Skadden

PRIVACY & CYBERSECURITY UPDATE

MARCH 2014

CONTENTS

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 13, or your regular Skadden contact.

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

Four Times Square
New York, NY 10036

EU PARLIAMENT CEMENTS POSITION ON PRIVACY PROTECTION REFORM

On March 12, 2014, the European Parliament voted overwhelmingly in favor of the data protection reform package proposed by the European Commission, making Parliament's commitment to reforming the EU data protection regime irreversible. With this vote, the European Union is one step closer to new data-protection rules. The vote in the European Parliament ensures that the regulation remains on the table and will not change even if Parliament's composition changes following the European elections in May. To become law, the proposed regulation has to be adopted by the Council of the European Union, which is scheduled to publish its position in June. The long-awaited reform to EU data protection legislation aims both to give people more control over their personal data and to make it easier for firms to work across borders by ensuring that the same rules apply in all EU member states.

The data protection package that has been approved by the European Parliament consists of two pieces of legislation: a general data protection regulation that covers personal data processing and the free movement of such data, and a directive on personal data protection that covers data processed for law enforcement purposes. The proposed regulation received overwhelming support with 621 votes in favor, 10 against and 22 abstentions, while the proposed directive was endorsed with a somewhat divided vote (371 votes in favor, 276 against and 30 abstentions).

According to the European Commission, the data protection reform will ensure that individuals have more control over their personal data and make it easier for businesses to operate in the EU single market. The proposed reform gives more power to the users of online services, provides stronger safeguards for EU citizens' data that gets transferred abroad and considerably increases the fines that can be imposed on companies that break the rules.

Initially proposed by the commission on January 25, 2012, and now adopted by Parliament with significant amendments, the new regulation provides for a comprehensive reform of the EU's 1995 data protection rules to strengthen online data protection rights and boost Europe's digital economy. The commission's proposal updates and modernizes the principles contained in the 1995 Data Protection Directive, adapting them to the current online environment and building on the high level of data protection that has been in place in Europe since 1995.

The regulation, as adopted by Parliament, will make several key changes to the data protection regime, which are summarized below:

1. **One continent, one law**. The current inconsistent patchwork of national laws will be replaced with a more uniform law across all EU member states, making compliance easier and cheaper. Companies will need to comply with one omnibus law, not 28 individual local laws. According to the European Commission, the benefits of the reform are estimated at €2.3 billion per year.

2. **One-stop-shop.** The regulation will establish a one-stop-shop for businesses: companies will only have to deal with the supervisory authority in the country where they principally operate. Currently, companies doing business throughout Europe could end up dealing with 28 different authorities. This change will reduce the administrative burden on businesses. A European data protection board also will be created to coordinate the work of the national data protection authorities.
3. **The same rules for all companies**. The new regulation will apply to any organization that operates within the single European market, including non-EU companies, to ensure a level competitive field. As explained by the European Commission, European companies have to adhere to stricter standards than their competitors established outside the EU but doing business within the EU. With the proposed reform, companies based outside of Europe will have to apply the same rules.
4. **Better protection of personal data**. The new rules include:
    - a right to have personal data erased when a data controller no longer has a legitimate reason for it to be retained (*i.e.*, the so-called right to be forgotten);
    - new limits on "profiling" an individual (*i.e.*, attempts to analyze or predict a person's performance at work, economic situation, location, etc.); and
    - a requirement to use plain language to explain privacy policies.
5. **Stronger restrictions on data transfers to non-EU countries**. The European Parliament has approved stronger safeguards for EU citizens' personal data that gets transferred to non-EU countries. To better protect EU citizens against surveillance activities like those recently revealed, the European Parliament has amended the rules to require any firm (*e.g.* a search engine, social network or cloud storage service provider) to seek the prior authorization of a national data protection authority in the EU before disclosing any EU citizen's personal data to a third country. The firm also would have to inform the person concerned of the request.
6. **Deterrent fines, The European Parliament further strengthened the framework set forth in the initial proposal made by the commission**. The amended version of the regulation notably provides for heavier sanctions for companies that violate the rules. Under the proposed text, national data protection authorities will be given the power to fine companies up to €100 million or up to 5 percent of their annual global turnover, whichever is greater. This is a significant step up from the sanctions set forth in the commission's initial proposal, where the thresholds were respectively €1 million or 2 percent of global turnover.

Furthermore, Parliament's revised proposal contains a new article 43(a), which purports that decisions of courts or administrative authorities from countries outside the union requiring the disclosure of personal data shall not be "recognized or enforceable in any manner," unless otherwise provided for in a mutual assistance treaty or international agreement.

The prospects for any of the foregoing provisions to become law now depends on whether, and to what extent, the 28 union member governments represented in the Council of the European Union give their accord, which remains uncertain at this stage.

On the same day, the European Parliament also approved a separate nonbinding resolution that condemned U.S. spying and called for the suspension of trade negotiations with the U.S. should it fail to address these issues. The European Parliament also called for the immediate suspension of the Safe Harbor agreement (the voluntary data-protection standards for non-EU companies transferring EU citizens' personal data to the United States). According to members of the European Parliament, these principles do not provide adequate protection for EU citizens, and they urge the U.S. to propose new personal data transfer rules that meet EU data protection requirements.

EU PARLIAMENT PASSES CYBERSECURITY DIRECTIVE

Days after the European Parliament voted in favor of the General Data Protection Regulation (GDPR), it passed the Network & Information Security Directive (NIS), which has become commonly known as the "cybersecurity directive." The cybersecurity directive has three main components: (1) minimum security standards for critical infrastructure organizations (such as financial services, energy, health, transport and for "enablers of key internet services), (2) an obligation for critical infrastructure organizations to report to a national authority (to be determined) in the event of a security breach that significantly affects the continuity of critical services and supply of goods and (3) obligations on member state governments to improve cybersecurity protection and to cooperate to prevent attacks.

The minimum security standard requirement, like that of the U.S. NIST framework, is short on specific mandates, and instead requires security standards that are commensurate with the risk they face. For example, companies in the critical industries must implement security measures to "guarantee a level of security appropriate to the risk presented … having regard to the state of the art." Today, these requirements extend only to communication network and service providers.

The final directive that was passed included one major concession to Internet companies. The original proposals would have required enablers of information society services to provide breach notice as well. In the end, this industry group was removed from the notification requirement, and only companies that own, operate or provide technology for critical infrastructure facilities are required to notify.

As with the vote on the new data protection regulation, Parliament's passage of the cybersecurity directive is only the first step to actual member state legislation. The next step is for the EU bodies to arrive at mutually agreeable text for the European Council to adopt. Even if this were to happen in 2014, it will be a good two years before member state legislation would go into effect. In addition, many are saying that the cybersecurity directive and the GDPR should be adopted simultaneously, which could lead to further delays given the back and forth that is likely to place with the GDPR. The GDPR and the cybersecurity directive ill also will have to be reconciled in some ways. Each include, for example, different data breach notification requirements.

SEC HOLDS ROUNDTABLE ON CYBERSECURITY

The Securities and Exchange Commission recently held a roundtable on the issues and challenges cybersecurity presents for market participants and public companies. The roundtable is a means by which the SEC Commissioners can hear a variety of viewpoints and become better informed. Armed with this knowledge, the Commissioners will consider whether the SEC should take additional steps, in terms of regulation or other guidance, either to public companies generally or to entities regulated by the SEC, such as exchanges, investment advisers, broker-dealers and transfer agents. There is no timetable for further SEC action.

Although panelists' views may have varied on particular matters, there was universal agreement that cybersecurity threats are varied, constantly evolving, omnipresent and present critical issues for government agencies, public companies and market participants.

A number of themes of particular relevance to public companies were discussed by panelists, including:

- cybersecurity is not "just an IT issue" but an enterprise-wide operational risk;
- planning for cybersecurity threats is never "done," and there are no solutions that make the issue go away;

- companies should develop plans for how to address cyber incidents, including mitigation and business resiliency/recovery, internal communications and external communications to consumers, regulators and law enforcement and/or intelligence agencies;
- companies should develop a culture of cybersecurity where employees at all levels and across functions take responsibility for considering vulnerabilities and mitigating cyber threats;
- like other enterprise risks, cybersecurity is an area requiring oversight by a board of directors or a board committee. Cybersecurity expertise is not a criteria for board membership, but directors should ask questions and satisfy themselves that management has developed systems to monitor, address, remediate and recover from cybersecurity incidents;
- cybersecurity threat assessments should be risk-based and solutions have to consider other operational imperatives; and
- planned responses to cyber threats should be drilled or "war-gamed" and cannot simply sit on the shelf to be pulled out when the need arises.

A particularly difficult question for the SEC and for public companies relates to company disclosures regarding cybersecurity risks and incidents. The SEC's Division of Corporation Finance published guidance in October 2011, as a result of which risk factor disclosure has become common place. An investor representative on one panel observed that the disclosure has become boilerplate and that more disclosure would be useful to investors. Other panelists observed that company disclosure of cyber

incidents is typically driven by consumer protection laws rather than a view that the information is material to investors. Many panelists cautioned against disclosure requirements that would increase company vulnerabilities to cyber-attacks, and a former SEC Commissioner on the panel observed that more company disclosure may not be in the public's interest. While the SEC, among other questions, is likely to give further consideration to the question of whether public companies should be required to provide additional cybersecurity disclosures, there was a clear message from the majority of panelists to tread lightly.

It is also clear that cybersecurity will continue to be a topic of significant interest to the SEC and other government agencies, market participants, and public companies and their boards of directors.

EU AND APEC INTRODUCE GUIDE FOR CROSS-BORDER DATA TRANSFER COMPLIANCE

On March 6, 2014, data protection authorities from the EU and the Asia-Pacific Economic Cooperation (APEC) presented a comprehensive road map to help companies comply with their respective, and sometimes dueling, global data transfer rules. This guide, called a referential, identifies common requirements and relevant differences under EU and APEC privacy rules that govern intraorganizational transfers of personal data across borders and provides a framework that helps companies navigate the respective systems for easier compliance.

DEVELOPMENT OF GLOBAL DATA TRANSFER SYSTEMS

Companies are increasingly storing their own data (such as employee records) remotely and transferring it throughout their companies' worldwide locations. In order to guarantee protection of personal data in these intraorganizational transfers, the EU enacted mandatory regulations and APEC set forth guidance to protect personal data leaving their borders, particularly when such data may be sent to a country with weaker data privacy rules. This fragmented approach in data privacy legislation can make it difficult for multinational companies to simultaneously comply with each country's specific frameworks when transferring data out of those countries.

EU SOLUTION TO FRAGMENTATION: THE BINDING CORPORATE RULES (BCRS)

The EU Data Directive[1] prohibits the transfer of personal information to a country that does not have "adequate" data privacy protection (most countries, in the view of the EU, do not). One solution offered by the EU for companies that transfer data intracompany, but to a country without adequate data privacy protection, is for the company to adopt binding corporate rules (BCRs). BCRs ensure that the company has adopted adequate safeguards exist for privacy protection as mandated by the Data Directive. BCRs thereby offer a streamlined solution for multinational companies to send personal data intracompany from the European Economic Area to countries that do not ensure an adequate level of protection.

ADDRESSING DATA PROTECTION IN APEC: THE CROSS-BORDER PRIVACY RULES (CBPRS)

APEC, which consists of 21 Pacific Rim member economies, faced a similar challenge in guaranteeing privacy protection for intraorganizational data transfers due to the widely differing privacy laws within its membership. For example, some members, like Australia, Canada, Japan, Mexico, New Zealand and Singapore, have comprehensive privacy laws, while others, such as China and Indonesia, do not. Moreover, other countries, like the United States, have privacy laws that apply only in specific circumstances.[2]

In 2004, APEC members began to address this fragmentation by endorsing the APEC Privacy Framework to promote the free flow of personal information across borders while establishing meaningful privacy protection for such information. Three years later, APEC began developing CBPRs, which were officially completed in 2011,[3] to protect personal information moving between APEC countries by having companies develop internal business rules on cross-border data privacy procedures. Although CBPRs are not legally required across APEC, many countries adopt them as sound corporate policy. CBPRs use independent auditors to review and approve a company's privacy practices with a government regulator in the participating country providing an enforcement backstop. In the U.S., TRUSTe Inc., oversees the application of the APEC system, with the FTC providing the enforcement authority.

CHALLENGES FACING COMPLIANCE WITH BCRS AND CBPRS

Because the requirements for BCRs and CBPRs differ, multinational companies that transfer personal data around the world found it burdensome to try and comply with each set of policies. There was also a concern that companies might simply ignore the voluntary APEC CBPRs and focus only on the EU's mandatory BCRs. On the other hand, as the protection of personal information becomes increasingly important to the public, companies want to demonstrate their commitment to protect private data, regardless of whether they are required to do so by law.

REFERENTIAL FOR COMPLYING WITH BOTH SYSTEMS

Recognizing that companies face two different data privacy protection systems, APEC and EU officials, after a year of collaboration, created a referential to serve as a tool for companies seeking double certification under both systems.[4] The referential is a checklist that highlights the commonalities between the BCRs and CBPRs, and identifies additional requirements that

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[2] Information Integrity Solutions, Towards a Truly Global Framework for Personal Information Transfers, Sept. 2013, available at http://www.iispartners.com/downloads/IIS%20CBPR-BCR%20report%20FINAL.pdf.

[3] Asia-Pacific Economic Cooperation, APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines, 2012, available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.

[4] Federal Trade Commission, FTC Signs of Memorandum of Understanding with UK Privacy Enforcement Agency, March 6, 2014, available at http://www.ftc.gov/news-events/press-releases/2014/03/ftc-signs-memorandum-understanding-uk-privacy-enforcement-agency.

companies may need to follow in order to simultaneously apply for authorization in the EU and certification by an APEC accountability agent. However, the authors emphasized that the referential does not create a mutual recognition system, so companies must still certify under each system separately. However, the referential highlights a number of key themes in both systems and provides details as to which requirements are common to both systems, as well as the specific requirements needed for each if they do not overlap.

The referential lists 21 requirements under the BCRs and CBPRs, including identifying the reasons for cross-border transfer of personal information, outlining remedies for breach of data privacy, and ensuring ongoing monitoring and auditing of data protection systems. For each requirement, the referential specifically identifies: 1) a "common block" that describes the main elements that are required both for BCRs and CBPRs, and 2) "additional blocks" that present the elements specific to the BCRs and CBPRs.[5] Based on this framework, companies are encouraged to develop data protection and privacy rules that reflect their respective structures, policies and procedures.

NEXT STEPS

This referential represents the first step towards assisting multinational companies in complying with global data transfer rules. Next, stakeholders will be asked for their input to refine the referential. These efforts are representative of the increasing importance of complying with data privacy laws on an international level.

CALIFORNIA DECISION PROVIDES GUIDANCE ON PRIVACY POLICY MODIFICATIONS

A recent California state court action provides websites with guidance on how they can modify their privacy policies without running afoul of the law, at least in California. In *Rodriguez v. Instagram*,[6] the plaintiffs, in a putative class action suit, challenged certain changes that photo-sharing application Instagram made to its privacy policies, particularly as it relates to user-generated content. The plaintiffs asserted that Instagram breached its contractual obligation of good faith and fair dealing and violated California unfair competition law. The court disagreed.

In December 2012, Instagram notified users that it intended to update its terms of use in one month. The most significant change, and the one that was the subject of the suit, related to Instagram's rights to user generated content posted on the site. Under the original terms, Instagram had certain license rights to use and modify such content. The new terms also gave Instagram the right to sublicense such content and removed any restrictions on Instagram's license rights.[7] During the one-month notice period, users had the right to opt out of using the site, but if they remained on the site they were deemed to have accepted the new terms.

The plaintiff challenged Instagram's unilateral decision to change its policies and to force users to stop using the service or be deemed to have consented to them. The plaintiff also argued that even if a user opted out of the service, Instagram would not purge the user's legacy content and would have the right to use such content under the terms of the new policy (to which the user never consented). Interestingly, and potentially fatal to her case, the plaintiff kept using Instagram even after the new policy went into effect.

---

[5] Asia-Pacific Economic Cooperation, Joint Work Between Experts from the Article 29 Working Party and from APEC Economies, on a Referential for Requirements for Binding Corporate Rules Submitted to National Data Protection Authorities in the EU and Cross Border Privacy Rules Submitted to APEC CBPR Accountability Agents, March 2014, available at http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

[6] CGC-13-532875 (San Francisco Sup. Ct. Feb 28, 2014).

[7] The revised policy also added a liability waiver.

The court ruled that, under the terms of its stated policies, Instagram had the unilateral right to change its policy, that it had provided clear notice to consumers of the planned change, that choosing not to opt out was an acceptable means of signifying consent to the change, and that plaintiffs had been given ample opportunity to opt out. As a result, Instagram had neither breached its contractual obligation of good faith and fair dealing nor violated California unfair competition law. With respect to the unfair competition claim, the court observed that Rodriguez could not "possibly have had a reasonable expectation of perpetual use of Instagram's service under the original terms," especially since Instagram "expressly claimed the right to modify the terms on notice or terminate service for any reason without notice."

While Instagram had the right to change its policy, the interesting question remained as to whether Instagram could apply its new policy to content that was posted under the old policy. Unfortunately for companies and practitioners looking for guidance on this common issue, the court was able to sidestep this question because the plaintiff never alleged that Instagram was using her legacy content in violation of the original policy (but in compliance with new policy). While the plaintiff maintained that such usage was inevitable, the court noted that the original policy allowed Instagram to preserve content after a user deleted her account, and the plaintiff had consented to the new policy by continuing her use of Instagram. The court also noted that by consenting to the new policy, the plaintiff waived any claim of harm.

It is important to note that some courts reject unilateral modifications to terms and conditions on the grounds that the right to so modify a policy creates an illusory contract. See, for example, *Harris v. Blockbuster*[8] and *In re Zappos.com Inc., Customer Data Security Breach Litigation*.[9] However, each of these cases is arguably distinguishable from *Rodriguez*. In *Zappos*, the court held that the terms of use were so buried and inaccessible that there was arguably no contract formed with the customer; while in Blockbuster, the user had no way to opt-out of the new terms, as *Blockbuster* made the new terms effective immediately.

Perhaps most importantly, even if companies adhere to the same process as set out in Rodriguez to change their terms and conditions, they still may face an FTC action. The FTC's 2012 Privacy Report was sharply critical of "take it or leave it" policies, particularly where customers have limited alternative options.[10] The FTC has also demonstrated a willingness to go after companies that change their policies in such a way that allows them to collect more data or use the data in more expansive ways. The FTC pursued one such action against Gateway Learning Corp.[11], finding that it changing its privacy policy to use information more expansively constituted an unfair business practice.

PRACTICE POINTS

The holding in *Rodriguez* provides companies with a roadmap, at least in California, as to how they can change their privacy policies or terms of use (including by expanding their rights) within the contours of the law. Companies should ensure they take the following steps:

- Expressly reserve the right to alter the terms in the original policy;
- Make changes that are consistent with the language of the original terms;
- Give users notice before implementing revisions, thereby creating a period during which users can opt out; and
- Inform users that continued use of the service constitutes acceptance of the new terms.

---

[8] *Harris v. Blockbuster Inc.*, 2009 WL 1011732 (N.D. Tex. April 15, 2009)
[9] *In re Zappos.com Inc., Customer Data Security Breach Litigation*, 2012 WL 4466660 (D. Nev. Sept. 27, 2012).
[10] FTC Report: *Protecting Consumer Privacy in an Era of Rapid Change*, March, 2012
[11] *In the Matter of Gateway Learning Corp.*, Docket NO. C-4120 (September 10, 2004).

Rodriguez provides precedent that in California, opt-in consent or click-wrap assent is not required if a website policy permits changes. What remains open, however, is whether a site can apply the terms of the new policy to information or content that was collected under a different policy in cases where the user opted out of the new policy. Sites seeking to use "legacy" content under the terms of a new policy should consult with counsel as to the best approach to minimize or eliminate any risk from such usage.

CALIFORNIA ISSUES SECURITY GUIDANCE FOR SMALL BUSINESSES

On February 27, the California attorney general — working with Lookout, a mobile security company, and the California Chamber of Commerce — issued guidance regarding cybersecurity for small businesses (defined as those with under 500 employees). The guide, titled "Cybersecurity in the Golden State: How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents,"[12] urges all small businesses to adopt good security practices and offers a compelling case for why doing so is in their best interests.

The guide is replete with statistics to reinforce the message that small businesses are increasingly becoming the targets of cybercriminals and failing to take preventative measures is simply bad for business. Highlights, which are noteworthy to large companies as well, include:

- more than 99 percent of all employers in the state are small businesses, employing over 8.7 million workers;
- 98 percent of small businesses report using wireless technology, 85 percent use smartphones in their operations and 31 percent use mobile apps;
- more than one billion cyberattacks occurred within the *first quarter* of 2013;
- in 2012, half of all targeted attacks were aimed at businesses with fewer than 2,500 employees, and businesses with fewer than 250 employees comprised 31 percent of all cyberattacks;
- the average cost to victims of a data breach per compromised record is $136, or $157 if the breach resulted from malicious criminal conduct;
- costs for businesses that are victims of Internet-based attacks have risen 78 percent per year over the past four years; and
- the average estimated cost to companies that are the victims of data breaches is in excess of $130 per victim whose personal information was compromised.

Suggestions for best practices are described in three categories: (1) paradigm shifts to increase the likelihood that businesses will adopt good security practices, (2) steps to mitigate the risk that a security breach will occur and (3) preparing for a security breach if it does occur.

PARADIGM SHIFTS

The guide stresses no business is too small to be a target, and that business owners and managers must lead by example by being involved in, and dedicating time and resources to, IT security.

IMPROVING SECURITY PRACTICES

It also discusses how security practices can be adopted and implemented without employing a fulltime IT specialist (which most small companies do not have). The guide provides a step-

[12] Available at https://oag.ca.gov/cybersecurity.

by-step illustration for small businesses to improve their security practices and implement a disaster recovery plan:

1. **IT Security 101**.
    a. Keep software and operating systems updated.
    b. Do not install software from an unknown source.
    c. Limit who has (and uses) administrator privileges.
    d. Ensure that corporate wireless networks are secure and avoid public wireless connections to conduct company business, unless the connection is identified as secure (*e.g.*, SSL, VPN).
    e. Implement hardware and software firewalls and install and maintain anti-virus software.
2. **Secure Banking**. The guide identifies several practices that businesses should consider relating to online banking:
    a. Conduct online banking sessions in a web browser's private mode and delete the browser's cache and other files after the session in case the system has been compromise.
    b. Implement two-factor authentication for account access.
    c. Require two signatories to transfer funds and limit dollar amounts of wire transfers.
    d. Require two executive team signatures to initiate foreign wire transfers.
    e. Establish account notifications for higher-risk activities.
3. **Passwords**. Companies should require passwords for user accounts and for routers and other hardware.
4. **Encryption**. Encryption technology, which scrambles data to render it inaccessible to cybercriminals and others without the password, is easy to use and freely available, and it adds an additional layer of data protection.
5. **Education**. Employees should be trained on how to avoid malware and similar attacks. Investing in hardware and software to protect a computer network is ineffective if employees click on links or attachments from unknown or untrusted sources.

DISASTER RECOVERY PLAN

1. **Data Mapping and Data Pruning**. A company can minimize the harm resulting from a security breach by reviewing the company's data, and identifying who has access to the data and how it is used — including any backup, archival and cloud storage. In addition, companies should:
    a. Purge the system of unnecessary data; the company retains without any business need.
    b. Understand who has access to data and limit access to an as-needed basis.
    c. Segregate systems that house sensitive data from computers used to browse the Internet.
    d. Ensure that valuable data is backed up regularly — at least once a month.
2. **Create a Plan**. Every company should have a plan to handle cyberattacks when they occur, including compliance with breach notification laws. The guide advises that small businesses should prepare a response plan that is appropriate for the size of the business, the types of technology that the business uses, and the types of data that the company collects and retains.

PRACTICE POINTS

By providing a suggested roadmap for businesses, albeit small ones, the state may also have effectively created a benchmark that plaintiff's lawyers might use when challenging a company's security protocols in the event of a data breach. As a result, all companies — regardless of size — should review the recommendations set forth in the guidance.

SKADDEN ATTORNEYS MEET WITH DOJ NATIONAL SECURITY DIVISION

Earlier this month, Skadden attorneys Stuart Levi, Jamie Talbot and Joshua Gruenspecht met with Kimberley Raleigh, a counsel in the National Security Division (NSD) of the Department of Justice. NSD is the DOJ branch charged with combating terrorism, espionage and other threats to national security, in coordination with prosecutors and the intelligence community. Ms. Raleigh spoke to our attorneys about the NSD's program to reach out to private sector companies to increase their awareness of the growing national security threat to their information technology, particularly within certain sectors of the economy.

Over the last few years, NSD has seen the nature of the cybersecurity threat online change and expand. Theft of confidential business information and proprietary technologies through cyber intrusions is occurring on an unprecedented scale; the financial sector has experienced a pattern of disruptive nation state attacks; and foreign adversaries are increasingly seeking the ability to sabotage U.S. critical infrastructure systems. The Computer Crimes and Intellectual Property Section (CCIPS) historically has been the arm of the DOJ charged with investigating and prosecuting computer crimes and other thefts of material protected by copyright, trademark or trade-secret designation. However, while CCIPS continues to have primary responsibility for pursuing computer criminals, NSD is increasingly playing a role in prosecuting this new wave of cyberattacks with implications for national security. CCIPS and NSD have joined together to create a new National Security Cyber Specialist (NSCS) network within the DOJ, which is responsible for ensuring that the appropriate expertise is brought to bear in the event of a national security-level cyberattack. The network works closely with the FBI's National Cyber Investigative Joint Task Force and with the cyber task forces located in each of FBI's 56 field offices.

Ms. Raleigh indicated that the NSD wants to inform Skadden's critical infrastructure clients — most notably those in the telecommunications, defense, banking/finance and energy infrastructure sectors — that after a national security cyber event, government resources stand ready to assist. The network has trained national security cyber specialist Assistant U.S. Attorneys in each U.S. attorney's office. In most cases, these attorneys also are designated as Computer Hacking and Intellectual Property (CHIP) or Anti-terrorism Advisory Council (ATAC) prosecutors. Clients can ask for these experts directly when they need access to prosecutors with an in-depth knowledge of network security breaches, national security threats or both in order to review security breach information and assist in pursuing those responsible. Clients also may contact the NSCS network in Washington at NSCS_Watch@usdoj.gov for additional information or assistance with national security cyber matters.

In addition, the FBI has created a new secure information exchange portal for industry partners. iGuardian allows pre-cleared staff members with cybersecurity responsibilities to securely file online reports on cybersecurity events and then follow any further government activity on the matter. Later this year, portal users will be able to submit malware files for technical analysis by the FBI using the Malware Investigator tool. Malware Investigator will not only collect and archive the files, but will provide a report to the submitter in a matter

of minutes or hours describing the damage the malware can inflict. A brief summary of the iGuardian program provided by the NSD can be found on the FBI's website.[13] The portal is scheduled to be available for use in April 2014. Clients can apply for an account on the FBI's website, www.fbi.gov.

FEDERAL JUDGE APPROVES NO-INJURY DATA BREACH CLASS SETTLEMENT

On February 28, 2014, a federal judge in the Southern District of Florida approved a $3 million data breach class action settlement between health insurance company AvMed, Inc. and insured plaintiffs.[14] The settlement, which provides compensation to class members regardless of whether they suffered any direct harm from the data breach, is the first of its kind and may spawn similar class settlements in the privacy arena.

The case arose out of a December 2009 theft of two unencrypted laptops containing the personal information of thousands of individuals receiving health care coverage through AvMed. The plaintiffs subsequently commenced a putative class action against AvMed, asserting claims for, *inter alia*, negligence, breach of contract, breach of fiduciary duty and unjust enrichment. The plaintiffs sought to represent a class of AvMed customers whose personal information was stored on the stolen laptops and a subclass of individuals whose identifies were stolen since the laptop theft. The district court dismissed the claims against AvMed on two separate occasions, finding, among other things, that the plaintiffs had failed to allege a cognizable injury under both Article III standing principles and Florida tort law. On appeal, the Eleventh Circuit reversed, holding that the complaint sufficiently alleged injury to withstand the defendant's motion to dismiss.[15]

The Court of Appeals first addressed the issue of Article III standing, holding that the plaintiffs' claim of actual identity theft resulting from the data breach "constitutes an injury in fact under the law." The court also found that the complained-of conduct — AvMed's negligent failure to secure personal information on the laptops — caused the subsequent theft of those laptops and the ensuing identity theft. The court's Article III standing analysis ended with a perfunctory conclusion that an award of compensatory damages would redress the plaintiffs' complained-of injuries.

The Eleventh Circuit then proceeded to evaluate the issue of injury and causation under Florida tort law. The court summarily determined that the plaintiffs' allegations of "financial injury" were sufficient under Florida contract and negligence law. The analysis regarding causation was somewhat more fulsome, with the Court of Appeals focusing on whether a sufficient "nexus" had been alleged between the data breach and the subsequent identity theft. The court focused on the following allegations with respect to one of the named plaintiffs: (1) personal information was stored on one of the stolen laptops, (2) the plaintiff's identity was stolen and (3) the stolen identity was used to open unauthorized accounts. Relying on an unpublished ruling by the Ninth Circuit, the Eleventh Circuit concluded that the allegations of causation were adequate. The court did so even though the time span between the actual data breach and the identity theft was between 10 and 14 months" — more than six times greater than the one" at issue in the Ninth Circuit case. Therefore, because the complaint sufficiently alleged injury and causation for purposes of Article III standing and Florida tort law, the Eleventh Circuit held that most of the claims could proceed.

---

[13] http://www.fbi.gov/stats-services/iguardian.
[14] *Curry v. AvMed, Inc.*, No. 10-CV-24513-JLLK (S.D. Fla. Feb. 28, 2014)
[15] *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012). While the Court of Appeals allowed most of the claims to proceed, it did conclude that plaintiffs had failed to state claims for negligence *per se* and breach of the implied covenant of good faith and fair dealing.

In the wake of the Eleventh Circuit's ruling, AvMed once again moved to dismiss the claims. After the district court denied the motion, the parties entered into settlement negotiations, which resulted in a $3 million settlement that recently was granted final approval. Under the terms of the settlement, class members whose personal information was on the laptops but who have not suffered identity theft will receive up to $10 for each year they paid AvMed an insurance payment, subject to a $30 cap. In addition, AvMed has agreed to pay actual damages to any class members who actually suffered identity theft as a result of the data breach. The settlement has allocated $250,000 to cover identity theft claims.

The settlement marks a significant development in the area of privacy class action law in that it awards money to individuals who were not harmed by the data breach underlying the lawsuit. Courts previously have rejected claims by consumers suing based on data breaches where the plaintiffs allege only that they may become victims of identity theft sometime in the future. Given the recent uptick in the number of data breach incidences being reported in the media, it will be interesting to see if this settlement results in more class actions, although the relatively small value of the settlement may make such class actions unattractive to plaintiffs' lawyers.

The settlement illustrates an increasingly vexing question in class action practice — namely, whether class members must satisfy Article III standing, even in the class settlement context. Indeed, this very issue was highlighted in a series of recent decisions issued by the Fifth Circuit in the Deepwater Horizon litigation. The Court of Appeals questioned whether individuals who did not suffer actual economic losses as a result of the oil spill could recover under a class settlement. While the Fifth Circuit ultimately resolved the question in favor of the class, the decisions suggest that some showing of Article III standing on the part of absent class members is a requirement for approving class settlements.

AN FCC PERSPECTIVE

Attorneys from Skadden's Privacy and Cybersecurity Group attended the Internal Association of Privacy Professionals' Global Privacy Summit meeting held in Washington D.C. in early on March 5-7. An associate general counsel of the Federal Communications Commission, Jennifer Tatel, addressed her agency's views on privacy. Given that the FCC is often not mentioned when considering privacy issues, we thought it would be useful to share her views.

Ms. Tatel highlighted that the jurisdiction of the FCC in the area of privacy is limited by the scope of the 1996 Telecommunications Act. This act has not been amended in close to two decades, and its privacy provisions did not contemplate the massive amounts of data mining and exploitation that is taking place today. As Tatel noted, the only provision in the Telecommunications Act that relates to privacy concerns the use of customer proprietary network information (CPNI). This provision prevents regulated entities from using or disclosing individually identifiable information about calls traveling over their networks, including number dialed, time date of all, and duration of the call, unless it is for the purpose of providing or supporting their telecommunications services. Any activity by a regulated entity regarding other data that is not included in the definition of CPNI would not be regulated. It should be noted that some groups have maintained that the CPNI definition is too narrow since data miners could identify an individual by reverse engineering their call data.

(Attorney contacts appear on the next page.)

SKADDEN CONTACTS

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

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

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

MARC S. GERBER
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

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

GREGOIRE BERTROU
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@skadden.com

OLIVIER BOULON
Associate / Paris
33.1.55.27.11.32
olivier.boulon@skadden.com