Skadden

Privacy & Cybersecurity Update

EU-US Privacy Shield Goes Into Effect — What Companies Should Be Doing Today

The European Union formally has approved the Privacy Shield, which replaces the Safe Harbor as a means to allow companies to transfer personal data from the European Union and the three additional European Economic Area member states (Norway, Liechtenstein and Iceland) to the United States. Although still subject to criticism and possible legal challenges, companies should consider whether to self-certify to avail themselves of the protections it offers. Companies that are complying with the current Safe Harbor framework will need to take additional steps to become Privacy Shield-compliant.

On July 12, 2016, the European Commission formally adopted the EU-U.S. Privacy Shield, a privacy self-certification framework that will enable companies to transfer personal data from the European Union and the three European Economic Area member states (Norway, Liechtenstein and Iceland) to the U.S., which does not, in the EU's view, have "adequate" data protection laws in place. The Department of Commerce began accepting self-certifications from companies on August 1, 2016. Despite its adoption, the Privacy Shield has been criticized sharply by a number of influential sources, therefore a risk remains that, like the Safe Harbor before it, the Privacy Shield will be challenged and invalidated by the Court of Justice of the European Union (the EU Court). Companies that previously relied on the Safe Harbor should understand that the Privacy Shield is more than "Safe Harbor plus" and that it may require companies to make significant changes to their operations.

Background

Current EU law forbids the transfer of personal data from EU countries to countries that do not have "adequate" data protection laws in place. Because the EU has concluded that U.S. privacy law does not meet the EU standard — and therefore companies would otherwise be unable to transfer personal data to the U.S. — the EU and the U.S. agreed on a "Safe Harbor" arrangement in July 2000 whereby companies could self-certify that they complied with certain privacy principles and then transfer personal data to the U.S. In October 2015, the EU Court invalidated the Safe Harbor framework based on the

court's finding that it did not adequately protect the interests of EU data subjects.[1]

The Privacy Shield replaces the Safe Harbor framework. Announced in February 2016, the Privacy Shield, like its predecessor, is principally a self-certification system under which companies commit to abide by certain data privacy principles. However, these principles are more expansive than those in the Safe Harbor, and also include new requirements to implement dispute mechanisms through which consumers may lodge complaints. Finally — though of less relevance to most entities — the Privacy Shield includes commitments from the U.S. government relating to the collection and use of information by the government (including by the intelligence community), and the appointment of an ombudsman to oversee the government's compliance with the Privacy Shield's requirements.

Overview of How the Privacy Shield Differs From the Safe Harbor

While the Privacy Shield is in many ways the same as the Safe Harbor, there are some notable differences.

- **More Robust Commitments.** The Privacy Shield imposes enhanced commitments and robust obligations as to how companies process personal data and protect EU data subjects' rights, including detailed notice obligations, data retention limitations, stricter purpose limitation requirements, tightened conditions for onward transfers, increased liability in certain contexts, and enhanced requirements for security and data protection.
- **Tougher Enforcement.** The Department of Commerce will monitor compliance with the Privacy Shield, which is subject to FTC enforcement. Recourse for noncompliance may involve sanctions or loss of eligibility to use the Privacy Shield.
- **Increased Protection of European Citizens With Opportunities for Redress.** Unlike the Safe Harbor, which did not provide for redress opportunities, individuals will be able to complain (1) directly to the companies, which have 45 days to resolve the complaint or (2) directly to EU data protection authorities (DPAs), which could refer unresolved complaints to the FTC. As noted below in greater detail, individuals are offered a free alternative dispute resolution mechanism if the FTC does not pursue an individual's case.
- **Explicit Government Safeguards and Transparency Obligations.** The U.S. justice and intelligence communities have given assurances that the collection of personal data of European citizens will be subject to clear limitations, protections and increased monitoring. Mass surveillance of personal data is not permitted under the Privacy Shield and there will be an annual joint review by the European Commission and the Department of Commerce to ensure compliance. National intelligence experts from the U.S. and European DPAs will be invited to participate in this review.

Privacy Shield Principles

Like the Safe Harbor, the Privacy Shield requires adherence to seven broad data privacy principles. The functional and administrative obligations underlying most of these principles, though set out in more detail than under the Safe Harbor, do not require companies who had relied on the Safe Harbor to make significant changes to their data transfers as conducted under the former arrangement. However, companies now have enhanced obligations related to accountability, enforcement and recourse. Key obligations for companies are highlighted below:

- **Notice.** A company participating in the Privacy Shield is required to notify individuals in clear and conspicuous language about a number of aspects of the company's privacy practices, including:
  - the types of personal data collected;
  - how such data is collected and used;
  - the company's commitment to abide by the principles of the Privacy Shield;
  - the identity of third parties to which it discloses such information and why;
  - the rights of individuals to access their personal data;
  - the means the company offers to individuals to limit the use of their data;
  - how to contact the organization with inquiries or complaints, including the relevant counterpart in the EU who can respond to such inquiries or complaints;
  - the independent dispute resolution body designated to address complaints and provide recourse free of charge (as discussed in further detail below);
  - the possibility under certain conditions for the individual to invoke binding arbitration;
  - the investigatory and enforcement powers to which the company is subject;
  - the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement needs; and

[1] For a discussion of the case invalidating the Safe Harbor, see our October 7, 2015, mailing. As the EU court's ruling did not apply to Switzerland, the Safe Harbor remains in effect for data transfers from Switzerland to the U.S.

- an acknowledgement that the company will be liable if it improperly transfers personal information to third parties.

This notice must be provided at the time the individual is first asked to provide personal information or as soon as practicable thereafter and must be given before the information is disclosed to a third party.

- **Choice.** A company participating in the Privacy Shield is 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 are required to provide a variety of assurances that any third parties to which they transfer European personal data will provide adequate protection as well, including entering into contracts with the third parties to which they provide the information. The specific requirements differ depending on whether the third party is a "data controller" or an agent of the transferor. A data controller is a party that determines the purposes for which, and the manner in which, personal data are to be processed. An agent is a party that processes personal data on behalf of a data controller.[2] It is possible for there to be more than one data controller in connection with any particular processing of personal data, if more than one party has the right to determine how or why data is processed.
  - **Third Party is a Data Controller.** Where the third party is a data controller, the company must provide individuals advance notice and the choice to opt out of the transfer. In addition, the company must enter into a contract with such third party that (1) limits data processing to purposes consistent with the data subject's consent and (2) requires the third party to afford the transferred data the same level of protection as required under the Privacy Shield.
  - **Third Party is an Agent**. Where the third party is an agent of the data controller, companies are required to (1) transfer data only for limited and specified purposes; (2) ascertain that the agent is obligated to provide at least the same level of privacy protection as required by the Privacy Shield; (3) 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; and (4) provide a summary or representative copy of the relevant privacy provisions of its contract with the agent to the Department of Commerce upon request.
- **Security.** Companies participating in the Privacy Shield are required to take "reasonable and appropriate measures" to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in handling personal data.
- **Data Integrity and Purpose Limitation.** Companies must 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. This imposes an affirmative duty on the organization to take reasonable steps in ensuring the personal data is reliable for its intended use, accurate, complete and current. This duty is imposed for as long as the organization retains such information.
- **Access.** Companies must give individuals access to the information held by the company about them and the ability to correct, amend or delete any inaccurate information. However, a company may decline to provide this access where the burden or expense of providing it would be disproportionate to the risks to the individual's privacy in the instance in question, or where the rights of persons other than the requesting individual would be violated.
- **Recourse, Enforcement and Liability.** This principle encompasses a number of subjects, including procedures for addressing disputes and data protection inquiries, liability for improper onward transfers, verification of a company's compliance and publicity for noncompliance.
  - **Consumer Complaints.** Consumers are encouraged first to raise any complaints with a company directly, and the company is required to respond within 45 days. In addition, since the Privacy Shield guarantees free independent dispute resolution processes to EU citizens, companies are required to select and provide an "independent recourse mechanism" to investigate unresolved complaints at no cost to individuals. This mechanism can take the form of a panel of data protection authorities established at the EU level, an EU-based alternative dispute resolution provider or a U.S.-based alternative dispute resolution provider; however, companies that transfer HR data for employment purposes under the Privacy Shield are obligated to select the DPA approach. Organizations such as JAMS and the Direct Marketing Association are offering Privacy Shield dispute resolution programs in the United States.

    Companies that elect (or are required) to rely on the panel of DPAs to fulfill the recourse requirement must declare this commitment in their self-certification. Companies are then required to cooperate in the investigation of complaints and

[2] The role of the agent is essentially equivalent to that of a "data processor" under EU privacy laws.

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. Damages can be awarded where applicable law or private-sector initiatives so provide.

Companies must respond promptly to inquiries, requests for information and complaints regarding compliance with the Privacy Shield. There are also obligations to remedy problems arising out of failures to comply, whereby dispute resolution bodies are encouraged to award sanctions that are "sufficiently rigorous to ensure compliance."

- **Arbitration for Unresolved Disputes.** Where both the complaint and independent recourse processes are unable to resolve a claim (though seemingly unlikely in the case of a DPA procedure), the Privacy Shield offers 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 are required to pay an annual contribution to an independently managed fund established by the Department of Commerce to the costs of the arbitration service. Individuals invoke binding arbitration by delivering notice in accordance with the Privacy Shield requirements.
- **Liability for Onward Transfers.** The organization is liable for the processing of personal information it receives under the Privacy Shield and then transfers to a third party acting as an agent on its behalf. The Privacy Shield organization remains liable if the agent then misuses the information in a manner inconsistent with the Privacy Shield, unless the organization proves it is not responsible for the event that gives rise to the damage.
- **Verification.** Companies also must provide follow-up procedures for verifying that representations the organizations make about their privacy policies are accurate and implemented as the organization claims, specifically with regard to previous cases of noncompliance. This verification can either be through a self-assessment (with proper recordkeeping) or a third-party program.
- **Publicity for Noncompliance.** When an organization becomes subject to an FTC or court order based on non-compliance with the Privacy Shield, the organization is required to make public any relevant sections of the compliance or assessment report submitted to the FTC, as long as this is not at odds with confidentiality requirements.

- **Key Exceptions.** The Privacy Shield principles include, among others, two key exceptions of which companies should be aware. First, there is an exception for both due diligence performed in the context of M&A activities and the activities of auditors and investment bankers in conducting audits. The principles acknowledge that both audits and due diligence often involve the collection and processing of personal data, and that, specifically with M&A transactions, 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,"[3] that the EU was prioritizing its fundamental right of privacy principles over the First Amendment.

Privacy Shield Self-Certification

Process

The Department of Commerce began accepting self-certification applications for the Privacy Shield program on August 1, 2016. The department has relaunched its Privacy Shield website to provide a means for more information and tools for self-certification applicants.[4]

Application Requirements

Privacy Shield applicants must meet a number of requirements in order to be eligible for the program, including:

- **Jurisdiction.** Companies must be subject to Federal Trade Commission or Department of Transportation jurisdiction.
- **Privacy Policy.** Companies must develop and publish a Privacy Shield-compliant privacy policy, which may be published on

[3] *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 *Privacy & Cybersecurity Update*.

[4] The Department of Commerce's Privacy Shield website is located here.

an internal website in the case of a privacy policy related to employee human resources information.

- **Independent Recourse Mechanism.** Companies must identify the organization's independent recourse mechanism, which will be tasked with investigating unresolved complaints at no cost to the data subject. This mechanism must be in place before self-certification, including (if the mechanism is managed by a third party) registering with the organization that provides the mechanism.
- **Verification Mechanism.** Companies must have in place the procedures they will use to verify compliance with the Privacy Shield's requirements.
- **Privacy Contact.** Companies must provide a contact for handling questions, complaints, access requests and other issues relating to the Privacy Shield.

As part of the application process the applicant will need to provide information related to the subjects above, as well as information about the data transfers and names of any affiliates it seeks to include in the self-certification.

Review by Department of Commerce; Effective Date of Privacy Shield Certification; Recertification

Once the Department of Commerce receives the application, it will take an unspecified amount of time to review it, then verify that the company has met the applicable requirements (including the contents of its privacy policy) and respond to the applicant to either ask for additional information or clarifications, or to approve the self-certification. Once the department has approved the self-certification, it will include the company on a public list of Privacy Shield companies and only then will the company be able to lawfully transfer data from the EU to the U.S. under its certification.

Once on the Privacy Shield list, the company must recertify its compliance every year, a process that will include conducting a verification process to confirm that the company complies with the Privacy Shield. This recertification process continues for as long as the company holds information that was collected while the company was on the Privacy Shield list, even if the company leaves the Privacy Shield program.

Nine-Month Grace Period for Amending Third-Party Contracts

The Privacy Shield allows early applicants a nine-month grace period with respect to the principle of accountability for onward transfers. As discussed above, this principle mandates that companies that transfer information to the United States and then seek to transfer it to third parties require those third parties to comply with the same Privacy Shield principles as the companies themselves. In order to comply with this principle, companies likely will have to amend their contracts with third parties to include appropriate language. The grace period allows companies nine months to make these changes.

This grace period is only available for those applicants that apply within the first 60 days after the Privacy Shield became effective. As the Privacy Shield technically became effective on July 12, 2016, the deadline will be September 10, 2016, though there is some possibility of an extension based on the delay between the date the Privacy Shield became effective and the date the Department of Commerce begins accepting applications.

The grace period is only for amending third-party contracts; it is not a waiver of the accountability for future transfers altogether. During the grace period, companies still must apply the notice and choice principles so that data subjects have input on whether their information is shared with third parties, and also must ensure that third-party agents that receive personal information provide the same level of protection as is required under the Privacy Shield principles.

What Companies Should Be Doing Today

Decide Whether to Self-Certify

Any company that seeks to transfer personal data out of the European Union should consider whether to self-certify for the Privacy Shield. Few companies should still, be operating without proper measures in place to permit transfers out of the EU — through either the EU's model contracts, EU-approved binding corporate rules or express data subject consents. For those that have put these alternate mechanisms in place, the Privacy Shield can provide an alternative option for lawful data transfers. For companies that have not put alternate mechanisms in place, they should put measures in place as soon as possible, and the Privacy Shield may be an attractive option.

Companies considering joining the program should understand the long-term obligations they take on and be certain they can meet those obligations. Self-certification with the Privacy Shield creates a legal obligation to comply with its requirements, one that remains in place for so long as a company continues to process data that was collected under the program's regime, even if the company has otherwise withdrawn from the program. The Privacy Shield includes requirements that are above and beyond the Safe Harbor, so companies that were Safe Harbor-compliant should not assume that they are also Privacy Shield-compliant.

There is legitimate risk that the Privacy Shield will be subject to legal challenge, though EU and U.S. negotiators insist the program meets EU legal requirements. However, investing in compliance is not likely to be wasted as, even if the Privacy Shield is invalidated, it is unlikely that a replacement regime will

require *less* than the Privacy Shield. Instead, a replacement likely would seek to add to the Privacy Shield to correct perceived deficiencies, just as the Privacy Shield built on the principles established in the original Safe Harbor. Companies that are already Privacy Shield-compliant likely will have to make fewer changes to their privacy practices in order to meet the requirements of a potential successor program.

Finally, companies should be aware that self-certification to the Privacy Shield exposes U.S. companies to greater enforcement risk by exposing them to claims by EU data subjects, EU data protection authorities, and U.S. regulators responsible for overseeing and enforcing the program. In particular, EU data protection authorities recently have been more aggressive in taking action to protect EU data subjects.

Review and Reform Privacy Practices

Companies that decide to seek self-certification should closely examine their existing data practices to see whether they meet the Privacy Shield's requirements — in particular its seven core principles. Once they have reviewed their privacy practices, companies will need to update their privacy policies, for both employee data and third-party data, to conform to Privacy Shield standards. The Department of Commerce will review these policies as part of the application process to see whether they meet the requirements.

Establish Dispute and Verification Mechanisms

Beyond documenting what their dispute and verification mechanisms will be, companies should implement them before submitting their self-certifications to the Department of Commerce. The Department of Commerce requires these to be in place before a company seeks to self-certify.

Legal Challenges Likely

Soon after negotiators released the Privacy Shield's details, the program came under criticism from some influential sources, including the EU Data Protection Commissioner (an independent supervisory authority responsible for protecting personal information and promoting good privacy practices), the Article 29 Working Party (a data protection advisory body whose membership comprises representatives from the DPA of each EU member state) and the individual plaintiff who brought the original case invalidating the Safe Harbor. Criticisms include continued concern over the ability of the U.S. intelligence community's ability to review personal information on a broad scale, as well as over the myriad of enforcement mechanisms (particularly those involving the government) that might confuse data subjects.

The original Privacy Shield has been amended to address some of these concerns, and on July 26, 2016, the Article 29 Working Party announced that DPAs would not challenge the Privacy Shield on their own initiative. Nevertheless, legal challenges akin to those lodged against the Safe Harbor seem likely. Whether these challenges will lead the EU Court to invalidate the Privacy Shield remains to be seen. Some companies may decide to postpone Privacy Shield self-certification until the program has survived some of these challenges and instead rely on the EU's "model contracts," binding corporate rules or data subject consents to continue transferring personal data outside the EU, even though the model contracts are currently subject to challenge.[5]

Conclusion

The EU's decision to adopt the Privacy Shield signals a new era in data protection, as it relates to transfers from the EU to the U.S. As challenges to the Privacy Shield mount, and as EU and U.S. regulators adapt to this new regime, we expect this to be a volatile area of the law and of data practice for years to come.

Return to Table of Contents

FTC Revives Case Against LabMD, Finding Consumer Harm

The FTC has overruled an administrative law judge's decision dismissing the commission's case against LabMD, based on its view that the judge used too high of a standard for reviewing whether the company's actions were likely to cause substantial injury to consumers.

The commissioners of the Federal Trade Commission have overturned an administrative law judge's decision dismissing its case against medical testing company LabMD, ruling that the judge had applied the wrong legal standard. The commissioners rejected the judge's decision that the commission had to show actual or probable harm to consumers in order to bring a claim that the company had engaged in unfair practices under the FTC Act. This decision — if it stands — could further strengthen the FTC's efforts to pursue companies for poor cybersecurity practices under Section 5 of the FTC Act.

[5] The model contracts are the subject of a challenge before Irish courts, as we noted in our May 2016 *Privacy & Cybersecurity Update*.

Background

As we have previously reported,[6] the FTC originally brought an administrative proceeding against LabMD based on two separate data breaches affecting information belonging to approximately 10,000 consumers. The first breach was uncovered in 2008 when a file with billing information for more than 9,000 customers was found on LimeWire, a P2P sharing site that had been installed on a billing computer. The second breach was uncovered in 2012 when law enforcement officers in Sacramento, California, found documents containing information for approximately 500 LabMD customers in the possession of identity thieves. According to the commission, the data breach resulted from poor security practices at LabMD, including failures to (1) appropriately protect its computer networks or use adequate risk assessment tools, (2) provide data security training to employees and (3) adequately restrict and monitor employees' use of its network. LabMD did not notify consumers of the breach.

The commission claimed that these poor security practices and ultimate data breach violated Section 5 of the FTC Act's prohibition on unfair business practices affecting commerce. Under the FTC Act, a practice may be deemed unfair if (1) it "causes or is likely to cause substantial injury to consumers," (2) the injury "is not reasonably avoidable by consumers themselves," and (3) the injury is "not outweighed by countervailing benefits to consumers or competition."[7]

LabMD, unlike most companies against which the FTC brought these types of claims, fought back. After losing a series of administrative law and federal court motions seeking to dismiss the complaint, LabMD received a victory in the November 2015 FTC administrative law judge's decision that, absent a showing of actual or probable substantial consumer harm, the FTC could not meet the first element of the unfairness test under the FTC Act.[8] The FTC appealed the administrative law judge's decision to the heads of the commission.

FTC Decision Overruling Administrative Law Judge

Likelihood of Substantial Injury

In their July 29, 2016 order,[9] the FTC commissioners overruled the administrative law judge's decision, concluding that the legal standard for unfairness includes claims where the impact of an injury is large even if the likelihood is low. In the LabMD case, where the disclosure included names, dates of birth, social security numbers, insurance company names and policy numbers as well as codes for the types of laboratory tests performed (such as HIV, herpes, prostate cancer and testosterone levels), the commissioners held that the potential harms that could result from such disclosure were substantial. These potential harms include monetary losses due to financial fraud, time and resources spent resolving fraud-related disputes, and the possibility of misdiagnoses or mistreatment of illness due to medical identity theft. The commissioners also cited the less tangible harms that result from a breach of privacy generally, such as embarrassment and reputational harm.

The commissioners also rejected the administrative law judge's decision that the phrase "likely to cause substantial injury" in the FTC Act means that the injury must be "probable." Instead, the commissioners ruled, the FTC Act requires an assessment of risk rather than probability. In other words, according to the commissioners, a small likelihood of significant harm is enough to meet the standard. In the LabMD case, sensitive information had been made available through a popular file-sharing network, meaning that while it was unlikely any particular user would choose to download the file, two to five million users were on the network at any given time — including identity thieves that routinely looked for such information — so there was a risk that someone could download it and have access to the information.

Consumers Could Not Reasonably Avoid the Injuries

Although primarily focused on the first element of the unfairness test, the commissioners also found that the other two elements had been satisfied.

The commissioners noted that most consumers were never notified that their information was being sent to LabMD, and that those who did learn of it after the fact received no information on LabMD's security practices. The commission rejected LabMD's argument that consumers could have avoided harm after the breach occurred on a number of grounds. First, the commissioners ruled that the unfairness test addresses the ability to avoid the harm *before it occurs*, not after the fact (and, the commissioners noted, even if the ability to mitigate the harm after the fact were relevant to the unfairness test, the fact that LabMD never notified the data subjects made it all but impossible to do so). Second, even if consumers had been notified, they would find it difficult or impossible to fully avoid the harm because they would not know who had accessed their information or who would do so in the future. Third, consumers cannot avoid or reverse some of the non-economic harms from a privacy breach, such as medical errors or reputational harm.

[6] See, *e.g.*, our December 2013 *Privacy & Cybersecurity Update*.

[7] 15 U.S.C. §45(n).

[8] For a discussion of the November decision, see our November 2015 *Privacy & Cybersecurity Update*.

[9] The FTC's order is available online here.

Not Outweighed by Countervailing Benefits

Finally, the commissioners rejected any argument that the cost savings to LabMD of not putting security precautions in place — such as monitoring tools, training and vulnerability detection — did not outweigh the injuries that consumers could suffer as a result of a security breach.

Key Takeaways

The FTC commissioners' decision will strengthen the commission's arguments against companies that experience data breaches, especially those where the risk of harm is low but the data is particularly sensitive. We expect that this decision will lead the FTC to increase its enforcement actions in the cybersecurity area, particularly where large amounts of data, or even relatively small amounts of sensitive data, are involved.

Return to Table of Contents

White House Releases New Directive on Responding to Cyber Incidents

The White House has released a new Presidential Policy Directive on responding to cyber incidents affecting the government or the private sector. The directive identifies key principles the government will observe in responding to incidents, as well as the government agencies responsible for leading the government's various efforts.

On July 26, 2016, the White House released Presidential Policy Directive/PPD-41, which describes how the federal government will respond to a cyber incident affecting the government or the private sector, including how it will coordinate and marshal its resources to respond to an incident. The directive also sets forth the key principles and lines of effort the government will follow, including the degree of deference afforded to private sector entities when disclosing an incident to the public.

Key Principles

PPD-41 identifies a set of key principles the government will follow when responding to a cyber incident, including an effort to maintain confidentiality on private sector incidents.

- **Shared Responsibility.** Individuals, the private sector and government agencies have a shared interest and complementary roles in protecting the United States from malicious cyber activity and managing cyber incidents.
- **Risk-Based Response.** The government will determine its response based on the risks posed to an entity, national security, foreign relations, the broader economy, public confidence, civil liberties or public health and safety.
- **Respecting Affected Entities.** Of particular note to the private sector, PPD-41 indicates that the government will safeguard details of the incident and sensitive private sector information, and generally will defer to the affected entities in notifying other private entities or the public. However, if a significant federal interest is served by making a public disclosure, the government reserves the right to do so, though it will coordinate the approach with the affected entities to the extent possible.
- **Unity of Government Effort.** Government entities will have different roles, responsibilities, authorities and capabilities in responding to an incident, so they will share information and coordinate their response. The federal government also will coordinate with state and local governments as needed and may coordinate with international partners as well.
- **Enabling Restoration and Recovery.** The government's efforts will be conducted in a manner to facilitate recovery of an entity that has experienced a cyber incident, balancing investigative and national security needs, public health and safety, and the need to resume normal operations quickly.

Concurrent Lines of Effort

PPD-41 also describes three concurrent lines of effort in responding to a cyber incident (and a fourth where the government itself experiences the incident) and identifies the lead federal agency on each front. This effort to identify the different actions to be taken, and to clearly identify the government body responsible for each, should help businesses understand which agency or agencies they should contact for government assistance with respect to cyber incidents.

- **Threat Response.** The Department of Justice, acting through the FBI and the National Cyber Investigative Joint Task Force, will lead the government's law enforcement and national security investigative activity.
- **Asset Response.** The Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, will coordinate the effort to provide technical assistance to the affected entities, mitigate vulnerabilities and reduce the impact of cyber incidents.
- **Intelligence Support and Related Activities.** The Office of the Director of National Intelligence, working through the Cyber Threat Intelligence Integration Center, will focus on building situational threat awareness and the sharing of relevant intelligence on cyber threats, as well as mitigating the capabilities of U.S. adversaries.

Unless a government entity itself is the victim of a cyber incident, the government does not expect to get involved in managing the impact of a cyber incident on the affected entity itself, such as maintaining business continuity, managing legal risks and the like. Per the principles identified in PPD-41, however, it will remain cognizant of the entity's response activities, typically through the relevant sector-specific agency.

Key Takeaways

PPD-41 is just the latest in a series of actions taken by the White House to address cybersecurity threats, and reflects an effort to organize the growing web of government-led task forces, agencies and other bodies tasked with cybersecurity responsibilities. In extending government assistance to the private sector — while promising some measure of confidentiality — the directive reflects the reality that neither the government nor the private sector can manage these risks alone.

Return to Table of Contents

European Parliament Adopts EU-Wide Cybersecurity Directive

The European Parliament has established the first EU-wide legislation on cybersecurity: the Directive on Security of Network and Information Systems. The new legislation requires governments to establish security strategies, as well as certain essential industries and digital service providers to put security systems and programs into place.

On July 6, 2016, following approval by EU member states in December 2015, the European Parliament established the first EU-wide legislation on cybersecurity by adopting the Directive on Security of Network and Information Systems.[10] The goal of this legislation is to create a "culture of security" across so-called "vital sectors," and to increase competency and cooperation throughout the EU on cybersecurity matters in order to ensure a high common level of network and information security, and to minimize disruption to essential services. The directive has implications for both member states and companies operating in certain industries in the EU, notably by imposing new network security and incident notification obligations for providers of essential and certain digital services.

[10] The text of the directive may be found here.

Overview

Because cybersecurity incidents often have a cross-border impact, the directive aims to facilitate a common, high degree of competency across the EU and a generally harmonized approach to security requirements in order to combat the vulnerabilities posed by fragmented policies. The directive also aligns with the EU's "Digital Single Market" strategy to enhance the internal EU market by providing regulatory predictability and increasing user confidence and trust in online activities.

Starting at the government level, the directive requires member states to develop national network and information security strategies; to designate competent national authorities to oversee the implementation of the security policies under the directive; and to establish Computer Security Incident Response Teams (CSIRT) to detect risks, prevent cyber incidents, and provide swift and effective cross-border operational support within an EU-wide CSIRT network. The European Union Agency for Network and Information Security and representatives of member states also will form a Cooperation Group to facilitate strategic cooperation and the exchange of information.

At the industry level, the directive imposes obligations on public and private entities that provide a service that is "essential for the maintenance of critical societal or economic activities," where such a service depends on network and information systems, and where security incidents could have significant disruptive effects on the services provided or public safety. Such providers will be required to implement "appropriate and proportionate" security systems and to notify competent authorities of security incidents. The directive divides these service providers into two categories, operators of essential services and digital service providers, with varying security and notification requirements.

Operators of Essential Services

Because the directive is primarily aimed at ensuring the continuous functioning of essential services, it imposes high security standards on what it deems "operators of essential services." The directive designates the following specific sectors as essential services:

- energy;
- transport;
- banking;
- financial market infrastructures;
- health care;
- drinking water supply and distribution (excluding those entities that distribute water for human consumption as only part of the general distribution of goods and commodities); and

- digital infrastructure (including DNS service providers, internet exchange points and top-level domain name registries)

Each member state will develop a list of essential service providers in its territory to which the law will apply or otherwise devise "objective quantifiable criteria" to communicate which providers will fall under its jurisdiction, to be updated every two years. While not expressly stated, it appears that essential service operators may fall under the jurisdiction of more than one member state, and thus relevant companies should be aware of the laws implemented in each of the member states in which they provide services. However, the directive provides for some level of coordination and consultation between the affected member states to address incidents appropriately.

Broadly, the directive mandates that essential service operators adopt "appropriate and proportionate technical and organizational measures" to manage reasonably identifiable risks posed to the security of the networks and information systems they use, and to prevent and minimize the impact of any incidents. The directive makes no specific recommendations as to measures that must be undertaken, but notes that the network and information security systems of essential service operators must have "regard to the state of the art." Member states will be able to impose stricter requirements than those laid out in the directive, although they are encouraged to cooperate with one another to maintain consistency across jurisdictions.

In addition to system security requirements, essential service operators will be required to notify competent authorities "without undue delay" after experiencing a security incident that has a "*significant* impact" on the provision and continuity of the operator's service. In determining whether notification is necessary, operators should consider the number of service users affected, the duration of the incident and the geographical spread affected by the incident. The notification must include all information relevant to enable the competent national authorities or CSIRT to determine the cross-border impact of the incident. The competent authorities may further notify the public, if necessary, to manage the incident or prevent further disruptions, but are encouraged to balance these interests against the possible reputational and commercial damage for the entity reporting the incident.

Digital Service Providers

Digital service providers are defined as providers of online marketplaces, search engines and cloud computing services. Small or micro-enterprises with fewer than 50 employees and an annual balance sheet total under €10 million are excluded. Unlike operators of essential services, member states will not specify the digital service providers under their jurisdiction.

A digital service provider covered by the directive will fall only under the jurisdiction of a single member state in which it has its main establishment in the EU. While in principle this corresponds to the provider's "head office" in the EU, determination of this head office will be with respect to the provider's "effective and real exercise of activity through stable arrangements," even if these are conducted through a branch or subsidiary. A digital service provider with no physical presence in the EU may nevertheless be subject to the directive if it is apparent that the digital service provider is planning to offer services in the EU, such as where the provider's services are offered in the language or using the currency of one or more member states. Such a digital service provider must designate a representative in one of the member states in which it offers services who is responsible for acting on behalf of the provider and as a point of contact for the competent authorities and CSIRTs. The location of this representative will dictate which member state has jurisdiction over the provider.

Given the cross-border nature of digital services, the directive seeks to establish a higher degree of harmonization and conformity between member states' implementation of requirements for digital service providers than for operators of essential services. While digital service providers will still have to implement "state of the art" security systems that are "appropriate and proportionate" to the reasonably identifiable risks presented by their systems, the directive includes slightly more specific guidelines for determining the security requirements applicable to digital service providers. Security measures undertaken by digital service providers in response to the directive should take into account (1) the security of systems and facilities; (2) incident management; (3) business continuity management; (4) monitoring, auditing and testing; and (5) compliance with international standards. Digital service providers also must take measures to mitigate the impact of incidents. In an additional effort to provide a predictable and harmonized approach, member states may not impose greater security or notification requirements on digital service providers than set forth in the directive. Rather, digital service providers should "remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems."

Under the directive, a digital service provider must notify competent authorities "without undue delay" after experiencing a security incident that has a "*substantial* impact" on the provision of its service. Like operators of essential services, digital service providers are instructed to consider the number of users affected, the duration of the incident and the geographical area affected. Additionally, digital service providers should consider the extent of the disruption to the functioning of the service and the extent of the disruption's impact on economic and societal activities.

The obligation to notify competent authorities of an incident only will apply where the digital service provider has access to the information needed to assess the impact of an incident. The competent authority or CSIRT may inform the public about individual incidents, or require the digital service provider to do so, when disclosure is necessary to manage or prevent an incident, or is otherwise in the public interest. Again, however, authorities are encouraged to balance these interests against the possible reputational and commercial damage for the entity reporting the incident.

Enforcement and Interaction With Other Laws

With respect to operators of essential services, competent authorities will have the power to oversee compliance by requiring operators to provide information necessary to assess the security measures in place and evidence of effective implementation. If any deficiencies are identified, the competent authority may then issue binding remedial instructions.

Competent authorities have no general duty to supervise digital service providers. Instead, they may only exercise supervisory authority when provided with evidence of suspected noncompliance. Following receipt of such notice, authorities may require the digital service provider to provide information necessary to assess security systems and to remedy any failure to meet the directive's requirements.

While there is little guidance yet as to what would be deemed a failure to meet requirements under the legislation, service providers may furnish results of independently conducted audits to demonstrate compliance. This presents one possible protection against a finding that a provider did not have "appropriate" security due to a significant incident alone.

The directive only provides for investigation of noncompliance and remedial measures. It is unclear at this time what other penalties there may be, and in which situations such penalties will be levied. Member states are to individually lay down rules on penalties for infringements of the directive, the penalties of which shall be "effective, proportionate and dissuasive."

Relation to Other Laws

While companies operating in the United States and the EU may already have, or be in the process of putting in place, security measures to comply with certain other laws that impose broad security standards, such as HIPAA, the Gramm-Leach-Bliley Act or the forthcoming GDPR, such companies should be mindful of the different core aims of the directive when implementing responsive protections. While the majority of existing laws and regulations are primarily concerned with securing personal information, the directive seeks to ensure the continuity of services that are essential to a functioning society. Thus, while there may be some overlap in breach notification requirements under other laws, different measures are likely to be necessary to comply with the directive's particular security standards.

The directive does note, however, that certain sector-specific regulatory regimes exist that already target network security issues. Where such current or future sector-specific EU legal acts provide network security protection that is at least equivalent to the directive, the sector-specific acts will apply instead of the directive.

Next Steps

The directive will enter into force on August 8, 2016, of this year. The European Commission will then have one year (by August 9, 2017) to adopt implementing acts further specifying the requirements placed on digital services providers, and member states will have 21 months to transpose the directive into national law (by May 9, 2018). Member states will then have an additional six months to identify operators of essential services within their jurisdiction (by November 9, 2018).

Companies should be aware that it may not take the full 21 months for all member states to implement national laws. Some states, including Germany, France and the Netherlands, already have, or have imminent plans to introduce, cybersecurity laws that may only need small adjustments to align with the directive. Accordingly, companies should stay apprised of developments in the member states in which they operate.

Return to Table of Contents

Automotive Industry Releases Best Practices for Cybersecurity in Vehicles

An automotive industry trade group has released a set of best practices for cybersecurity in vehicle computer systems, reflecting a growing concern over the increasing reliance on computer technology in vehicle systems.

On July 21, 2016, the auto industry's Information Sharing and Analysis Center (ISAC) released a set of automotive cybersecurity "best practices" (the Best Practices)[11] for cybersecurity in vehicle computer systems. Recent developments and research related to computer-enabled vehicles have raised the specter of vehicles being hacked while on the road. The industry's effort to develop a set of guidelines are meant to help manufacturers reduce this risk.

[11] The Best Practices are available online here.

Background

As the automotive industry has begun incorporating networked technology into vehicles, the cybersecurity risks related to that technology have increased. Several years ago, automotive cybersecurity was not in the public eye; however, a year ago, after a much-publicized remote hacking of a Jeep Cherokee, cybersecurity risks associated with vehicles moved to the forefront of the industry.[12] Given that these attacks can pose an immediate and very real risk to public safety, the Automotive Information Sharing and Analysis Center (Auto-ISAC) was formed in 2015 to create and maintain a set of automotive best practices.

Best Practices

Although the Best Practices focus on United States light-duty, on-road vehicles, Auto-ISAC notes that they are applicable to other markets, including heavy-duty and commercial vehicles. As with many guidelines, the Best Practices are high-level and refrain from naming specific technical and organizational solutions. Auto-ISAC developed the Best Practices using a risk-based approach to allow automakers and others to fold them into their organization in an efficient and appropriate way that reflects the organization's degree of risk exposure.

The Best Practices detail the following seven standards that those in the automotive industry should focus on in order to improve their organization's ability to manage cybersecurity risks:

- **Governance.** Companies should have a strong cybersecurity program that works in conjunction with the organization's mission and fosters a culture of cybersecurity. Companies should consider organizational structures that include defined roles and responsibilities related to cybersecurity, appropriate resource dedication and a governance process that ensures compliance with regulations, internal policies and external obligations.
- **Security by Design.** Organizations should integrate hardware and software cybersecurity features into the development process, including by identifying potential risks, layering cybersecurity defenses, limiting and separating network interactions, and performing software vulnerability testing.
- **Risk Assessment and Management.** Although developing a vehicle with zero risk is "unobtainable and unrealistic," organizations should establish a standardized process to identify, measure and prioritize cybersecurity risks and provide a process for reporting and communicating risks to appropriate individuals, including involving the supply chain in the risk assessment process.
- **Threat Detection and Protection.** Companies should seek to proactively detect risks via various means such as routine scanning and testing of high-risk areas and anomaly detection for vehicle operations systems. In addition, the Best Practices note that threats and vulnerabilities should be reported to third parties as appropriate.
- **Incident Response and Recovery.** Companies should have an incident response plan to aid them in responding to issues in a reliable and expeditious manner. The plan should document the incident response lifecycle, put an incident response team in place, require tests and simulations to prepare the response team, and outline methods for continually improving incident response teams based on lessons learned throughout the process.
- **Awareness Training.** To promote a culture of cybersecurity, companies should establish training programs across the motor vehicle ecosystems, tailoring the training to the roles the stakeholders play, and educating employees on security awareness, roles and responsibilities.
- **Collaboration With Third Parties.** Companies should develop relationships with third parties and take advantage of available third party resources, including by reviewing information put out by industry bodies and engaging with governmental bodies, academic institutions and researchers.

The Auto-ISAC's Best Practices also point to various industry ISACs and other organizations that the automotive industry can use to work toward increasing its cybersecurity risk management and response capabilities.

In the future, Auto-ISAC will be looking to update the Best Practices and develop supplemental materials to assist organizations in developing and implementing them.

Key Takeaways

Although the recommendations in the Best Practices are similar to those put forward in other industries and by regulators, they are a useful reminder that the need for cybersecurity awareness is spreading. As cars and other vehicles become increasingly reliant on computer systems, and as these systems are increasingly designed to allow for remote access, this focus on cybersecurity is understandable.

Return to Table of Contents

[12] For more information see the August 2015 *Privacy & Cybersecurity Update*.

Florida Federal Court Dismisses Data Breach Class Action Because Purported Harm Is Too Speculative

In *Torres v. Wendy's Company*, a Florida federal court held that a data breach class action could not proceed because the named plaintiff failed to allege an actual injury in-fact, even where fraudulent charges were made on his credit card, and thus lacked standing to sue.

On July 15, 2016, a Florida district court dismissed a putative class action brought on behalf of customers of Wendy's restaurants affected by data breaches, holding that the plaintiff lacked standing because the complaint did not allege facts showing actual harm or "certainly impending" harm as a result of the breaches. The decision held that fraudulent charges alone are not enough to establish standing and concluded that where information is compromised as a result of a data breach, a plaintiff does not have standing to sue based on the mere threat of future harm.

Background and Claim

On January 27, 2016, Wendy's announced that it had discovered malware on its payment processing system. After the announcement, the plaintiff, a Wendy's customer, filed a putative class action against the company asserting claims for breach of implied contract, negligence and violations of Florida's Deceptive and Unfair Trade Practices Act. The complaint alleged that Wendy's failed to adequately safeguard customers' financial and personal information and that, due to this failure, the plaintiff and members of the putative class faced an increased risk that the hackers would use that information for fraudulent charges and other forms of identity theft. The plaintiff also alleged that after he purchased food from Wendy's, his credit union notified him that his debit card had been used to make unauthorized purchase at two other businesses. The plaintiff reported the theft to the police and notified his credit union that the charges were unauthorized. The plaintiff did not allege that these charges went unreimbursed by his credit union or that he suffered any additional unreimbursed costs in connection with the allegedly fraudulent charges.

The Court's Decision

The Florida district court dismissed the plaintiff's claims. The court held that the plaintiff did not have Article III standing because none of his theories of injury constituted an injury-in-fact.

The court rejected the plaintiff's assertion that he had suffered a concrete injury as a result of actual monetary loss. Noting the absence of any 11th Circuit case law addressing the extent of injury, the court followed the reasoning of the 11th Circuit and other district courts in the identity theft context. The Florida court held that the plaintiff's allegations of fraudulent charges on his credit card were insufficient to plead an injury-in-fact because he had not alleged any unreimbursed charges or any other actual loss in connection with the two supposed fraudulent charges, and thus had not established the "concrete" injury necessary to establish standing.

Next, the court held that the plaintiff's allegation that he was at an increased risk of future identity theft was too speculative to establish standing. Citing the Supreme Court's decision in *Clapper v. Amnesty International USA*[13](which was not a data breach case) and a host of post-Clapper decisions, the court explained that allegations of possible future injury are insufficient to establish standing. The court clarified that the threat of future harm in data breach cases is only sufficient to establish standing if the harm is "certainly impending." The court distinguished the present case, where only one person allegedly incurred two fraudulent charges and the size of the data breach and number of other customers alleged affected were unclear, from other data breach cases where thousands of customers' credit cards were used to make fraudulent charges.

The court further rejected the plaintiff's attempt to plead standing based on the costs he incurred for credit monitoring services. Quoting *Clapper*, the court remarked that "plaintiffs cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." The court noted that the majority of courts in data breach cases have held that the cost to mitigate the risk of future harm is not sufficient to establish standing unless the harm sought to be mitigated is imminent. The court held that it was unclear what mitigation costs the plaintiff actually had incurred or how they were related, if at all, to the two allegedly fraudulent charges, and that the risk of harm, in any event, did not appear to be imminent.

Lastly, the court rejected the plaintiff's other assertions of injury (that he overpaid Wendy's for products and services purchased during the data breach and that he suffered a decreased value of personal information) because the complaint failed to allege facts supporting either of those theories.

[13] 568 US _ (2013).

Key Takeaway

Standing continues to be a major obstacle to putative class actions arising from data breaches. The *Wendy's* decision highlights that injury-in-fact can be particularly difficult to establish where the plaintiffs rely on unreimbursed fraudulent charges to support a theory of actual monetary harm, and where the plaintiffs allege future, speculative harm as the basis for their claims. Companies facing putative class actions based on allegations of future harm should carefully analyze complaints to determine whether the plaintiffs have alleged facts to show that the future harm is "certainly impending" or that suggest that a "substantial risk that the harm will occur."

Return to Table of Contents

Department of Health Settles With Business Associate for HIPAA Violations

The Department of Health and Human Services' Office for Human Rights has entered into its first-ever settlement agreement with a HIPAA business associate for data security violations. The office's action may signal a new effort to enforce HIPAA's data security requirements against business associates.

On June 24, 2016, the Department of Health and Human Services' Office for Human Rights (OCR) entered into its first-ever resolution agreement with a "business associate" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to settle a potential violation of the HIPAA Security Rule. This action suggests that OCR may be stepping up its enforcement activities with respect to business associates and security practices.

Background

The HIPAA Security Rule[14] establishes national standards intended to protect electronic protected health information (ePHI) and requires business associates under HIPAA to implement appropriate administrative, physical and technical safeguards to protect such ePHI.

Business associates are entities that are not directly subject to HIPAA (which generally applies only to entities that provide health care or health insurance) but are subject to certain HIPAA requirements because of their role in providing services to HIPAA-covered entities. Business associates have access to ePHI in the course of the services they provide, so HIPAA-covered entities have obligations to ensure that these companies protect that information.

The Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) is a nonprofit corporation that provides management and information technology services as a business associate to six nursing facilities. CHCS originally had owned the nursing homes, but in November 2014 it transferred ownership to Catholic Clinical Consultants. Following the transfer, CHCS continued to provide its services to Catholic Clinical Consultants.

The potential HIPAA violations arose after the theft of a CHCS employee's iPhone, on which was stored unsecured ePHI of 412 nursing home residents. The iPhone was not encrypted or password protected and contained extensive, sensitive information about the residents, including social security numbers, diagnosis and treatment information, medical procedures, names of family members and legal guardians, and medication information.

OCR Investigation and Settlement

OCR initiated an investigation on April 17, 2014, after receiving notification of the ePHI breach from each nursing home CHCS managed. OCR's investigation found that from September 23, 2013, (the compliance date of the Security Rule for business associates) until the present, CHCS failed to:

- conduct adequate assessments of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the ePHI it held; and
- implement appropriate security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) of the Security Rule.

At the time of the incident, CHCS did not have any risk analysis or risk management plan and did not have any policies or procedures in place for responding to security incidents or addressing the removal of mobile devices containing ePHI from its facilities.

Under the final settlement between OCR and CHCS, CHCS is subject to a two-year corrective action plan that will be monitored by OCR, and it must pay a fine of $650,000.[15] In its press release announcing the resolution, OCR stated that the "unique and much-needed services in the Philadelphia region to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS" that CHCS provides played a role in determining the resolution amount. This observation, coupled with the fact that the CHCS

[14] 45 CFR Part 160 and Subparts A and C of Part 165.

[15] The Resolution Agreement and Corrective Action Plan are available online here.

is a nonprofit, religion-affiliated institution, and that the data breach affected relatively few individuals, suggests that other types of companies could be subject to heftier penalties for security issues.[16]

Key Takeaway

Although business associates have been directly liable under HIPAA since the enactment of the Health Information Technology for Economic and Clinical Health Act in 2009, this is the first HIPAA noncompliance settlement related to security issues, suggesting that more such enforcements actions may occur in the future against business associates.

Return to Table of Contents

Minnesota District Court Relies on Special Litigation Committee Report to Dismiss Target Data Breach Derivative Suit

In *Davis et al. v. Target Corporation, et al.* a Minnesota federal district court relied on the report of the special litigation committee of Target to dismiss the consolidated cybersecurity-related derivative litigation filed against Target Corporation's directors and officers.

On July 7, 2016, the United States District Court for the District of Minnesota granted the motions of the special litigation committee and the Target director and officer defendants to dismiss the consolidated shareholder derivative action filed against the company's directors and officers, in reliance on the report of the special litigation committee and in the absence of opposition from the plaintiffs.

Background and Claim

In late 2013, cyber criminals breached Target's data systems and gained access to up to 70 million customers' credit card and other private information. Beginning in February 2014, Target shareholders filed several derivative lawsuits, alleging that the company's directors and officers breached their fiduciary duties by failing to oversee Target's information security program and by failing to give the company's customers prompt and accurate information in disclosing the data breach. The various lawsuits were consolidated.

In response to the complaints, Target's board of directors formed a two-member special litigation committee (SLC), composed of a University of Minnesota law professor and a former chief justice of the Minnesota Supreme Court. Over a period of 21 months, the SLC investigated and evaluated the claims asserted in the derivative complaints. As part of its investigation, the SLC reviewed thousands of documents, interviewed 68 witnesses, received information and opinions from independent experts, and considered the applicable law. In March 2016, the SLC released a 91-page report in which it concluded that it is not in Target's best interests to pursue the claims.

The SLC notified the shareholder plaintiffs that Target would not pursue an action against the company's directors and officers. The SLC also filed a motion to dismiss the consolidated shareholder litigation. The director and officer defendants likewise filed motions to dismiss. In its report and related motion papers, the SLC noted that under Minnesota law, courts defer to a special litigation committee's conclusions if the SLC's members are disinterested and independent, and if the SLC's methodology reflects that its decision was the product of a good faith investigation. The shareholder plaintiffs did not oppose the motions to dismiss.

The Court's Decision

In a two-page order, the Minnesota district court granted the motions to dismiss. Although the order did not explain the court's reasoning, the court noted that the plaintiff shareholders stipulated that they did not oppose the motions, except to retain the right to move for legal fees and expenses.

Key Takeaway

The *Target* dismissal is a recent example of the growing number of dismissals of cybersecurity derivative lawsuits. For example, prior to *Target*, in October 2014 the United States District Court for the District of New Jersey dismissed a similar lawsuit against the directors and officers of Wyndham Worldwide, finding that the board's refusal to pursue claims in response to shareholder demands was a good faith exercise of business judgment made after reasonable investigation. While the *Target* decision is not particularly surprising, it is an important reminder of the procedural hurdles that plaintiffs in shareholder derivative litigation face when seeking to pursue derivative claims. Companies facing data breach derivative litigation should be mindful of these hurdles and carefully consider their various options for addressing such claims.

Return to Table of Contents

[16] The average settlement amount of OCR's HIPAA enforcement actions between January 2008 and June 2016 is a little more than $1 million, significantly higher than CHCS's penalty of $650,000. See HIPAA enforcement numbers here.

Report Explores Gaps Between Insurance and Information Security Professionals and Proposes Solutions to Promote the Use of Cyber Insurance

A report released last month by the SANS Institute featuring the results of a cyber insurance survey jointly conducted with Advisen Ltd. explores the conceptual gaps that often make it difficult for insurance and information security professionals to effectively work together in the cyber insurance arena. The report proposes practical solutions for a productive path forward toward minimizing the financial impact of cyber incidents through cyber insurance coverage.

With the severity and frequency of cyber incidents on the rise, the cyber insurance market continues to expand rapidly. A recently released report by the SANS Institute (SANS),[17] however, reveals the existence of what SANS refers to as "conceptual gaps" between cyber insurance and information security (InfoSec) professionals that are preventing these communities from working together to effectively manage cyber-risk through cyber insurance. Indeed, SANS reports that only 48 percent of the chief information security officers (CISOs) and other InfoSec professionals it surveyed in connection with the report find their organization's cyber insurance to be "adequate" when dealing with the aftermath of a data breach.

The SANS Report, which is based on a joint survey conducted by SANS and insurance research firm Advisen Ltd., polled a total of 397 respondents falling into the following categories: InfoSec professionals, including CISOs (203 respondents), brokers (128 respondents) and underwriters (66 respondents). Using the survey results, SANS explores four so-called "conceptual gaps" between insurance and InfoSec professionals, which, according to SANS, must be bridged before the two communities can effectively work together on the cyber insurance front: (1) the terminology gap, (2) the assessment gap, (3) the communications gap and (4) the investment gap.

The Terminology Gap

SANS reports that InfoSec and insurance professionals do not share the same understanding of the fundamental concept of risk, leading to different expectations and approaches with respect to cyber security. While InfoSec professionals view risk in terms of potential threats and vulnerabilities, insurers view risk in terms of the uncertainty or probability that a loss will occur, SANS explains. Highlighting the terminology gap, SANS reports that 55 percent of survey respondents involved in their organization's decision to purchase cyber insurance believe that they lack a common language with which to communicate about cyber insurance. SANS attributes this gap in part to the fact that cyber insurance is relatively new and ever-evolving, thereby causing insurance professionals to use inconsistent language from policy to policy. To bridge the gap, SANS maintains that a universal vocabulary must be established to enable insurance professionals and clients to clearly and accurately communicate about their expectations and actions with respect to cyberrisk management.

The Assessment Gap

While both InfoSec and insurance professionals use risk frameworks to measure and benchmark themselves internally or against other organizations, their standards and tactics for assessing and managing cyberrisk differ, according to SANS. SANS reports, for example, that 57 percent of surveyed InfoSec professionals approach risk assessment largely from qualitative methods or basic quantitative methods, whereas insurance professionals traditionally rely upon quantitative approaches.

SANS concludes that insurance professionals and clients alike would benefit from the creation of a common cybersecurity framework. Moreover, SANS suggests that any such framework should include criteria addressing the top reasons that underwriters decline applications for cyber coverage, so as to increase the likelihood that organizations will be able to secure cyber coverage if desired. According to surveyed underwriters, SANS reports, the most frequently cited reasons for rejecting cyber insurance applications include: inadequate cybersecurity testing procedures and audits (44.7 percent), inadequate processes to stay current on new releases and patches (40.4 percent), inadequate cyber incident response plans (38.3 percent), and inadequate backup processes and recovery (34 percent).

The Communications Gap

SANS also identifies a communications divide between the InfoSec and insurance communities and within organizations, which has caused some companies' cyber insurance coverage to fall short of expectations. Evidencing this gap, SANS reports that only 14 percent of surveyed brokers believe that CISOs understand the role and value of cyber insurance "very well," which suggests that underwriters and brokers should make greater efforts to educate and communicate with CISOs and other InfoSec professionals.

Within organizations, communication must increase as well, SANS advises. According to SANS, the survey results indicate that CISOs often play some role in developing recommendations for cyber insurance, but rarely have a decision-making role, with only 15 percent of surveyed brokers reporting that CISOs have "much" influence in this arena. SANS reports that the purchase decision most often lies with the C-suite, which may not fully appreciate their

[17] See the SANS Institute, "Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey," June 2016, available here.

organization's cyberrisk profile. SANS advises that senior security management must therefore take steps to communicate with executives concerning the cyberrisks their organization faces, which will enable them to make informed decisions as to the appropriate level of cyber insurance necessary to address those risks. SANS further advises that the alignment of InfoSec and risk management activities is vital to securing appropriate cyber insurance.

The Investment Gap

Finally, SANS reports a lack of transparency in the cyber insurance underwriting process, which according to SANS has led to misaligned investments by organizations seeking cyber insurance. SANS reports that 41 percent of survey respondents had to implement or update cybersecurity policies and procedures to obtain satisfactory cyber insurance coverage. SANS notes, however, that it is unclear whether organizations' security investments for the purpose of securing cyber insurance actually reduce cyberrisk or make cyber insurance cost-effective. To remedy the investment gap, SANS advises that both underwriters and InfoSec professionals must gain a better understanding of relevant cost element — the cost of InfoSec investments and the cost of coverage limits — so that organizations can readily evaluate the potential return on an investment in cyber insurance.

Key Takeaways

As more and more companies fall victim to cyber incidents, an increasing number of organizations are turning to cyber insurance to protect against cyberrisks. As the SANS report suggests, companies of all types that are considering cyber insurance would be well-advised to engage both their CISOs and enterprise risk managers in the process of procuring cyber insurance. They also should openly communicate with insurance professionals to establish a common understanding of cyberrisks and a framework outlining minimum acceptable levels of cyber hygiene. Such efforts are likely to assist organizations in securing coverage that meets their particular needs and promote a robust cyber insurance market.

Return to Table of Contents

3rd Circuit Holds That Certain Device Identifiers Are Not Personally Identifiable Information Under Federal Video Protection Privacy Act

The 3rd Circuit has ruled that persistent device identifiers are not personally identifiable information that is protected under the Video Protection Privacy Act of 1988, but did not provide a clear test for determining what identifiers would be protected.

A recent decision by the U.S. Court of Appeals for the 3rd Circuit in *In re Nickelodeon Consumer Privacy Litig.* highlights the struggle courts face as to whether device identifiers constitute personally identifiable information (PII), particularly under the Video Privacy Protection Act (VPPA). In this case, the 3rd Circuit affirmed the district court's refusal to hold Viacom Inc. and Google Inc. liable for allegations that they collected children's PII online in violation of the VPPA.[18] The court's decision comes at a time when privacy advocates are asserting that the ability to identify a specific device — such as a mobile phone — should be treated no differently than knowing an individual's name and physical address. Indeed, the new EU General Data Protection Regulation, which enters into application in May 2018, treats device identifiers as PII.

Background

The suit was a class action claim on behalf of children younger than 13 who claimed that Viacom collected their PII while they were playing or viewing video games on Viacom-owned websites, namely Nick.com, Nickjr.com and Neopets.com. According to the complaint, these websites required children to register as users before playing or viewing video games, at which point Viacom would record the age and gender of the user and the name of the video requested. Viacom also would place a "cookie" text file on the plaintiffs' computers, which would allow them to obtain additional information, such as internet protocol (IP) addresses, browser settings, operating systems and other "static digital identifiers." According to the complaint, Viacom took these actions without the consent of users or their parents. Google contracted with Viacom to place advertisements on these websites. Viacom would then share this information with Google, which would collect and compile the information.

The plaintiffs sought to establish that Google and Viacom's actions violated their privacy rights under the federal Video Protection Privacy Act of 1988 (VPPA).[19] Generally, the act prevents nonconsensual disclosure of PII, defined under the act as "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." Since Viacom only collected device identifiers and not more traditional forms of PII such as names and addresses, the key question was whether device identifiers "identify a person" under the VPPA.

[18] No. 15-1441, 2016 WL 204767 (3rd Cir. June 27, 2016). While all federal claims and California state claims were dismissed, one New Jersey state claim against Viacom (for intrusion upon seclusion) was remanded for further proceedings.

[19] 18 U.S.C. § 2710 (2002).

Google Not Liable as Mere Recipient

In dismissing the VPPA claims against Google, the 3rd Circuit agreed with the district court's reasoning that the "Act permits the plaintiffs to sue only entities that disclose protected information," not parties like Google who were "mere recipients of it."

Viacom Not Liable Because Device Identifiers Are not PII Under the Act

The panel rejected the VPPA claims against Viacom on different grounds. The plaintiffs alleged that, among other information, Viacom disclosed the following pieces of information about consumers who accessed its websites: (1) the user's IP address, (2) the user's "browser fingerprint" consisting of browser and operating system settings and (3) their computing device's unique device identifier. This information allegedly allowed Google to track the same computer across time, which, in the plaintiffs' view, effectively identified a user requesting or obtaining specific video materials in contravention of the act.

Viacom argued that static digital identifiers do not qualify as PII under the act, since they do not, in the word of the VPPA, "identify a person." Rather, it was "coded information ... to facilitate the operation of the Internet." Viacom urged the court to interpret the act in the context of the problem it was designed to address: the disclosure of a customer's video rental history by a sales clerk at a brick-and-mortar video rental store. The 3rd Circuit acknowledged that an average person could not use a device identifier alone to identify an individual. The question to the court was whether such information nonetheless rises to the level of personally identifiable information, because if it was combined with other information, it could identify a person.

The panel first looked at the statutory interpretation of the VPPA and concluded that for purposes of the statute, PII referred to "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior." The court also was persuaded by the fact that the VPPA was amended in 2013 to address how consumers provide consent, but explicitly declined to modify the definition of PII even though device identifiers were in full use at that time. The court also noted that the concept that device identifiers could conceivably be combined with reams of *other* information to decipher the identity an individual is "simply too hypothetical to support liability under the [VPPA]."

The 3rd Circuit went to great lengths to explain that its decision did not create a circuit split, despite an arguably contradictory decision earlier in the year by the 1st Circuit. In May 2016, the 1st Circuit ruled in *Yershov v. Gannett Satellite Info. Network, Inc.*,[20] holding that device identifiers could, in fact, be PII under the VPPA. The 3rd Circuit explained that the *Yershov* decision did not stand for a more general proposition that device identifiers, standing alone, can be PII under the VPPA, but rather presented a unique set of facts in which identifiers were combined with other data and then became PII. In that case, the provider disclosed not only a device identifier but also GPS coordinates for the device. To the 3rd Circuit, this additional information was sufficient to reasonably be able to identify a person for purposes of the VPPA.

The court declined to establish a general rule for device identifiers, noting that, "given the rapid pace of technological change in our digital era," a bright-line rule capable of providing "mechanistic" certainty in future cases was not advisable. As the court noted, "norms about what ought to be treated as private information on the Internet are both constantly in flux and often depend on the novelty of the technology at issue." But, in choosing to articulate a more general framework for whether device identifiers constitute PII, the court left the door open for future class action plaintiffs to advance that claim.

Key Takeaways

As internet-connected devices become even more ubiquitous, particularly through the explosion of the so-called "Internet of Things," whether device identifiers are PII will become even more important of an issue. The *In re Nickelodeon* decision highlights that courts will continue to struggle with this issue, especially in cases such as the VPPA where PII is not more specifically defined. We expect further developments in this area.

Return to Table of Contents

FTC Commissioner Reiterates Concern That FCC's Proposed Data Privacy Rules Fail to Serve Consumers' Needs

The Federal Trade Commission has sharply criticized the Federal Communications Commission's proposed data privacy rules for internet service providers, highlighting the two commissions' different approaches toward privacy regulation.

Federal Trade Commissioner Maureen Ohlhausen sharply critiqued the Federal Communications Commission's (FCC) proposed data privacy rules during a speech in late June 2016, arguing that the FCC's recommendations insufficiently protected sensitive forms of consumer data while stifling uses of non-sensitive

[20] 2016 WL 1719825 (1st Cir. 2016).

data. Ohlhausen's remarks echoed other criticism the Federal Trade Commission (FTC) has directed toward the FCC in recent months, particularly toward the FCC's forays into regulating internet service providers.

Background

The FCC's ability to regulate broadband internet service providers (ISPs) is relatively new, a result of its February 26, 2015, vote to reclassify high-speed ISPs as a telecommunications service, instead of an information service, under Title II of the Telecommunications Act. According to the FCC, its so-called "Open Internet" rules, made possible by the reclassification, are intended to protect consumer access to, and use of, the internet. Several tenets of the rules strongly echo the net neutrality movement, which emphasizes a "free and open" internet and the need to limit the ability of broadband ISPs to block, throttle or create special "fast lanes" for lawful internet content.

Proposed Rules

As part of its effort, in March 2016 the FCC proposed certain privacy rules that seek to apply the privacy requirements of Section 222 of the Communications Act to ISPs.[21] The proposed rules established three categories of how ISPs collect consumer data, each requiring a different type of consent:

- practices for which consent to collect and use of personal information is implied, because that collection and use is connected to the service being provided, and for which no further consent is required;
- first-party and affiliate marketing of telecommunications services, which requires opt-out consent; and
- other first-party uses and sharing with third parties that, in either case, are unrelated to providing communications-related services, which require affirmative opt-in consent.

The proposed rules would require all ISPs to obtain consumers' affirmative opt-in consent for the use and sharing of data that has not been specifically collected for the purpose of providing communications-related services.

FTC Critique

Until the FCC's adoption of the "Open Internet" rules, the FTC — rather than the FCC — historically regulated privacy practices of ISPs. The FTC did so based on Section 5 of the FTC Act, which prohibits unfairness and deception impacting consumers. According to the FTC, its "reasonableness" standard is a nuanced regulatory approach that allows for flexibility in considering the sensitivity of consumer data at issue. Since the FCC released its proposed rules, the FTC has, in various instances, criticized the FCC's approach generally and the proposed rules specifically.

The FTC's overarching criticism is that the FCC's approach is inflexible and fails to recognize varying levels of sensitivity of data collected in specific contexts. For example, the FTC staff, in its May 27, 2016, published comment to the proposed rules, noted that the FCC's approach did not adequately distinguish between types of data in proposing the types of consent that would be required. For example, the proposed rules would require ISPs to obtain affirmative consent for the use of non-sensitive data if the use was unrelated to communication-related services, but would allow ISPs to share the content of consumers' communications (including information from a consumer's online search or shopping history) for internal and affiliate marketing purposes without requiring affirmative consent, but merely by providing an opportunity to opt-out of this sharing.[22]

In the FTC's comments, the commission also noted that, since the FCC's jurisdiction is limited to ISPs, the FCC's involvement in data privacy matters is suboptimal in that it does not apply to other entities that collect sensitive consumer data.

Simultaneously with the FTC comment's release, Ohlhausen released a separate statement in support of the FTC comments, warning that the proposed rules may fail to adequately address consumers' needs. She repeated these criticisms in speaking to the Heritage Foundation last month, saying the proposed rules "have big problems" and that the FCC's approach "ignores the sensitivity of the consumer data at issue, and it focuses instead on what entity holds the data."[23]

Key Takeaways

The dispute between the FCC and the FTC over privacy rules reflects the government's ongoing struggle over how to properly regulate privacy collection practices, and which agency or agencies should bear responsibility. The FCC's approach favors industry-specific rules, while the FTC favors a more general reasonableness approach across all industries. To date, the FTC's approach has carried the day in Washington, but under increasing pressure from public advocates and other governments, the approach — and the authority — may change.

Return to Table of Contents

[21] The proposed rules are available here.

[22] The full FTC comment is available here.

[23] A video of Commissioner Olhausen's speech is available here.