Skadden

Privacy & Cybersecurity Update

European and US Officials Release Details of 'Privacy Shield' to Replace Safe Harbor

European and U.S. officials have reached an agreement on a replacement for the U.S.-EU Safe Harbor, called the "Privacy Shield," that if enacted will provide a new mechanism to allow transfers of personal data from the European Union to the U.S. While the principles governing such transfers remain largely the same as those of the Safe Harbor, there are a number of new reporting and dispute resolution obligations with which U.S. companies who use the Privacy Shield would need to comply.

As discussed in a special edition of *Privacy & Cybersecurity Update*, European and U.S. officials declared on February 2, 2016, that they had reached an agreement on a framework to replace the former U.S.-EU Safe Harbor invalidated by the Court of Justice of the European Union in October 2015. Christened the "Privacy Shield," the new framework seeks to alleviate European concerns about indiscriminate access to personal data by the U.S. intelligence community, guarantee European citizens effective avenues of redress when their privacy has been compromised and increase oversight and enforcement. On February 29, 2016, the parties released the text of the agreement as well as a draft adequacy decision by the European Commission. While the Privacy Shield would provide a new framework to transfer personal data from the EU to the U.S. for companies that had relied on the Safe Harbor, the framework still must go through several stages of bureaucratic review and formal adoption in the EU.

Background: *Schrems* and the EU-US Privacy Landscape

In October 2015, in *Schrems v. Data Protection Commissioner*,[1] the Court of Justice of the European Union invalidated the then-current Safe Harbor framework agreement between the EU and U.S. The framework had allowed companies that self-certified to

[1] Case number C-362/14, in the Court of Justice of the European Union.

the Safe Harbor with a means to transmit personal information from the EU to the U.S. despite the European Union's assessment that the United States does not have "adequate" data protection laws in place. In its *Schrems* decision, the court found that the existing framework did not adequately protect the interests of data subjects, primarily because of the ability of the U.S. government to access personal data for national security purposes and the lack of recourse available to EU residents who felt their privacy rights had been violated fundamentally.

Following this ruling, the Article 29 Working Party (WP29), comprised of representatives from the data protection authorities of each EU member state, issued a statement that they would not take enforcement actions against companies relying on the Safe Harbor until January 31, 2016, to give the U.S. and EU time to negotiate a new framework for the transfer of personal data from the EU to the U.S.

The Privacy Shield

On February 2, 2016, two days following the deadline set by WP29, U.S. and EU officials announced that a new framework agreement had been reached. Text containing the framework principles was subsequently released on February 29, 2016, by the U.S. Department of Commerce. In light of the agreement on the Privacy Shield announced by U.S. and EU officials, WP29 has extended its grace period for use of the Safe Harbor at least through its review of the written framework, currently estimated to take place in April 2016.

The Privacy Shield consists of the framework principles plus official representations and commitments by six U.S. governmental authorities. Although substantively similar to the Safe Harbor principles, the Privacy Shield imposes on U.S. government entities and companies obligations aimed at providing transparency regarding national security limitations, effective avenues of recourse for European citizens whose data has been misused and more rigorous enforcement mechanisms.

Compliance With the Privacy Shield Principles

While the greatest focus of the Privacy Shield appears to be U.S. government transparency and accountability (discussed in further detail below), companies would have to undertake more robust commitments under the new framework. Of particular note, the Privacy Shield now contains certain specific requirements for the transfer of intracompany human resources data.

Privacy Shield Certification

As part of its oversight efforts, the Department of Commerce would require companies wishing to participate in the Privacy Shield to publicly declare their privacy commitments, making the commitments enforceable under U.S. law by the Federal Trade Commission. Companies that use the Privacy Shield to transfer HR data from the EU to the U.S. in the context of an employment relationship would be required to state this at the time of certification and conform to specific requirements regarding such data. Companies would be required to undergo annual recertification and could be removed from the list of certified companies at any time for persistent failure to comply. The Department of Commerce would publish not only a record of organizations that are certified but also a conspicuous list of organizations that had previously self-certified but that have been removed from the Privacy Shield List. Any company that has been removed from the list must cease to hold itself out as a participant in the Privacy Shield. Companies would be required to respond to detailed questionnaires from the Department of Commerce designed to verify ongoing compliance with the Privacy Shield. Companies that cease to exist as a separate legal entity as a result of a merger or otherwise must notify the Department of Commerce and indicate whether the resulting entity will continue to be bound by the Privacy Shield by operation of law or new election to self-certify. Otherwise, they must delete any personal data acquired under the Privacy Shield. The increased focus on recertification is undoubtedly in response to one of the main criticisms of the Safe Harbor — namely, that companies would simply renew their certifications without doing the necessary diligence to ensure they were still in compliance.

Privacy Shield Principles

Like the Safe Harbor, the Privacy Shield would require adherence to seven broad data privacy principles: notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement and liability. The functional and administrative obligations underlying most of these principles, though set out in more detail than under the Safe Harbor, will not require companies to make drastic changes to their data transfers as conducted under the former arrangement. However, companies should anticipate certain enhanced obligations related to accountability, enforcement and recourse. Key obligations for companies are highlighted below:

- **Notice:** A company participating in the Privacy Shield would be required to notify individuals in clear and conspicuous language about a number of aspects of the company's privacy practices, including (1) the types of personal data collected, (2) how such information is collected and used, (3) the identity of third parties to which it discloses such information and why, (4) the means the company offers to individuals to limit the use of their data, (5) the independent dispute resolution body designated to address complaints and provide recourse free of charge (as discussed in further detail below), and (6) the investigatory and enforcement powers to which such company is subject. This notice must be provided at the time the individual is first asked to provide personal information or as soon as

practicable thereafter, but in any event before the information is disclosed to a third party.

- **Choice:** A company participating in the Privacy Shield would be required to offer individuals the opportunity to opt out of disclosure of their information to a third party or use of their information for a purpose materially different from that for which it was originally collected. The opt-out mechanism must be clear, conspicuous and readily available. Note that if the information is sensitive (*e.g.*, medical information or information relating to ethnicity, political views, religion or the like), the opt-out mechanism is not sufficient and the company must obtain an affirmative opt-in from the individual before any such disclosure or use.
- **Onward Transfer:** Companies would be required to provide a variety of assurances that any third parties to which they transfer European data will provide adequate protection as well. As noted above, companies must provide individuals advance notice and the choice to opt out of transfer to third parties that will act as data controllers, and must enter into a contract with any such third-party controller that limits data processing to purposes consistent with the consent provided by the data subject and requires the third-party controller to accord the transferred data the same level of protection as the Privacy Shield provides. Companies would also be required to enter into contracts where they transfer data from the EU to the U.S. for processing purposes only, in order to ensure that the processor will act only on the controller's instructions and will provide appropriate protections against unauthorized use, access or loss of data. While companies would not be bound to these specific steps when data is transferred to a third party acting as an agent, similar principles apply: companies would be required to transfer data only for specified purposes, to ascertain that the agent is obligated to provide at least the same level of privacy protection as required by the Privacy Shield, and to take reasonable steps to ensure that data is processed in a manner consistent with the companies' obligations and to remedy the situation when it is not. Companies would be liable under the Privacy Shield where an agent processes personal information in a manner inconsistent with the framework, unless the company can prove that it is not responsible. Companies that certify within the first two months following the Privacy Shield's effective date would have nine months to bring existing commercial relationships into compliance.
- **Security:** Companies participating in the Privacy Shield would be required to take "reasonable and appropriate measures" to protect personal information from loss, misuse and unauthorized access.
- **Data Integrity and Purpose Limitation:** Companies would be required to refrain from processing personal information in a way that is incompatible with the purposes for which it had been collected or as otherwise authorized by the individual.
- **Access:** A company participating in the Privacy Shield would be required to give individuals access to the information held by the company about them and be able to correct or delete any inaccurate information. A company may charge a fee for this access that is not excessive. In addition, a company may decline to provide this access where the burden of providing it would be disproportionate to the risks to the individual's privacy, or where the rights of persons other than the requesting individual would be violated.
- **Recourse, Enforcement and Liability:** Consumers would be encouraged first to raise any complaints with a company directly. Companies would be required to respond to these complaints within 45 days. The Privacy Shield would guarantee free independent dispute resolution processes to EU citizens, the cost of which would be borne largely by the companies that certify to the Privacy Shield. Companies would be required to select and provide an "independent recourse mechanism" to investigate unresolved complaints at no cost to individuals, which may take the form of a panel of data protection authorities (DPAs) established at the EU level, an EU-based alternative dispute resolution provider or a U.S.-based alternative dispute resolution provider. Companies that transfer HR data for employment purposes under the Privacy Shield would be obligated to select the DPA form of independent recourse mechanism.

  Companies that elect (or are required) to rely on the panel of DPAs to fulfill this requirement must declare this commitment in their self-certification. Companies would then be required to cooperate in the investigation of complaints and comply with any advice given by the DPA panel, including remedial or compensatory measures, within 25 days. Failure to comply could be referred to U.S. authorities. Companies choosing this option would pay an annual fee of no more than US$500 (with lesser amounts that have not yet been specified for smaller companies) and necessary translating expenses.

  Dispute resolution bodies would be encouraged to award sanctions that are "sufficiently rigorous to ensure compliance." These sanctions include publicity for findings of noncompliance, data deletion, compensation for losses and injunctive awards, as determined based on the severity of violation and the sensitivity of the data concerned.

  Where both the complaint and independent recourse processes leave claims unresolved, the Privacy Shield would offer consumers the option of an arbitration proceeding authorized to provide nonmonetary equitable relief, such as access, correction, deletion or return of data. Although each party would bear its attorney's fees, companies certified under the Privacy Shield would be required to pay an annual contribution to an independently managed fund established by the Department of Commerce to cover arbitral costs.

- **Key Exceptions:** The Privacy Shield principles include, among others, two key exceptions of which companies should be aware. First, there is an exception for due diligence performed in the context of M&A activities. The principles acknowledge that due diligence often involves the collection and processing of personal data, and that premature disclosure of the transaction to data subjects for data privacy purposes could impede the transaction or violate securities regulations. Accordingly, the Privacy Shield principles would permit investment bankers and attorneys engaged in due diligence to process information without the knowledge of the data subject to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances where application of the principles would prejudice the legitimate interests of the organization (including the need for confidentiality connected with possible M&A activity). Second, there is a journalistic exception, which states that where the rights of free press under the First Amendment to the U.S. Constitution intersect with privacy protection interests, the First Amendment governs the balancing of those interests with regard to the activities of U.S. individuals or organizations. This exception may be an indirect response to criticisms following the European Court of Justice's decision on the "right to be forgotten"[2] that the EU was prioritizing its fundamental right of privacy principles over the First Amendment.

Commitments of US Authorities

In the biggest departure from the Safe Harbor, as part of the Privacy Shield, certain U.S. authorities have written letters to the European Commission in which they make official representations and commitments regarding, as applicable, their administration, monitoring and enforcement of the Privacy Shield and related U.S. laws, and their collection and use of EU personal data. The official representations and commitments are made by the following U.S. authorities: (1) the Department of Commerce, (2) the Secretary of State, (3) the Federal Trade Commission, (4) the Department of Transportation, (5) the Office of the Director of National Intelligence, and (6) the Department of Justice (Criminal Division). The representations and commitments of each U.S. authority are summarized below:

Department of Commerce: Responsible for administering the Privacy Shield, including verifying that each self-certifying organization complies with its obligations. It will maintain a list of U.S. organizations that have self-certified and a list of organizations that have withdrawn or had their self-certification revoked for failure to comply. In addition, for those organizations that withdraw or fail to comply, the department will follow up to ensure that they are treating the personal data collected under the Privacy Shield appropriately and that they are not misrepresenting their participation in the Privacy Shield, and will refer such matters for enforcement if necessary. The department also is responsible for maintaining a Privacy Shield website directed to EU individuals, EU businesses and U.S. businesses that describes the rights of EU individuals and the recourse mechanisms available to them, and will provide details to EU businesses regarding U.S. businesses' self-certification. Finally, the department will designate a dedicated contact for European data protection authorities who will provide information about the Privacy Shield and receive complaints regarding noncompliance.

Secretary of State: Will establish a new mechanism to facilitate the processing of requests relating to national security access to EU personal data that is transmitted to the U.S. under the Privacy Shield. The mechanism will be administered by the Privacy Shield ombudsperson, who is independent of the U.S. intelligence community and reports direct to the secretary. The member states, either themselves or through a centralized EU body, will initially receive and verify any complaints from EU individuals related to U.S. national security access. The ombudsperson will be responsible for coordinating with other U.S. government authorities, including the Office of the Director of National Intelligence and the Department of Justice, to investigate any such complaints in order to confirm that any surveillance complies with all applicable laws or, in the event of any noncompliance, to remedy such noncompliance. Notably, the ombudsperson is not required to either confirm or deny whether the complaining individual has been the target of surveillance or confirm the specific remedy that was applied.

Federal Trade Commission: Commits to prioritize Privacy Shield referrals from member states and referrals from other organizations regarding noncompliance with the Privacy Shield. For member state referrals, the Federal Trade Commission (FTC) will create a standardized referral process and designate an FTC point of contact. It also will work closely with EU data protection authorities to provide enforcement assistance and will meet periodically with WP29 to discuss how to improve Privacy Shield enforcement cooperation. In addition, the FTC will conduct its own investigations and enforcement actions where warranted, including in cases where it or the Department of Commerce identifies an organization that may be misrepresenting its compliance with the Privacy Shield or may not be complying with an FTC order related to the Privacy Shield.

Department of Transportation: Responsible for ensuring the privacy of information provided by consumers to airline and ticket agents. Once a carrier or seller of air transportation self-certifies under the Privacy Shield, the department will use its Office of Aviation Enforcement and Proceedings to investigate complaints, enforce compliance with the Privacy Shield and

[2] *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, Case C-131/12, May 13, 2014. We discussed this case in our May 2014 edition of *Privacy & Cybersecurity Update*.

monitor compliance with any department orders related to the Privacy Shield.

Director of National Intelligence: Summarizes the information provided to the European Commission regarding the operations of the U.S. intelligence community with respect to signals intelligence collection. The director provides an overview of key provisions of (1) Presidential Policy Directive 28, issued on January 17, 2014, which imposes limitations on signals intelligence operations and is binding on the U.S. intelligence community, (2) Section 702 of the Foreign Intelligence Surveillance Act (FISA), which is focused on the collection of foreign intelligence from individually identified legitimate targets and subject to oversight by all three branches of government, including the FISA Court, which reviews the procedures used in foreign intelligence data collections to ensure they comply with applicable law, and (3) the USA FREEDOM Act, which modified the proceedings before the FISA Court to increase transparency and protect privacy, including by creating a standing panel of security-cleared lawyers versed in privacy, intelligence collection and other relevant areas. The director also emphasizes that there is great deal of transparency around U.S. intelligence activities, as well as a number of avenues of redress for EU citizens who have been the subject of unlawful electronic surveillance for national security purposes, including under FISA, the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act and the Right to Financial Privacy Act.

Department of Justice (Criminal Division): Provides an overview of the investigative tools used to obtain information from U.S. companies for criminal law enforcement or public interest purposes and limits on the use of those tools. These tools are used without regard to the nationality of the data subject and include grand jury, trial and administrative subpoenas, court orders for pen registers and trap-and-traces (which allow acquisition of real-time dialing, routing and signaling information about phone numbers or emails), court orders for surveillance pursuant to federal wiretap law and search warrants. The DOJ notes that there are limits imposed on the use of all these tools, whether through the Fourth Amendment to the U.S. Constitution, case law, the statutes that create or authorize use of the tool, or Department of Justice (DOJ) guidelines and policies.

Challenges Ahead

The Privacy Shield still faces significant obstacles on both the European and American fronts before becoming law. The framework must survive scrutiny at several stages of European bureaucratic approval and is subject to change throughout this process. In addition, upcoming U.S. political and judicial decisions may affect the approval process by shifting perceptions about U.S. commitment to the framework as negotiated.

For the Privacy Shield to become law, a qualified majority of the Article 31 Committee, composed of EU member state representatives, must issue a binding opinion approving the "adequacy decision" released by the European Commission on February 29, 2016, after which the EU College of Commissioners must formally adopt the decision. This process is expected to be completed in June 2016.

Even following such adoption, the Privacy Shield is likely to face court challenges by those who are skeptical that the arrangement provides little more assurance than the original Safe Harbor, including challenges by any data protection authorities that determine that the agreement does not meet local standards.

In the United States, Congress recently passed the Judicial Redress Act, which provides important avenues of redress for EU citizens by conditionally extending the protection of the Privacy Act of 1974, and applicable jurisdiction in U.S. courts, to EU citizens. However, the act limits that grant of jurisdiction to citizens of countries whose policies regarding the transfer of personal data for commercial purposes, and related activities, have been determined by the U.S. attorney general not to "materially impede the national security interests of the United States." Thus, although the act appears to accord with the spirit of the Privacy Shield and has been positively received by EU commissioners, some believe this condition conveys to European counterparties that U.S. national security interests will still prevail over EU citizens' rights, which may give rise to challenges to the draft adequacy decision during the review and adoption process outlined above.

Post-Adoption Reviews

Even if the adequacy decision is adopted in relatively short order, the effectiveness of the Privacy Shield as adopted will be continuously evaluated. Following adoption of the adequacy decision, the European Commission will check periodically to determine whether the adequacy of the level of protection afforded by the EU-U.S. Privacy Shield is still justified. The decision also will be subject to an annual joint review of all aspects of the Privacy Shield, which the commission will summarize in a report to the European Parliament and Council. In the event that the commission finds at any time that there are "clear indications that effective compliance with the Privacy Principles in the United States might no longer be ensured," which may include a failure of the U.S. government to cooperate with the commission's request for information, it will inform the Department of Commerce and request corrective measures within a specific time frame. If the corrective measures are not completed within the time frame, the commission may suspend, modify or repeal the adequacy decision.

Business in the Near Term

Companies that rely on the Safe Harbor today should be mindful that the Privacy Shield may not come into effect for some time, and perhaps not at all. While we expect that the WP29 will extend its grace period for keeping the Safe Harbor framework in place if review and approval of the Privacy Shield is delayed for a short period, if the process extends for a long period, the WP29 might have second thoughts. We will provide an update if the WP29 position changes. In the meantime, companies that rely on Safe Harbor should continue to abide by those standards, as the FTC has indicated that it intends to enforce this self-certification until the Privacy Shield is approved.

Return to Table of Conents

President Obama's 2017 Budget Allocates $19 Billion to Cybersecurity

President Obama's 2017 budget proposal includes $19 billion in cybersecurity spending, which represents a significant increase over the 2016 budget and is in keeping with the administration's emphasis on improving national cybersecurity.

President Barack Obama's new budget proposal includes a $19 billion investment in cybersecurity — roughly a 35 percent increase from the 2016 budget — through a Cybersecurity National Action Plan. The plan focuses on three major categories of cybersecurity strategy: (1) overhauling outdated technology the federal government relies on that is vulnerable to cyber-attacks, (2) investing in the cybersecurity workforce, and (3) improving the government's preparation for and response to cyberthreats.

Improving Existing Federal Information Technology

In the budget materials, the Obama administration emphasized the importance of retiring, replacing or upgrading antiquated government hardware and infrastructure on which many federal departments and agencies currently rely, and transitioning to more secure and efficient systems. The old systems are difficult and costly to secure and update, which makes them particularly vulnerable against cyberthreats. Such threats have become reality, as demonstrated by the recent Chinese theft of security records on 22 million Americans from the Office of Personnel Management. To accomplish this overhaul, the Obama administration has proposed creating a revolving Technology Modernization Fund at the General Services Administration, seeded with an initial capital injection of $3.1 billion. The fund would be self-sustaining by enabling agencies to make initial investments and to realize the return over time with efficiencies gained from the modernization efforts.

The fund also would help address the inefficiencies in securing, maintaining and updating different information technology platforms across different areas of the federal government. A new project review board would evaluate and select projects for funding, and would aim to replace multiple legacy systems with a smaller number of common platforms. One of the goals is to create common IT solutions across the federal government, such as enterprisewide email and cybersecurity tools and services.

Training, Recruiting and Retaining Cybersecurity Talent

There is a shortage of skilled cybersecurity experts and privacy professionals generally, and the federal government in particular faces difficulties recruiting and retaining such workers. In order to grow the cybersecurity workforce, the White House proposes spending $62 million on three primary initiatives in order to address workforce shortages and skill gaps:

- Expand the National Science Foundation's Scholarship for Service program by establishing a CyberCorps Reserve program to offer scholarships to Americans who wish to obtain a cybersecurity education and work for the federal government;
- Develop a foundational Cybersecurity Core Curriculum for academic institutions to consult and adopt, which would ensure that individuals studying cybersecurity obtain the requisite knowledge and skills to perform cybersecurity work for the federal government; and
- Expand the National Centers of Academic Excellence in Cybersecurity Program by providing grants to academic institutions to develop or expand cyber education programs in order to increase the number of participating academic institutions and students.

The budget also provides enhanced student loan forgiveness programs for cybersecurity experts who join the federal government workforce and funding for President Obama's Computer Science for All Initiative, which allots money to states to spend on computer science education for children from kindergarten through high school. Additionally, the Department of Homeland Security is allotted $37 million to expand standing teams of cybersecurity experts that provide readily available cybersecurity capabilities to departments and agencies within the federal government.

Reforming Management of and Response to Cyberthreats

The budget would create within the Office of Management and Budget a new role of federal chief information security officer, who would be charged with driving cybersecurity policy, planning and implementation across the federal government. It would

also establish a blue ribbon commission consisting of leaders in various technology and privacy fields that would provide cybersecurity awareness and protection recommendations for both the government and the private sector. The commission would support efforts to replace passwords with more secure multi-factor authentication and identity proofing, including for U.S. citizens to use on multiple online federal government services.

Return to Table of Conents

Professional Liability Insurer Owes Coverage to Genealogy Website

In Evanston Insurance Co. v. Gene by Gene Ltd., a federal district court in Texas found that a professional liability insurer owed coverage to a genetic genealogy website in connection with a DNA data privacy breach lawsuit.

Courts throughout the country — alongside insurers and policyholders — continue to grapple with questions of insurance coverage for cyber and privacy losses. Although some courts have determined that reliance on traditional insurance policies to cover cyber and privacy losses falls short, the U.S. District Court for the Southern District of Texas' recent decision in *Evanston Insurance Co. v. Gene by Gene Ltd.*[3] illustrates that at least some courts are still open to the possibility of coverage for such losses under traditional insurance policies.

Background

The insured in *Evanston*, Gene by Gene, Ltd., owns and operates a genetic genealogy website that gives its customers the opportunity to use DNA testing to learn more about their ancestry and connect with other customers whose DNA test results matched their own to varying degrees. In May 2014, Michael Cole commenced a putative class action against Gene by Gene alleging that it improperly published his DNA test results on its website without his consent, in violation of Alaska's Genetic Privacy Act.

When Gene by Gene sought coverage for the *Cole* litigation under two professional liability policies issued by Evanston Insurance Company (Evanston), Evanston denied coverage, citing the policies' "Electronic Data and Distribution of Material in Violation of Statutes" exclusion. Evanston subsequently filed suit against Gene by Gene seeking a declaration that it had no duty to defend or indemnify Gene by Gene for the *Cole* litigation. Gene by Gene counterclaimed, seeking, among other things, a declaration that Evanston had a duty to defend and indemnify Gene by Gene for the *Cole* litigation.

The Court's Decision

On its motion for summary judgment in the coverage litigation, Gene by Gene argued that Evanston had a duty to defend and indemnify under the policies' "Personal Injury and Advertising Injury Liability" coverage part. The court agreed, determining that the claim alleged in the *Cole* litigation fell within the policies' coverage for "personal injury," which the policies defined to include "oral or written publication of material that violates a person's right of privacy." The court reasoned that "[c]omparing the factual allegations within the four corners of the [*Cole* litigation] and the four corners of the Policies, the claim in [the *Cole* litigation] falls within the definition of Personal Injury because it includes the publication of material — the DNA analysis — that allegedly violates a person's right to privacy."

The court then turned to the applicability of the exclusion, concluding that it did not apply. The exclusion precluded coverage for claims arising from violations of (1) the Telephone Consumer Protection Act of 1991, amendments thereto and any similar or related federal or state laws, (2) the CAN-SPAM Act of 2003, amendments thereto and any similar or related federal or state laws, and (as relevant here) (3) "any other statute, law, rule, ordinance, or regulation that prohibits or limits the sending, transmitting, communication or distribution of information or other material."

Evanston urged the court to apply the exclusion, arguing that the claim in the *Cole* litigation fell squarely within Subsection (c) because it was brought pursuant to a statute, the Genetic Privacy Act, that prohibits the "transmitting, communication or distribution of information or other material," — to wit, the public disclosure of a person's genetic information absent informed consent. In addition to arguing that Evanston's reading of the exclusion would render illusory the policies' "Personal Injury and Advertising Injury Liability" coverage, Gene by Gene employed the *ejusdem generis* canon of construction to argue that because Subsections (a) and (b) of the exclusion concern statutes regulating the use of unsolicited forms of communication to customers, the scope of Subsection (c) also must be limited to laws regulating "forms of unsolicited communication to customers 'that intrude[] into one's seclusion,'" rather than the broader scope Evanston advocated.

Adopting Gene by Gene's *ejusdem generis* argument, the court held that the exclusion did not bar coverage for the *Cole* litigation because the Genetic Privacy Act upon which the *Cole* litigation claim was based "does not concern unsolicited communication to customers, but instead regulates the disclosure of a person's DNA analysis." Moreover, the factual allegations

[3] No. 14-cv-1842, 2016 WL 102294 (S.D. Tex. Jan. 6, 2016).

at issue "deal solely with Gene by Gene's alleged improper disclosure of DNA test results" and "do not address the type of unsolicited seclusion invasion contemplated by the Exclusion." Accordingly, the court granted Gene by Gene's motion for summary judgment and determined that Evanston had a duty to defend and indemnify Gene by Gene in the *Cole* litigation.

Practice Points

Although the court in *Evanston* narrowly construed the exclusion such that it did not bar coverage for Gene by Gene's data breach liability, courts are hardly settled on the availability of coverage for cyber and privacy losses under traditional policies. As further illustrated by *Evanston*, moreover, even if policyholders have good claims for coverage under traditional policies, insurers often take the position that traditional policies do not cover such losses. As such, risk management personnel would be well-advised to identify and evaluate their company's potential risk scenarios with respect to cyber and privacy loss and craft a comprehensive risk management plan that protects against these potential losses. If procuring cyber insurance to protect against such losses, risk managers should bear in mind that cyber insurance products vary widely throughout the marketplace and selecting coverage that is appropriately tailored for a company's needs will require careful consideration of the policy language and an appreciation of the cyber security and privacy risks that the company faces.

Return to Table of Conents

FDIC Releases 'A Framework for Cybersecurity'

The FDIC's Division of Risk Management Supervision releases guidance on how financial institutions' security programs should be designed to address cybersecurity risks.

In its Winter 2015 edition of *Supervisory Insights* published earlier this month, the Division of Risk Management Supervision of the Federal Deposit Insurance Corporation (FDIC) released "A Framework for Cybersecurity," in which the FDIC outlines the ways in which financial institutions' cybersecurity programs should be enhanced to address evolving cybersecurity risks in each of the four key areas of corporate governance, threat intelligence, security awareness training and patch-management programs. The framework emphasizes the importance of board and senior management involvement in understanding cyberthreats and promoting a cybersecurity culture across the organization.

Corporate Governance

The FDIC notes that cybersecurity is no longer simply the concern of IT employees but should be treated like any other risk management issue. The framework instructs the boards of financial institutions to institute a corporate culture that prioritizes cybersecurity on an enterprise level.

Threat Intelligence

The framework references the "Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement" issued in November 2014 by the Federal Financial Institutions Examination Council (FFIEC), which states that all financial institutions should have in place a system for gathering and sharing information about cybersecurity threats so that they can develop "actionable intelligence." As part of such a system, the FFIEC statement suggested that financial institutions participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC), which is a public-private partnership that provides analysis and mitigation strategies and practical training such as threat exercises. The framework also notes that the U.S. Computer Emergency Readiness Team (US-CERT) is a useful source of threat intelligence for financial institutions that provides threat alerts and educational materials.

Security Awareness Training

The FDIC emphasizes the importance of cybersecurity awareness training for employees, contractors and customers of financial institutions, noting that such programs should highlight the importance of protecting against cyberrisks across all business lines and functions and all levels of seniority. This does not mean that a "one size fits all" training program is appropriate; the FDIC advises financial institutions to make its training role-specific and to take into account the sensitivity of the data to which each person has access. The framework notes that the most frequent targets of cyberthreats are information security professionals, executives, comptrollers and cashiers. The training should be available not only to employees but to any other party that presents an access point to the bank's systems, including contractors and customers.

Patch-Management Programs

The FDIC states that lack of an effective patch-management program has contributed significantly to the increase in security incidents. The framework advises that an effective patch-management program is built on an accurate asset inventory that identifies the assets that require patch management, including software, routers and firewalls. The patch-management program should include (1) written policies and procedures to identify, prioritize, test and apply patches promptly, (2) information regarding known threats and vulnerabilities, (3) identification

of products that are nearing their end of life or are no longer supported, and strategies for mitigating vulnerabilities presented by the old products and migrating to supported products, (4) regular, standardized reporting to the board and senior management regarding patch management, and (5) independent audits and internal reviews to validate the effectiveness of the program.

Additional Resources

Finally, the FDIC notes that it continually examines its own procedures to identify areas of improvement and encourages financial institutions to adopt practices to protect against threats. The framework lists a number of resources provided by both the FDIC and other parties to assist financial institutions of various sizes in identifying, managing and mitigating cyberthreats.

Return to Table of Conents

California Data Breach Report

The California Department of Justice released a comprehensive analysis of data breaches reported to the state attorney general from 2012-15. The report includes specific recommendations companies should adopt to demonstrate reasonable security procedures and practices and mitigate the effects of any breach.

The California Department of Justice released a report summarizing and analyzing all data breaches affecting more than 500 Californians that have occurred since 2012, when such data breaches were first required to be reported to the attorney general's office. The report also provides recommended practice that companies should adopt to demonstrate reasonable security practice and procedures. California has long been a leader in privacy law and cybersecurity matters, so while the report is specific to California, the recommendations may be adopted by other states, particularly since the report encourages state policy makers to work together to harmonize state data breach laws. Companies using Californians' personal data should follow the recommendations, and it would be prudent for all companies to do so, regardless of their nexus with California, since the California recommendations may be viewed as a "best practice."

Breach Statistics

From 2012 through 2015, there were 657 such data breaches affecting over 49 million records of Californians. There were three main types of breaches: (1) malware and hacking, which were used in 54 percent of the breaches and which accounted for the vast majority (90 percent) of the records breached, (2) physical breaches resulting from the theft or loss of devices, which accounted for more than half of all health care sector breaches, and (3) breaches caused by errors such as misdelivery of email, which accounted for half of all government breaches. Notably, the data breaches most often affected sensitive personal information, such as Social Security numbers (24 million records) and medical records (18 million records), rather than payment card information, which the report notes is becoming a less attractive target for thieves thanks to more secure methods adopted by the payment card industry. While the breaches touched a wide variety of public and private sectors, the retail sector accounted for the greatest number of breaches (25 percent), with the financial sector (18 percent) and the health care sector (16 percent) close behind. Small businesses across sectors accounted for 15 percent of all breaches, perhaps reflecting smaller cybersecurity budgets and fewer and less sophisticated cybersecurity practices, in addition to a growing awareness of the reporting requirement among small businesses.

Recommendations

California's information security statute requires companies to use "reasonable security procedures and practices ... to protect personal information from unauthorized access, destruction, use, modification, or disclosure." The recommendations in the report, summarized below, serve as a guide to companies as to what constitutes the reasonable security procedures and practices required under the law; accordingly, companies should ensure that they are complying with these recommendations or risk running afoul of California's statute. The report recommendations are as follows:

- At a minimum, companies must meet the level of information security described in the 20 controls in the Center for Internet Security's Critical Security Controls. Failure to implement all 20 controls that apply to a company constitutes such company's failure to comply with California's statute. The controls address areas such as asset inventories, continuous vulnerability assessments, access control and incident response.
- Companies should use multifactor authentication on consumer-facing online accounts that contain sensitive personal information. The report notes the specific importance of protecting individuals' email accounts and states that if consumer email providers are currently not using multifactor authentication, they should implement it promptly.
- Companies should use strong encryption to protect personal information on laptops and other portable devices, and should consider doing so for desktops. The report notes that this is particularly true for the health care sector.

- In the event of a breach affecting Social Security numbers or driver's license numbers, companies should include a prominent message in their breach notifications encouraging affected individuals to place fraud alerts on their credit files. The report notes that fraud alerts can be implemented by individuals with a single phone call, or online, and are free; thus, they are an efficient means for individuals to mitigate the effects of a breach, and companies should be sure to make individuals aware of that option.
- State policymakers should collaborate to harmonize state data breach laws on some key points. The report notes that harmonization would maintain consumer protections while reducing the compliance burden for companies. The report expresses a strong preference for state law harmonization over a pre-emptive federal data breach law, since state laws can be changed more rapidly in response to new information.

Takeaways

As noted above, any company that collects personal information of Californians should ensure that it is complying with the recommendations of the report applicable to it, most notably the 20 controls included in the Critical Security Controls. Companies collecting data of residents of other states should keep abreast of changes in state data privacy laws to see if other states adopt California's recommendations.

Return to Table of Conents

DHS Publishes CISA Guidance

DHS released interim guidelines and procedures regarding the sharing of cyberthreat information and defensive measures under CISA. The guidelines provide instructions on the types of information that should and can be shared and the mechanisms for sharing such information. The final guidelines will be issued in June 2016.

The Department of Homeland Security (DHS) released four sets of interim guidelines and procedures related to sharing cyberthreat information and defensive measures among federal government and nonfederal entities under the Cybersecurity Information Sharing Act of 2015 (CISA) on February 16, 2016.

CISA, which was passed on December 18, 2015, authorizes and establishes a system for the voluntary sharing of cyberthreat indicators and defensive measures among the federal government, private entities, and state and local governments. As an incentive for participation in this system, CISA provides a variety of liability protections and exemptions for nonfederal entities that share or receive information in accordance with the law. DHS was given 90 days to develop interim guidelines to facilitate and promote the system envisioned under the Act. These interim guidelines are summarized below.

- Guidance to Assist Nonfederal Entities to Share Cyberthreat Indicators and Defensive Measures With Federal Entities. This guidance is designed to "assist non-federal entities who elect to share cyberthreat indicators with the Federal Government to do so in accordance with [CISA]" by describing the types of information that should and should not be shared, with a particular eye toward privacy concerns. As a preliminary matter, "the only information that can be shared under [CISA] is information that is directly related to and necessary to identify or describe a cybersecurity threat," meaning that such information is "necessary to assist others [to] detect, prevent, or mitigate the cybersecurity threat." Before sharing any cyberthreat information, a company must remove any and all information that it "knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat." If protected information must be provided to describe the threat adequately (*e.g.*, in the case of a social engineering attack such as phishing), companies should present such information in anonymized form to the extent possible. The document goes on to describe both (1) the types of information that are likely to be directly related to a cyberthreat or defense, such as software vulnerabilities, web server logs, a particular firewall rule or software that can detect a pattern of malicious activity in web traffic, and (2) examples of personal information that is unlikely to be directly related to a cyberthreat and therefore should not be shared, particularly if it is the subject of otherwise applicable privacy law, including protected health information, financial information and identifying information about children under the age of 13.

  In addition to outlining best practices related to the types of information that should and should not be shared, the guidance notes that companies must use one of four avenues to report cyberthreat information and defensive measures in order to benefit from CISA's liability protections: (1) a web form established by DHS specifically for such reports and available on a DHS National Cybersecurity and Communications Integration Center website (including www.us-cert.gov), (2) email to ncciccustomerservice@hq.dhs.gov, (3) DHS' Automated Indicator Sharing (AIS) initiative, which utilizes standardized fields and automated exchange technology to communicate with DHS servers in real time, or (4) Information Sharing and Analysis Centers or Information Sharing and Analysis Organizations, which will share the information with the government on the companies' behalf. The guidance clarifies that, in addition to "no cause of action" liability protection,

companies that share information through these avenues will be protected under various exemptions from antitrust laws and state and federal disclosure laws, as well as under specific confidentiality protections under the act. Information shared pursuant to CISA, other than unlawful activity, will not be used against companies in regulatory enforcement actions, but nor does it fulfill any regulatory reporting requirements. Finally, sharing information under CISA does not waive privilege. Companies may share cyberthreat and defense information with the government through other means, but they will not receive CISA's liability protection, only the other protections enumerated above.

- Sharing of Cyberthreat Indicators and Defensive Measures by the Federal Government. This document outlines procedures through which federal entities named under the act may share information with nonfederal entities, including private entities, state and local governments, and even the public, where appropriate. Although CISA generally encourages federal entities to share cyberthreat indicators and defensive measures as broadly and as quickly as possible, this document provides guidance to assist federal entities in determining when — and to whom — sharing information is appropriate based on the sensitivity and classified status of the information. In addition to timely sharing of threat knowledge, including sharing targeted information with affected entities to prevent or mitigate adverse effects of cyberthreats, the guidance contemplates periodic outreach and publication of cybersecurity best practices aimed at accessibility and implementation challenges faced by small business concerns.
- Interim Procedures Related to the Receipt of Cyberthreat Indicators and Defensive Measures by the Federal Government. These procedures provide federal entities instructions and statutory interpretation related to receiving, handling and disseminating cyberthreat information under CISA. The document provides more detail on the electronic information-sharing mechanisms enumerated in the guidance for nonfederal entities, focusing in particular on the capabilities of the AIS system. Through the AIS system, federal entities will remove unnecessary personally identifiable information from cyberthreat indicators received from nonfederal entities using a combination of automated technical analyses and elements of human review, will anonymize the identity of the entity that submitted the information unless that entity has otherwise consented to sharing its identity, and will disseminate the cyberthreat information, as appropriate, to other federal departments and agencies and nonfederal entities participating in the program.
- Privacy and Civil Liberties Interim Guidelines. As a result of heated debate over privacy and civil liberties concerns, CISA requires that the U.S. attorney general and secretary of Homeland Security develop "interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyberthreat indicators by a Federal entity obtained in connection with activities authorized" under the act. In order to limit any negative effects of the act on privacy and civil liberties, including by unauthorized distribution or receipt of personal information, federal entities are instructed to follow certain procedures under these guidelines. These procedures include notifying any U.S. person whose personal information has been shared in violation of CISA and adhering to certain CISA-specific implementations of the Fair Information Practice Principles (FIPPs) set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace. The FIPPs include data safeguarding measures, dissemination restrictions and audit procedures. The privacy guidelines also contemplate sanctions for improper use of information by federal entities.

Next Steps

DHS will issue final guidance on these matters by June 2016 and welcomes comments and feedback on the interim guidance from privacy advocates and private sector entities. In the meantime, assuming the final guidance will be substantially the same as the interim guidance, companies that wish to take part in information sharing under CISA should take steps to ensure that the procedures outlined by the guidance are incorporated into their own cybersecurity procedures.

Return to Table of Conents

(Attorney contacts appear on the next page.)

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James R. Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Ivan A. Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David E. Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jennifer L. Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Helena J. Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Gregoire Bertrou
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com