (S.D. Cal. Jan. 21, 2014).

The lawsuit dates back to April 2011, when Sony discovered that individuals had hacked into its network and obtained its online gaming customers' personal information, including credit and debit card information. The Judicial Panel on Multidistrict Litigation consolidated a number of the resulting consumer lawsuits in August 2011, and the plaintiffs filed their first amended complaint in December 2012. The gravamen of the proposed nationwide class action is that Sony "failed to provide reasonable network security, including utilizing industry-standard encryption, to safeguard Plaintiffs' personal and financial information stored on Sony's network." The plaintiffs asserted 51 separate claims that fall into nine different sub-groups: (1) negligence; (2) negligent misrepresentation; (3) breach of express warranty; (4) breach of implied warranty; (5) unjust enrichment; (6) violation of state consumer-protection laws; (7) violation of the California Database Breach Act; (8) violation of the federal Fair Credit Reporting Act; and (9) partial performance/breach of the covenant of good faith and fair dealing. Sony moved to dismiss the first amended complaint, arguing that the plaintiffs lacked standing and that the claims were not viable.

Judge Battaglia first rejected Sony's standing argument, finding that the plaintiffs' allegations that their personal information was collected by Sony and wrongfully disclosed as a result of unlawful hacking was sufficient to confer Article III injury-in-fact standing. Even though the named plaintiffs did not actually claim that their personal information was accessed by a third party, the court determined that they plausibly alleged a "credible threat" of future harm based on the potential disclosure of their personal information. Judge Battaglia's standing ruling is noteworthy since plaintiffs in most data breach cases rely on future threats rather than actual harm to establish standing.

The court then turned its attention to the viability of each of the claims asserted in the first amended complaint. Judge Battaglia dismissed the negligence claims for a variety of reasons, including that the economic-loss doctrine barred negligence claims seeking purely economic damages. The court's decision serves as an important reminder that negligence and gross negligence provisions are often meaningless in breach of contract and other claims where monetary damages are available.

The court found that plaintiffs' claims for negligent misrepresentation were similarly deficient because, inter alia, plaintiffs failed to sufficiently allege a pecuniary loss caused by Sony's alleged misrepresentations. As the court explained, the plaintiffs' personal information did not have any independent monetary value, and registration and use of Sony's online services was provided to its customers free of charge. The court also dismissed the breach-of-warranty claims for multiple reasons, relying on choice-of-law clauses and disclaimers contained in various user agreements entered into by the plaintiffs. The claims for unjust enrichment fared no better, the court explained, because express contracts governed the same subject matter as the dispute between the parties.

The court next addressed the plaintiffs' consumer-fraud claims, dismissing some, but allowing others to proceed. Judge Battaglia declined to dismiss the plaintiffs' claims under California's Unfair Competition Law, False Advertising Law and Consumer Legal Remedies Act to the extent those claims were based on Sony's alleged misrepresentations and omissions regarding reasonable network security and industry-standard encryption. According to the court, "[a]lthough Sony seeks to combat these allegations by stating that Sony disclaimed any right to so-called 'perfect security,' … whether or not Sony's representations regarding 'reasonable security' were deceptive, in light of Sony's additional representations regarding 'industry-standard' encryption, are questions of fact not suitable for disposition on a motion to dismiss." The court's decision in this area highlights for companies the critical importance of vetting what statements they are making regarding data security.

Judge Battaglia also refused to dismiss claims brought under other states' consumer-fraud laws, including Florida, Michigan and Missouri. The court reasoned that the plaintiffs sufficiently alleged that Sony made misrepresentations or omissions regarding the security of its online network. Although the court permitted these claims to proceed, it did so only to the extent they sought declaratory or injunctive relief. According to the court, the Florida, Michigan and Missouri plaintiffs did not adequately allege actual damages caused by Sony's allegedly deceptive and unfair conduct. Judge Battaglia also refused to dismiss the consumer-fraud claim brought under New Hampshire law, recognizing that a showing of "actual damages" is not a prerequisite to obtaining statutory damages under that state's law.

The court found, however, that the plaintiffs failed to state a claim under New York, Texas and Ohio law. Judge Battaglia concluded that, under New York law, a loss of privacy resulting from the disclosure of personal information is not actionable. The court reached the same result with respect to the claim asserted under the Texas Deceptive Trade Practices-Consumer Protection Act. The court dismissed the consumer-protection claims brought under Ohio law, finding that the plaintiffs did not identify an act "substantially similar to an act or practice previously declared to be deceptive" by the Ohio attorney general or an Ohio state court.

Finally, the court evaluated the remaining claims under the California Database Breach Act and the Federal Fair Credit Reporting Act and for partial performance and breach of the covenant of good faith and fair dealing. The plaintiffs' claim under the California Database Breach Act was based on the allegation that Sony failed to notify plaintiffs of the hacking intrusion in the most expedient manner. The court concluded that plaintiffs could seek injunctive relief under the California Database Breach Act, but not economic damages because plaintiffs failed to allege how Sony's notification delay caused them any damages. The court dismissed the claims under the Federal Fair Credit Reporting Act on the ground that Sony is not a consumer reporting agency. But the court refused to dismiss the plaintiffs' claim for partial performance and breach of the covenant of good faith and fair dealing regarding a settlement agreement allegedly entered into between Sony and the plaintiffs' counsel, reasoning that such a claim can be based on an alleged breach of an "agreement to negotiate."

PRACTICE POINTS

There are a few key takeaways from the *In re Sony* ruling:

- Courts are split on what is required to establish Article III standing in data breach cases. As Judge Battaglia's ruling demonstrates, at least some courts are willing to find that the mere potential for unauthorized use of personal information is sufficient to confer Article III standing.
- Defendants facing privacy class actions involving negligence claims should be invoking the economic-loss doctrine and attacking plaintiffs' allegations regarding causation and injury.
- Plaintiffs may have a relatively easy burden for pleading consumer-fraud claims seeking declaratory and injunctive relief and recovering minimum statutory damages, even where the plaintiffs are unable to plausibly allege any actual damages.

WHITE HOUSE LAUNCHES "BIG DATA" REVIEW

In 2013, the FTC announced that "big data" — the collection and analysis of large troves of personal information — would be a front-burner item for the agency going forward. Now, the executive branch has big data on its radar as well.

On January 23, John Podesta, a counselor to President Obama, posted on the White House blog that he has been asked by the president to lead a comprehensive review of big data.[7] The working group will include Secretary of Commerce Penny Pritzker; Secretary of Energy Ernie Moniz; the president's science advisor John Holdren; the president's economic advisor, Gene Sperling; and other senior government officials.

The stated goal is to assess how privacy, the economy and public policy are impacted by developments in big data, and whether policy changes are required to deal with this technology advancement. Interestingly, the report will focus on both the private and public sectors and will suggest where "government action, funding research and consideration may be required." The group will consult with a wide range of stakeholders including industry groups, civil liberty groups, privacy experts, think tanks, academic institutions and other governments.

The group plans to generate a report within 90 days focusing on future technology trends and the key questions regarding big data, although Podesta cautions that it will be a preliminary overview and not a comprehensive new policy proposal.

Along with the working group, the President's Council of Advisors on Science and Technology will conduct an in-depth technological study of the intersection between big data and privacy.

Podesta's announcement is yet another example of the executive branch taking a leading role on privacy issues. In November 2012, President Obama appointed Nicole Wong as the White House's first chief privacy officer. And in February 2013, President Obama signed an executive order that has triggered a flurry of activity in the privacy area, including the NIST report discussed later in this mailing.

SENATOR ROCKEFELLER ISSUES DATA BROKER REPORT

On December 18, 2013, the Senate Committee on Commerce Science and Transportation, chaired by Sen. Jay Rockelfeller (D-W.Va.) issued its long-awaited report on the data broker industry: "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes" (the Report). The report marks the culmination of a 14-month investigation by Sen. Rockefeller, into an industry he characterized as worse than National Security Agency spying.

Data brokers are those entities that collect, analyze and maintain data on hundreds of millions of consumers, almost always without their knowledge, and then sell that data. In some cases, the purchasers of this data use it for fraud prevention and credit risk assessment, but of special concern to the committee, and the focus of the report, is the vast amount of data that is sold for marketing purposes without the permission or knowledge of the consumer. Such activity has raised significant privacy concerns.

The report includes as an example the much-publicized case of a teenager who data brokers determined must have been pregnant and then sent pregnancy materials to her home, even though she had not disclosed that information to her family. The report also expresses concern with the "buckets" that data brokers use to classify consumers, effectively creating lists of vulnerable consumers that predatory marketers purchase and exploit (*e.g.*, though the sales of high-cost loans and financially risky products).

[7] A copy of the announcement may be found at http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy.

In October 2012, Sen. Rockefeller kicked off the investigation by submitting questionnaires to nine representative data broker companies.[8] The questionnaires focused on four basic areas:

- what data is collected;
- how specific is that data;
- how does the data broker obtain that data; and
- who purchases the data and how is it used?

The report notes that a number of data brokers were not forthcoming in their responses, further convincing the committee that this industry lacks transparency. The report includes four key findings:

- Data brokers collect huge troves of information about hundreds of millions of consumers, including health and financial information, and items purchased and the method of payment. The amount of data being collected is increasing dramatically as consumers use smartphones and tablets to make purchases, and disclose their habits and preferences through social media sites. The "internet of things" (discussed on Page 13) will only further exacerbate this situation. The report expressed concern that, in many cases, consumers provide information — such as in a sweepstakes or survey — without realizing how their data will be used by a data broker.

- Data brokers classify data in a manner that identifies financially vulnerable consumers, without the knowledge of such consumers. This includes categories such as "credit crunched city families."

- Data brokers also collect and market "offline" information that their customers use to market online products. The report found that customers of data brokers include leaders in almost every possible industry, including credit card issuers; banks; automotive manufacturers; media companies; life/health insurers; lodging companies; airlines; and pharmaceutical manufacturers.

- Data brokers operate without any transparency since they are not consumer-facing. In addition, they often contractually require their customers not to disclose how they obtained the consumer data they have purchased. As a result, companies may have access to, and use, sensitive personal information about a consumer, without that consumer ever knowing.

It is difficult to assess whether the report is the first step towards some type of regulation of this industry. The report notes that a September 2013 U.S. Government Accountability Office report concluded there was no comprehensive law governing the collection and sale of consumer data, and that consumers had no ability to learn what information had been collected about them or to correct inaccuracies.[9] In addition, the FTC has been investigating the data broker industry since December 2012 and continues to list this industry as one of its main areas of concern.[10] However, without an omnibus and comprehensive data privacy law — which does not seem likely in 2014 — Sen. Rockefeller may be hard-pressed to push forward legislation that addresses the key concerns raised by the report. In addition, the Direct Marketing

---

[8] The nine companies were Acxiom, Experian, Epsilon, Reed Elsevier, Equifax, TransUnion, Rapleaf, Spokeo and Datalogix.

[9] Government Accountability Office, "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace," GAO-13-663 (Sept. 2013).

[10] Press Release, "FTC to Study Data Broker Industry's Collection and Use of Consumer Data, Federal Trade Commission" (Dec. 18, 2012) (available at http://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data).

Association has been advocating strongly for the voluntary adoption of its Ethical Business Practice guidelines, which would address some of these concerns if widely adopted.

APPOINTMENT OF NEW EUROPEAN DATA PROTECTION SUPERVISOR ON HOLD

On January 16, 2014, Peter Hustinx, the European Data Protection Supervisor (EDPS), completed his second and final five-year term. While Hustinx's shoes were seen as challenging to fill, many are surprised that a replacement has yet to be appointed.

The EDPS position was initially created in 2001 and held by Hustinx since 2004. The EDPS is tasked with monitoring privacy compliance in all EU institutions. Perhaps more importantly, the EDPS also has evolved into a highly-regarded body that advises the data protection authorities of individual member states, the European Parliament and the European Commission (EC) on data protection legislation. EU citizens who have filed complaints over right-to-privacy violations are funneled through the EDPS as well. Hustinx himself is widely respected, and influential, within the EU data protection community and has built a staff of some 50 people over the past 10 years.

The process to find a successor for Hustinx and for the assistant supervisor began in July 2013 with a public call for candidates, after which the EC would create a list to be vetted by the European Parliament and the European Council. On January 7, 2014, with a successor not yet selected, Hustinx wrote a letter to the European Commission; the Chairman of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs; and the Greek presidency of the council expressing his concern about the uncertainty that was being created because no successor was selected:

> *This uncertainty and the possible long delays that may be involved, as well as their different consequences, are likely to harm the effectiveness and the authority of the EDPS over the coming months. The EU is presently in a critical period for the fundamental rights of privacy and data protection, and a strong mandate is required to provide the authority to ensure that these fundamental rights are fully taken into account at EU level.*

Many had expected that, in response to Hustinx's letter, the EC would state that the process was nearing its conclusion. Instead, the EC announced, without further explanation, that no suitable candidates had been found and that the process was starting again. The EC also indicated that Hustinx would be encouraged to stay on. Some feel that political infighting over the direction of the EDPS and plans for a reform of EU data protection laws are behind the delay. We will continue to monitor developments in this area.

FTC TAKES ACTION AGAINST TWELVE COMPANIES FOR SAFE HARBOR VIOLATIONS

As reported in our December Privacy Mailing, the European Commission has expressed concern with the FTC's enforcement of the US-EU Safe Harbor — one of the frameworks available to U.S. companies to satisfy the "adequacy" requirement for transborder data flows from the EU under the EU Data Directive. These concerns sparked a report in which the European Commission set forth 13 recommendations to improve the protection afforded to EU residents under the Safe Harbor.

On January 21, the FTC announced that it had settled administrative actions brought against a dozen companies for claiming to be certified under the Safe Harbor, when in fact their certifications had lapsed. Significantly, it is not clear any of these companies were actually in violation of the seven EU privacy principles set forth in the Safe Harbor.

The FTC went after a diverse set of companies, perhaps as a signal that no industry is immune from FTC enforcement in this area. The 12 companies included, for example, three National Football League (NFL) teams, a broadband provider a mobile application developer, an accounting firm, a DNA testing lab, a clinical lab provider and a manufacturer of aluminum foil. Although the FTC noted that these companies "handle a variety of consumer information, including in some instances sensitive data about health and employment," some of the companies — such as the three NFL teams — are not the sort of companies that one would associate with heavy users of transborder data flows.

There is little doubt that the FTC was signaling to the European Commission a more active role in Safe Harbor Enforcement. Indeed, FTC Chairwoman Edith Ramirez said in a statement that these actions "help ensure the integrity of the safe harbor framework." Nonetheless, the FTC's action was in an area that was probably the least of the European Commission's concerns. The European Commission also wants greater enforcement against companies that are actually violating the Safe Harbor requirements.

The proposed settlement agreements are now subject to public comment. Under the settlements, the companies would be prohibited from misrepresenting the extent to which they participate in any privacy or data security program sponsored by the government or any other self-regulatory or standard-setting organization.

PRACTICE POINTS

- The FTC's actions might signal far greater enforcement of the Safe Harbor going forward. Companies should therefore be especially vigilant about making sure they are in compliance with the Safe Harbor and that they recertify each year. It is also important to remember that recertification is not a quick "check the box" process, but requires a careful review of the company's privacy activities to make sure the company is still in compliance.
- The FTC's actions also serve as a reminder that relying on the Safe Harbor presents FTC enforcement risks that are not present if an entity relies instead on the "model contracts" alternative offered by the EU.

NIST ABANDONS CONTROVERSIAL PRIVACY APPENDIX

As we have reported in previous privacy mailings, the National Institute of Standards and Technology (NIST) has been working towards a final draft of the Privacy Framework required by President Obama's February 2013 Executive Order. **The final report, which proposes guidelines for critical infrastructure entities, is due out on February 13, 2014.**

Prior drafts of the framework included an appendix that were described as a "methodology to address privacy and civil liberties considerations around the deployment of cybersecurity activities and in the protection of personally identifiable information (PII)." The methodology was based on the fair information practice principles referenced in the executive order and was organized by function and category to correspond with the framework.

Some provisions in the appendix were relatively innocuous such as "limiting the use and disclosure of PII to the minimum amount necessary to provide access to applications, services, and facilities" and "understand any mandatory obligations for reporting breaches of

PII." However, many felt that, overall, the appendix created the impression that there was consensus on data privacy, when none really existed. For example, the appendix also stated that companies should "provide that use of PII be solely for the specified purpose(s) and that sharing of PII should be for a purpose compatible with the purpose for which the PII was collected." There also was concern that the "references" listed in the appendix suggested there was more guidance on privacy available than really exists. NIST therefore concluded that "While stakeholders have said they see the value of guidance relating to privacy, many comments stated a concern that the methodology did not reflect consensus private sector practices and therefore might limit use of the framework."

The appendix will be replaced by a more general statement of companies' responsibilities for the collection of PII and will stress that those guidelines apply only as they relate to cybersecurity, and not more generally to commercial activity.

AMENDED AUSTRALIAN PRIVACY LAW GOES INTO EFFECT

A revised and more robust Australian Privacy Law that was passed in November 2012 goes into effect on March 12, 2014. The law, the Privacy Amendment (Enhancing Privacy Protection) Act 2012, amended the Privacy Act 1988 and was the culmination of nearly a decade of efforts directed towards strengthening data privacy laws and their enforcement mechanisms.[11]

The law applies to all businesses that earn more than AU$3 million per year and collect personal data, such as online retailers and technology-based companies. All federal government departments and agencies also will be required to follow the new privacy requirements.

The Privacy Amendment will introduce a number of important changes to Australia's current data privacy law:

- **HARMONIZATION OF PUBLIC AND PRIVATE SECTOR DATA PRIVACY REQUIREMENTS.** The Privacy Act 1988 initially applied only to the Australian government's use of personal information. Parliament did not develop data privacy requirements for the private sector until 2000. As a result, the public and private sectors are each covered under separate privacy principles. The Privacy Amendment unifies these parallel systems under one set of rules.
- **ESTABLISHMENT OF AUSTRALIAN PRIVACY PRINCIPLES.** The Privacy Amendment establishes 13 key principles for privacy protection in Australia, called the Australian Privacy Principles (APPs). These principles address the following subjects:
    1. *Open and transparent management of personal information.* Organizations must have ongoing practices and policies in place ensuring that personal information is managed in an open and transparent way.
    2. *Anonymity and pseudonymity.* Individuals have the option of remaining anonymous or using a pseudonym when dealing with the organization that has their personal information.
    3. *Collection of solicited personal information.* Organizations generally are prohibited from collecting personal information unless it is reasonably necessary for the entity's functions or activities.

[11] The Privacy Amendment is available online at http://www.comlaw.gov.au/Series/C2012A00197.

4. *Dealing with unsolicited personal information*. If an organization receives personal information that it did not solicit, it must destroy or de-identify the information, unless it could have collected the information under another principle.
5. *Notification of the collection of personal information*. Organizations must ensure individuals are aware that they collect their personal information.
6. *Use or disclosure of personal information*. Organizations that hold information for a particular purpose must not use or disclose that information for another purpose without consent, unless use or disclosure is permitted for another reason (for example, use or disclosure may be required by law or necessary to assist in locating a missing person).
7. *Direct marketing*. If an organization holds personal information, it must not use or disclose that information for direct marketing unless the individual consents or has a reasonable expectation that the personal information will be used for this purpose.
8. *Cross-border disclosure of personal information*. Before an organization discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.
9. *Adoption, use or disclosure of government-related identifiers*. Organizations must not adopt, use or disclose government-related identifiers as their own unless permitted under Australian law.
10. *Quality of personal information*. Organizations must take reasonable steps to ensure that personal information is accurate, up-to-date, complete and relevant to the reasons for its use and disclosure.
11. *Security of personal information*. Organizations must take reasonable steps to protect personal information from misuse and unauthorized access. Information that is no longer needed must be destroyed or de-identified.
12. *Access to personal information*. Individuals can request access to their personal information, unless an exception applies.
13. *Correction of personal information*. If an organization holds inaccurate or outdated personal data, it must take reasonable steps to correct the information. If the organization provided other organizations with the information, it must notify them of the corrections if requested by the individual.

While several of the APPs represent a consolidation of the old public and private systems, a number of them differ significantly from the existing principles, such as APP 7 on the use and disclosure of personal information for direct marketing, and APP 8 on cross-border disclosure of personal information.

- **EXPANDED DISCLOSURE REQUIREMENTS FOR DATA SHARING**. The Privacy Amendment expands the obligation to disclose data sharing. Under the Privacy Act 1988, if Company A collected personal information from an individual and wanted to share it with Company B, only Company A had an obligation to state in its privacy policy that it was sharing information with a third party; Company B had no obligation to provide similar information to that individual. The Privacy Amendment changes the existing obligation to also require Company B to state in its policies if and how the personal information it received will be used. Third-party online advertisers fall under these expanded disclosure requirements. The guidelines for the APPs explicitly discuss the use of purchase history and browsing habits stored on cookies to target online advertising to individuals, and state that these advertisers are required to have policies that inform individuals how their information will be used.[12] Opt-out mechanisms also are required.

[12]The guidelines are currently in draft form, and the privacy commissioner will issue the final guidelines prior to March 12, 2014. Consultation for the draft guidelines closed on December 16, 2013.

- **EXPANDED LIABILITY FOR DATA SHARING.** The Privacy Amendment makes data collectors liable for the misuse of personal information by authorized third parties. If a company collects personal information from users and then shares that information with a third party, not only is the company liable for misuse of the information by its own staff, but it also is liable for any misuse by the third party. It will be important, therefore, for companies that provide personal information to others to have clear contractual limitations on the third parties' information use, and clear liability coverage should the third parties violate those restrictions. Contractual limitations and liability coverage will be particularly important for companies that share personal information with third-party online advertisers in light of this expanded liability.
- **CIVIL PENALTIES FOR DATA PRIVACY VIOLATIONS.** Failure to adhere to the Privacy Amendment could result in significant monetary penalties. There was no financial penalty for non-compliance with the Privacy Act 1988. By contrast, under the Privacy Amendment, individuals who commit serious or repeated invasions of privacy will face fines up to AU$340,000, and government agencies or businesses could be fined up to AU$1.7 million for such violations. Australian Privacy Commissioner Timothy Pilgrim intends to take these enforcement mechanisms seriously, stating, "[T]he regulator would take its traditional conciliatory approach to breaches," but also warning that this approach "shouldn't be mistaken for a soft touch."[13]
- **ADDITIONAL CHANGES UNDER THE NEW PRIVACY LAW.** The Privacy Amendment implements a number of additional changes to Australia's privacy law, including greater use of external dispute resolution schemes to handle privacy-related complaints and more comprehensive credit reporting systems with a simplified complaints process.

The European Union traditionally has been a global leader in promoting data privacy and protecting personal information. However, Australia's Privacy Amendment is representative of an increasing number of countries making efforts to strengthen their privacy laws. As privacy regulations become stricter on a global level, companies should expect to revisit their privacy policies and practices to ensure compliance.

THE INTERNET OF THINGS — WHAT YOU NEED TO KNOW

The "Internet of Things" is the somewhat pedestrian name given to the wide range of physical products that can be operated through an internet connection: thermostats that one can program from a phone, refrigerators that signal what groceries to buy, roads that can monitor their own traffic patterns or wristbands that can report on your physical activity. As the technology to enable these devices becomes less expensive, manufacturers and developers are discovering innovative ways to enable devices to gather and transmit useful information. While these devices will present numerous benefits, there are concerns over physical safety. Some question whether security could ever be robust enough to stop a hacker from remotely commandeering a car or opening a door lock. However, an even greater concern is that these devices will transmit, and potentially expose, an unprecedented amount of personal information. As a result, the FTC has begun to take serious notice, proving that 2014 may indeed be a watershed year in the evolution of Internet-enabled devices and privacy.

In November, the FTC convened a public workshop to discuss the privacy and data security issues presented by the Internet of Things. In her remarks to the workshop, FTC Chairwoman Edith Ramirez signaled that the FTC is going to look closely at these issues. Ramirez cited the

[13] Andrew Colley, "Privacy Commissioner Plans Hardline Approach to New Act" (Nov. 25, 2013), available at http://www.itnews.com.au/News/365375,privacy-commissioner-plans-hardline-approach-to-new-act.aspx.

FTC's recent TRENDnet, Inc. enforcement action (in which a webcam company was charged with misrepresenting the security of its remotely operated webcams),[14] as a warning to companies to take security and privacy issues seriously. Ramirez indicated that developers should take three core principles into account when designing Internet-enabled products:

- *Privacy by Design*. Developers should build privacy and security features into new products during early development stages, rather than trying to add them later.
- *Consumer Transparency*. Consumers should be fully informed about the information being collected and how it is used and shared.
- *Consumer Control*. Consumers should have a degree of control over the use of their data.

In December, the FTC published a request for comment on these issues, asking that commenters consider a number of specific questions, including how privacy and security can be weighed against the potential societal benefits from these devices. Perhaps most significantly, the FTC also asked for comments on what it can do to encourage innovation in this area while protecting consumer privacy.

These questions from the FTC, and its decision to take action against TRENDnet, show that the commission intends to take an active role in protecting consumers as the Internet of Things evolves, and that it is considering whether to implement new regulatory recommendations or requirements in this area. Should more security and privacy issues with these devices come to light, the FTC may feel compelled to take a far more active role.

---

[14] For more information on the TRENDnet, Inc. case, see our October 2013 edition of *Privacy and Cybersecurity Update*, available online at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Alert_October_2013.pdf.

SKADDEN CONTACTS

STUART D. LEVI
Partner / New York
212.735.2750
stuart.levi@skadden.com

JESSICA D. MILLER
Partner / Washington, D.C.
202.371.7850
jessica.miller@skadden.com

JOHN H. BEISNER
Partner / Washington, D.C.
202.371.7410
john.beisner@skadden.com

JAMES S. TALBOT
Counsel / New York
212.735.4133
james.talbot@skadden.com