Skadden

Privacy & Cybersecurity Update

1 EU Advocate General Endorses Standard Contractual Clauses in *Schrems II* Opinion; Questions EU-US Privacy Shield

2 Federal Court Finds Coverage for Social Engineering Loss Under Computer Fraud Policy

3 Chinese Government Issues Guideline on Apps' Illegal Collection and Use of Personal Information

5 FTC Improves Data Security Orders

6 Supreme Court of Georgia Holds That Criminal Hacking Gives Rise to Legally Cognizable Injury for Negligence

7 National Institute of Standards and Technology Releases Version 1.0 of Privacy Framework

9 Recent Events Confirm Continued Ransomware Risk

EU Advocate General Endorses Standard Contractual Clauses in *Schrems II* Opinion; Questions EU-US Privacy Shield

In a widely watched case, the EU's advocate general issued an advisory opinion supporting the validity of the so-called "standard contractual clauses" under the General Data Protection Regulation (GDPR). In the same advisory opinion, he also questioned the validity of the EU-U.S. Privacy Shield.

On December 19, 2019, Advocate General Saugmandsgaard Øe (AG) issued his advisory opinion on *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (*Schrems II*) relating to the validity of the GDPR's standard contractual clauses (SCCs) as a means for enabling transfers of personal information from the European Economic Area (EEA) to countries outside the EEA that have not been deemed adequate by the European Commission (commission), including the U.S.[1] While not binding with the Court of Justice of the European Union (CJEU), the court routinely follows the AG's opinion, so it may serve as a good indication of how the CJEU is likely to rule in the case. The CJEU's decision is expected in the first quarter of 2020.

Background

Under the GDPR, personal data only can be transferred outside of the EEA using safeguard mechanisms described in the regulation. These mechanisms should ensure that personal data transferred outside of the EEA continues to be protected to the same degree as data passed within the EU under the GDPR. Under the first of these mechanisms, the commission can decide that a third country ensures an "adequate level of protection" for transferred EEA personal data. Absent such an adequacy decision, EEA personal data only may be transferred to a third country if appropriate safeguards ensure a level of protection "essentially equivalent" to that provided in the EEA. Typically, this protection is achieved through the use of SCCs, which have been established in a series of commission decisions covering both controller-to-controller and controller-to-processor relationships.

The case began in June 2013 when Maximilian Schrems, an Austrian national, filed a complaint with Ireland's data protection commissioner (DPC), which sought to prohibit Facebook from transferring EEA personal data to the U.S. Facebook defended the transfer under the argument that it had certified to the Safe Harbor framework that had been

[1] The AG's advisory opinion is available here.

negotiated between the U.S. government and EU data protection regulators to enable transfers of personal information from the EEA to the U.S. In a decision that surprised many, the CJEU ruled in Schrems' favor in *Schrems I* and invalidated the Safe Harbor. The CJEU also held that supervisory authorities, such as the DPC, are not prevented from investigating complaints related to commission agreements or decisions. Following *Schrems I*, the commission also established a new framework, known as the EU-U.S. Privacy Shield, under which U.S. data importers can self-certify that they provide an adequate level of protection to any EEA personal data that would be transferred to them.

In light of *Schrems I*, the DPC reopened its investigation. Facebook asserted that following the invalidity of the Safe Harbor agreement, it relied on the SCCs for the transfer of EEA personal data to the U.S. Mr. Schrems therefore modified his complaint to focus on whether the SCCs satisfied the GDPR's requirements. The DPC, in a draft decision, determined that the CJEU needed to examine the validity of the SCCs before Mr. Schrems' complaint could be adjudicated.

The Opinion

In his December 2019 opinion, the AG indicated that the SCCs should not be invalidated. He explained that, in his view, the SCCs provide adequate contractual protections and it is the responsibility of the data exporter or, failing that, the relevant supervisory authority to ensure that these contractual terms are actually implemented and that compliance with them is monitored.

This assessment is to be done on a case-by-case basis for each specific transfer of EEA personal data and will require active due diligence of all "the circumstances characterising each transfer." As a result, a data exporter would be expected to (1) conduct prior due diligence on the third country's laws to ensure no conflict with the SCCs, (2) ensure that the SCCs are implemented by the data importer and (3) monitor compliance on an ongoing basis. If the SCCs are not being complied with, the AG expects the data exporter to suspend personal data transfers. If this does not occur and a complaint is made to the relevant supervisory authority, the AG believes that the supervisory authority should use adequate measures to remedy the illegality, including by, if necessary, suspending the transfer of personal data.

The AG also expressed doubts over the validity and efficacy of the Privacy Shield, saying it would be "premature" for the CJEU to rule on whether the Privacy Shield provides an adequate level of protection for the transfer of EEA personal data to the U.S.[2] Additionally, he stated his concern that the Privacy Shield does not provide individuals with an effective remedy for violations.

Key Takeaways

The AG's opinion that the SCCs should not be invalidated is positive news for the many businesses that rely on the clauses for their personal data transfer arrangements out of the EEA. However, in the AG's view, it is not enough to simply rely on the SCCs as a basis for transferring personal data. Rather, the data exporter must make sure that the SCCs are capable of being implemented abroad and ensure they are effectively and consistently implemented.

Regarding the Privacy Shield, while the AG concluded that the CJEU does not need to address that mechanism in this case, the doubt cast by the AG creates a degree of uncertainty for those who currently work with and rely on the framework. While companies who rely on the Privacy Shield do not need to take action at this time, they should monitor developments in this area.

Return to Table of Contents

Federal Court Finds Coverage for Social Engineering Loss Under Computer Fraud Policy

A federal court in Virginia recently held that a commercial truck dealer's social engineering loss resulted "directly" from the use of a computer, thereby triggering the dealer's computer fraud coverage.

On December 20, 2019, the U.S. District Court for the Eastern District of Virginia issued a decision holding that insurer Cincinnati Insurance Co. (Cincinnati) owed coverage under a computer fraud policy issued to its insured Norfolk Truck Center (Norfolk Truck), for a loss sustained as a result of a social engineering email scam that caused Norfolk Truck to mistakenly wire $300,000 to a fraudster.[3]

[2] The AG noted that *Schrems* cases do not expressly question the validity of the Privacy Shield and that there is already an action for annulment of the Privacy Shield before the CJEU (Case T 738/16, *La Quadrature du Net and Others v. Commission*).

[3] *Cincinnati Ins. Co. v. Norfolk Truck Ctr., Inc.*, No. 2:18-cv-531, 2019 WL 6977408 (E.D. Va. Dec. 20, 2019).

Norfolk Truck's Social Engineering Loss

In August 2017, the city of Norfolk, Virginia, placed an order for two trucks with commercial truck dealer Norfolk Truck. To fulfill the order, Norfolk Truck ordered parts from vendor Kimble Mixer Co. (Kimble). Unbeknownst to both companies, a fraudster had learned the details of Norfolk Truck's order and, on the day the order was placed, sent an email posing as a Kimble employee to Norfolk Truck's CEO using an email address that closely resembled the appearance of an official Kimble email address. The email attached two legitimate invoices along with wire instructions directing payment to the fraudster's account. The CEO forwarded the fraudster's email to Norfolk Truck's bank with instructions to pay the invoices from the company's accounts. The bank followed the instructions and unwittingly transferred $333,724 to the fraudster's account. On October 5, 2017, Kimble followed up for payment of the invoices, at which time Norfolk Truck realized that it had been the victim of fraud.

Norfolk Truck's Computer Fraud Insurance Claim

On October 6, 2017, Norfolk Truck filed a claim for the loss with its insurer Cincinnati under an insurance policy providing coverage for, among other things, "loss of … 'money' … resulting *directly* from the use of any computer to fraudulently cause a transfer of that property from inside the 'premises' or 'banking premises': … to a person … outside those 'premises[.]'" Cincinnati denied coverage, claiming that Norfolk Truck's loss did not result directly from computer fraud because Norfolk Truck made the payment pursuant to legitimate Kimble invoices, not the fraudster's emails; and that Norfolk Truck could have prevented the fraud by adequately investigating the wiring instructions.

Court Decision: Loss Resulted 'Directly' from Computer Fraud

In Cincinnati's declaratory judgment action against Norfolk Truck, the court found in favor of the trucking company. Addressing the definition of "directly," the court found that the term unambiguously meant "something that is done in a 'straightforward' or 'proximate' manner and 'without deviation' or 'without intervening agency' from its cause." Applying that definition, the court held that Norfolk Truck's loss was "directly" caused by the use of a computer because "[c]omputers were used in every step of the wa[y]." The fraudster, using an email address designed to mimic a legitimate Kimble address, sent an email containing false payment information. Upon receiving the email, Norfolk Truck emailed its bank to initiate the payment, setting off a chain of events that continued "in a straightforward and proximate manner" until the money was transferred to the fraudster's account.

In support of its claim that the loss was not directly caused by the use of a computer, Cincinnati argued that the use of a computer did nothing to cause the fraudulent transfer of money because Norfolk Truck was attempting to pay legitimate invoices that it already owed. The court rejected that argument, reasoning that the policy does not require a fraudulent payment by computer; it only "requires a computer's use to fraudulently cause a transfer of money," as was the case with Norfolk Truck's loss. The court similarly rejected Cincinnati's argument that the loss was not direct due to the involvement of multiple actors inside and outside of Norfolk Truck. Each of the actors "were necessary links in the chain that led to the loss," the court found, and the involvement of multiple actors "does not change the fact that the preparation and payment was initiated and completed by the fraudulent transfer of money by the use of a computer." The court also found that Norfolk Truck's failure to discover the fraud did not bar coverage on the basis that such a finding would "impermissibly read […] an implied exclusion into the insurance contract."

Key Takeaways

This case serves as another example of the differing approaches taken by courts in analyzing coverage for social engineering losses under computer fraud policies. While some courts have adopted a narrower interpretation of what it means for a loss to be directly caused by the use of a computer, the court in *Cincinnati* appears to have adopted a broader interpretation in concluding that Norfolk Truck's loss was directly caused by the use of a computer, despite the involvement of various noncomputer-related acts and actors in the causal chain.

Return to Table of Contents

Chinese Government Issues Guideline on Apps' Illegal Collection and Use of Personal Information

Chinese governmental authorities released a new guideline on the collection and use of personal information through mobile apps.

On December 30, 2019, China's Cyberspace Administration, Ministry of Industry and Information Technology, Ministry of Public Security and State Administration for Market Regulation jointly released the Guideline on Determination of Apps' Illegal Collection and Use of Personal Information[4] (guideline)

[4] The Guideline on Determination of Apps' Illegal Collection and Use of Personal Information is available here.

to facilitate the implementation of China's Cybersecurity Law (CSL), which came into effect on June 1, 2017 and became the country's first national-level law to address cybersecurity and data privacy protection. The guideline provides references for Chinese law enforcement agencies to identify apps' illegal collection and use of personal information, and also serves as guidance for app operators to conduct self-examination and self-correction.

Enforceability and Applicability

The guideline is a legally enforceable document, akin to a regulation under U.S. law. It is not entirely clear, however, to which app operators the guideline applies, as there is no mention in the document of jurisdiction. In practice, it is clear that China-based app operators are subject to the guideline. Furthermore, it is commonly recognized that multinationals collecting personal information using servers located within Chinese territory through apps are subject to the CSL and the guideline, even if the company is based outside of China. It remains unclear, however, whether the CSL and the guideline apply to app operators located entirely outside of China that collect information on Chinese citizens.

Prohibited Behaviors

The guideline identifies six categories of prohibited behaviors related to the collection and use of personal information through apps (which are further broken down into 31 subcategories). The six categories of prohibited behaviors are:

- nondisclosure of collection and use rules;
- failure to expressly state the purpose, method and scope of collecting and using personal information;
- collecting and using personal information without users' consent;
- collecting personal information unrelated to the services being provided and in violation of the principle of necessity;
- providing personal information to third parties without the users' consent; and
- failure to (1) provide the function to delete or correct personal information in accordance with the law or (2) announce information, such as channels to make complaints or act as a whistleblower.

Notice and Consent

The guideline is largely based on a structure of notice and consent.

Notice

Overall, the guideline requires app operators to clearly notify users before collecting their personal information. App operators must formulate a clear privacy policy containing rules for collecting and using personal information, and must use pop-up windows or other conspicuous methods to prompt users to read the privacy policy when first using the app.

The guideline also requires app operators to specify the purpose, method and scope of the personal information collected or used by the apps (including third-party code or plug-ins that are commissioned or embedded in the app). Operators must notify the users of any changes to such purpose, method or scope, such as by updating, and reminding users to read, their privacy policy.

Additionally, the guideline establishes some requirements with respect to the methods for providing notice to app users, including prohibiting the use of confusing terminology in privacy policies and requiring app operators to provide simplified Chinese versions of their privacy policies. Finally, the guideline includes requirements as to the accessibility of privacy policies, requiring that these documents must be less than four clicks away from the main interface of the app.

Consent

The guideline requires operators to obtain users' express consent before collecting personal information through an app. However, it also prohibits a range of activities relating to how to obtain this consent, including:

- disrupting users' normal use of the app by frequently asking the users to give consent;
- collecting personal information out of the scope of users' authorization;
- configuring the app so that the user consents to the privacy policy by default;
- changing the status of users' setup permissions to collect personal information without users' consent; and
- utilizing users' personal information and algorithms to push targeted information by not providing an option to deliver nontargeted information.

App operators also must provide users with channels and methods for withdrawing consent to collect personal information, and must be able to effectively correct and delete personal information or deregister users' accounts without setting unnecessary or unreasonable conditions.

Necessity

The guideline also sets forth a principle of necessity to govern personal information collection. Under this principle, the types of personal information collected — or the app permissions being turned on to collect personal information — must be "related to" the existing business function. Furthermore, app operators may not refuse to provide business functions to users on the grounds that users have not agreed to collect "unnecessary" information or turn on "unnecessary" permissions. In practice, it remains to be seen how this principle of necessity will be interpreted or enforced.

Some Ambiguities Remain

While the guideline appears relatively clear and thorough in many respects, there are some areas of ambiguity. In addition to the question of applicability to app operators based outside of China as described above, there are questions as to what steps operators must take after they make the required changes to their privacy policies. As noted above, the guideline requires operators to update the privacy policies to reflect these changes and remind users to read the updated policy. However, it is unclear whether the app operators must obtain the users' consent to the changed policy before continuing to collect information, or if simply advising them to read the changes is sufficient. The emphasis on consent may suggest the authors would prefer that operators obtain a new consent, but the language of the guideline itself suggests it is not required. Ambiguities such as these need further interpretation or enforcement actions made by Chinese judicial and administrative authorities.

Key Takeaways

The guideline reflects China's latest effort to regulate the use of Chinese users' personal information. App operators should carefully review their privacy policies and other personal information collection rules to ensure they are compliant with the detailed requirements under the guideline. As ambiguities are resolved over time, companies should continually monitor how the guideline is enforced in China and adjust their own compliance efforts accordingly.

Return to Table of Contents

FTC Improves Data Security Orders

The Federal Trade Commission (FTC) has strengthened its data security orders to include clearer guidance and increased accountability for companies.

On January 6, 2020, the FTC announced in a blog post that it had recently made significant improvements to its data security orders, updating the relatively standard language that had been in place since the early 2000s. As part of a new initiative by FTC Chairman Joseph Simons and FTC Bureau of Consumer Protection Director Andrew Smith, three major changes have been made to heighten deterrence and improve data security practices, all within the scope of the FTC's existing authority. The initiative is in part a response to the Eleventh Circuit's 2018 *LabMD* decision, which struck down an FTC data security order as unenforceable and vague, leading to the agency subsequently holding a hearing in December 2018 as part of its "Hearings on Competition and Consumer Protection in the 21st Century" on how it could improve data security orders.

Improvements

According to the FTC blog post, the improvements fall into three categories:

More Specific

Going forward, FTC orders will require companies to implement a comprehensive, process-based data security program and specific safeguards to address the problems alleged in a complaint, such as employee training, access controls, monitoring systems for data security incidents, patch management systems and encryption. According to the FTC, these clearer requirements will help companies to more effectively remedy their data security issues and make its orders more enforceable.

Increased Accountability of Third-Party Assessors

The FTC has relied on third-party assessors to review the data security programs mandated by its orders, but now requires more rigorous assessments and heightened scrutiny of the assessors themselves. Assessors must identify evidence to support their conclusions, retain documents related to the assessment and

cannot refuse to provide those documents to the FTC on the basis of privilege. The FTC considers access to these documents crucial in its ability to investigate companies' compliance and enforce its orders. In addition, the FTC will now be able to approve (or disapprove) its third-party assessors every two years.

Cooperation With a Company's C-Suite and Board

The new orders create additional incentives for high-level oversight and attention to data security. For example, senior officers must provide annual certifications of compliance to the FTC, and companies must present their written information security program to their board (or similar governing body) on an annual basis. According to the FTC, this encourages senior managers to assess their company's information security program in sufficient detail so they can personally corroborate that the company has achieved compliance each year.

Key Takeaways

The FTC's changes are designed to provide more specific requirements for companies on the receiving end of an order. Companies will receive lists of steps they must take to comply and also may experience heightened scrutiny from third-party assessors. Finally, the FTC likely will require greater internal oversight and reporting on cybersecurity practices.

Return to Table of Contents

Supreme Court of Georgia Holds That Criminal Hacking Gives Rise to Legally Cognizable Injury for Negligence

The Supreme Court of Georgia has ruled that allegations of probable identify theft — short of actual identify theft — are sufficient to state a cause of action under Georgia law.

On December 23, 2019, the Supreme Court of Georgia held in *Collins v. Athens Orthopedic Clinic, PA*[5] that allegations of probable, as opposed to merely possible, identify theft or fraud is a sufficient injury to state a cause of action following a data breach. This decision adds to the growing volume of legal opinions grappling with what type of injury is sufficient to establish a cognizable claim and standing in a data breach case.

[5] *Collins v. Athens Orthopedic Clinic*, 347 Ga. App. 13 (2018).

Background

In June 2016, a hacker accessed and exfiltrated personally identifiable information, including Social Security numbers, addresses, dates of birth and health insurance details, of at least 200,000 current and former patients of Athens Orthopedic Clinic. The hacker demanded a ransom, but the clinic refused to pay. Certain of the stolen data was offered for sale on the "dark web," or made available on Pastebin, a data-storage website that facilitates online data sharing.

Affected patients brought a putative class action against the clinic, asserting negligence, breach of implied contract and unjust enrichment claims under Georgia law. They alleged an "imminent and substantial risk of future injury," in that criminals could assume class members' identities and fraudulently obtain credit cards, issue fraudulent checks, fraudulently file for tax refunds, liquidate bank accounts and open new accounts in the class members' names. One of the named plaintiffs also alleged fraudulent charges on her credit card account. The plaintiffs sought injunctive relief requiring the clinic to undertake actions to ensure the security of personal data in the future, as well as damages to recover the costs of credit monitoring and identity theft protection.

The Court of Appeals of Georgia's Opinion

A divided panel of the Court of Appeals of Georgia affirmed the trial court's summary dismissal of the claims at the pleading stage, reasoning that the "fact of compromised data is not a compensable injury by itself in the absence of some 'loss or damage.'" The court also reasoned that while "credit monitoring and other precautionary measures are undoubtedly prudent," they are "not recoverable damages" under the alleged facts, demonstrating that the plaintiffs were attempting to recover only for "an increased risk of harm." Accordingly, the court concluded that the plaintiffs' allegations were "insufficient to state a cognizable claim under Georgia law."

The Supreme Court of Georgia's Opinion

Reversing the Court of Appeals' ruling, the Supreme Court of Georgia held that the plaintiffs had sufficiently alleged a cognizable injury to satisfy the injury element for their negligence claim. Under Georgia law, a wrongdoer can be held liable in tort for probable, but not merely possible, injury. A mere fear of future injury is too speculative to support recovery. Applying that standard to the case, the court determined that the plaintiffs' allegations of injury crossed the line to probable.

The court distinguished two cases relied on by the Court of Appeals where the injury arising from the exposure of sensitive personal information was speculative rather than probable. Unlike in those cases, where one would have to engage in a "a long series of speculative inferences, including that someone with malicious intent would obtain the data in the first place, that this person would attempt to use that data to steal the claimant's identity or make the data available to someone who would attempt to do so, and that the would-be identity thief would succeed in fraudulent usage of the [victim's] identity," the court reasoned that the allegations in the case at hand were "much further along in the chain of inferences." Specifically, the plaintiffs had alleged probable injury by pointing to "large-scale criminal activity," namely the theft of large amounts of data, the unsuccessful demand for a ransom, the offering of the data for sale on the "dark web" and the sensitive nature of the data, which could be used to assume class members' identities and engage in other fraudulent activities, such as fraudulently issuing checks or filing for tax refunds. Accordingly, the "large-scale criminal activity" placed the case into a "different category of data-exposure cases," distinct from previous cases, including the two relied on by the Court of Appeals, where the plaintiffs had failed to show that the stolen data was at least in criminal hands.

The court stressed that its holding did not "depend on the plaintiffs' allegations that the breach has caused them to spend money attempting to mitigate the consequences of the breach by avoiding actual identity theft," or that one named plaintiff already had suffered identity theft. It sufficed that, because of the criminal involvement and other alleged facts, the alleged theft left the plaintiff class at an imminent and substantial risk of identity theft.

The court also distinguished between injury-in-fact for standing purposes and a cognizable injury for Georgia tort law. The court concluded, however, that the "allegations that we determine are enough here to plead a legally cognizable injury are also sufficient in this procedural posture to satisfy the injury-in-fact element of standing."

Despite reviving their case, the court reminded the plaintiffs that they would still need to support their allegations with actual evidence as the case proceeds beyond the pleading stage. It forewarned that the risk of identity theft "may become easier or more difficult to prove as time goes on and the plaintiffs do or do not experience actual identity theft." It also forewarned that proving proximate cause may become more difficult too with the passage of time, citing a case involving a failure to link stolen data to the theft of the defendant's computers as opposed to some other source. Given these challenges, the court noted that traditional tort law was relatively ill-suited to address the "fairly new kind of injury" that could arise out of data breach cases. It noted that the "complex tradeoffs" in such cases may be better resolved by the legislative process.[6]

Key Takeaways

In data breach cases, courts continue to grapple with what constitutes sufficient injury for the injury element of common law causes of action, such as negligence. Whether the allegations suffice is highly fact-dependent, but courts may be more likely to find an injury sufficiently alleged when the allegations indicate criminal involvement. Proof relevant to actually establishing injury, however, could strengthen or weaken over time, depending on whether actual identity theft or fraud occurs and can be linked to the breach.

Return to Table of Contents

National Institute of Standards and Technology Releases Version 1.0 of Privacy Framework

The National Institute of Standards and Technology (NIST) has released version 1.0 of its privacy framework to help organizations improve their overall privacy practices.

Introduction

On January 16, 2020, the NIST published version 1.0 of its "Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management" (privacy framework).[7] This version, developed from a preliminary draft released in September 2019, is intended to help organizations optimize beneficial uses of data while minimizing adverse privacy-related consequences. The privacy framework is the result of a collaborative effort between the NIST and various stakeholders in the public and private sector.

This is the second framework published by the NIST in the privacy and cybersecurity area. The first was a cybersecurity framework, a draft of which was released in 2014 and the final version in April 2018 (the cybersecurity framework). Though not a regulation and not legally binding, the cybersecurity framework has since become an industry standard for addressing cybersecurity-related risks and best practices. The privacy framework also is not legally binding, but closely follows the structure of the cybersecurity framework and, as such, also may become an industry standard.

[6] The court's opinion is available here.

[7] The privacy framework can be found here.

Below is a short summary of the key components of the privacy framework.

The purpose of the privacy framework is to help organizations manage risk by encouraging effective privacy practices that facilitate internal communication and collaboration.

Privacy Risk Assessment

The privacy framework recommends that, as part of the privacy management process, organizations conduct a privacy risk assessment. It suggests that organizations identify potential privacy problems that individuals may experience in connection with system, product or service operations involving data, starting from data collection through the final disposal of the data. The framework notes these problems can manifest in a wide array of ways, ranging from organizational embarrassment to more tangible problems such as discrimination, economic loss or even physical harm. The privacy framework proposes that organizations identify the likelihood of these potential risks, as well as their impact — both to an affected individual and to the organization itself — should they occur.

Once an organization has conducted its privacy risk assessment, it can use the information to weigh the benefits of particular data processing operations against the risks and formulate an appropriate response. A response could take a variety of forms, such as:

- mitigating or avoiding the risk by changing operations;
- transferring the risk to — or sharing the risk with — a third party via contractual arrangements, or through privacy policies and consents; or
- accepting the risk.

The privacy framework is designed to provide organizations and industries with a common language for understanding, managing and communicating privacy risks. It is composed of three parts: core, profiles and implementation tiers.

Framework Core

The framework core is a set of privacy protection activities and outcomes designed to enable organizations to communicate prioritized privacy protection activities and outcomes from the executive level to the implementation and operations level. The core is further divided into key functional areas, each of which are then divided into categories and subcategories of privacy outcomes tied to the needs and practices within a given organization. The five functions are:

- Identify-P: Understand how to manage privacy risks that affect individuals.
- Govern-P: Develop and implement a governance structure that encompasses privacy risk management priorities.
- Control-P: Develop and implement practices for organizations and individuals to manage privacy risk.
- Communicate-P: Develop and implement procedures to educate organizations and individuals about data processing and associated privacy risks.
- Protect-P: Develop and implement appropriate safeguards to prevent cybersecurity-related privacy events.

Framework Profiles

Framework profiles are a selection of specific functions, categories and subcategories from the core that an organization has prioritized to help manage its privacy risk. Each organization will develop its own profiles using elements from the core tailored to its specific needs and risk profile. The framework recommends separating the profiles into two categories: (1) current profiles that represent current privacy practices and outcomes, and (2) target profiles that represent desired privacy practices and outcomes.

To develop a profile, the privacy framework suggests organizations consider, among other things, business objectives, privacy values and risk tolerance; relationships with other actors within the data processing ecosystem; legal and regulatory requirements; and risk management priorities and resources.

Framework Implementation Tiers

The framework implementation tiers capture the current level of sophistication of an organization's privacy practices, categorized into four distinct and incremental tiers:

- Tier 1: Partial (*e.g.*, organizations that do not have formalized privacy risk management practices or policies).
- Tier 2: Risk Informed (*e.g.*, organizations have formalized privacy risk management practices that may not be established as policy).
- Tier 3: Repeatable (*e.g.*, organizations have formalized privacy risk management policies).
- Tier 4: Adaptive (*e.g.*, organizations adapt their privacy risk management policies in response to privacy-related events).

The implementation tiers are intended to help organizations benchmark internal progress. However, the privacy framework notes that successful implementation should not be determined by an organization's framework implementation tier.

How To Use the Privacy Framework

The NIST presents a few ways in which the privacy framework may be used, including to:

- map privacy practices to relevant tools, standards, laws and regulations;
- strengthen internal accountability across all levels within an organization;
- support the creation or improvement of privacy programs;
- support the achievement of prioritized privacy outcomes;
- determine an organization's role within the broader data processing ecosystem; and/or
- inform decisions about products and services that help minimize privacy risks.

Notwithstanding the above recommendations, the privacy framework is flexible and intended to be used by organizations as they see fit. The NIST emphasized this feature, stating that the privacy framework is "flexible enough to address diverse privacy needs." The NIST also recommends adopting the privacy framework in conjunction with its cybersecurity framework For example, in managing cybersecurity-related privacy risks, organizations can leverage the privacy framework's core by incorporating the cybersecurity framework's functions. Organizations, particularly those that have already adopted the cybersecurity framework, should therefore keep that guidance in mind when working with the privacy framework.

Key Takeaways

The privacy framework eventually may prove to be as influential as the cybersecurity framework. Organizations should consider using the privacy framework to assess and manage their own privacy practices, particularly those organizations that have already incorporated practices from the previous framework. In light of recent privacy laws, including the California Consumer Privacy Act and the EU's GDPR, the privacy framework may be a useful guide for organizations in complying with regulatory obligations.

Return to Table of Contents

Recent Events Confirm Continued Ransomware Risk

Ransomware attacks are likely to continue in 2020, and vendor vulnerabilities can create problems for an organization's customers.

The new year started with news of a ransomware attack on a global foreign currency exchange provider, forcing the company to go offline to contain the attack and its impact. The disruption had a ripple effect across a number of financial institutions that relied on the provider to fulfill currency orders for their customers. The incident was a reminder of the continued threat of ransomware and other cyberattacks, and reiterates the need for companies to ensure they have systems in place to protect against and otherwise mitigate the effects of such attacks against their organizations and their trusted service providers.

The Ransomware Attack

The attack against the currency provider is understood to have involved the use of ransomware known as Sodinokibi/REvil. The attackers demanded $6 million from the company for the return of customer data that they allegedly took, though the currency provider disputes that any customer data was taken. The attackers also threatened to sell the customers' data if the currency provider did not pay the ransom.

It has been reported that attackers exploited a known vulnerability that could have been corrected if the company used a patch released in April 2019. However, as reported by *The Wall Street Journal*, the currency provider was not alone in failing to implement the patch, with a number of major global companies still vulnerable at the turn of the year. The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency also issued an alert warning organizations that the vulnerability "continue[s] to be an attractive target for malicious actors."

Risks Continue in 2020

Malicious parties that exploit companies' failures to patch systems is not a new issue. The WannaCry ransomware attack of May 2017 affected thousands of computers worldwide despite a patch being released in March of that year that addressed the exploited vulnerability. Unpatched systems also are not a diminishing issue, as the risks facing organizations are increasing, both

due to the direct impact such attacks are having on companies, as well as the stance being taken by regulators. For example, the U.K.'s Information Commissioner's Office and the FTC have both emphasized the importance of patching systems and the subsequent enforcement risks that could result from failing to do so. The enforcement actions taken against Equifax following a 2017 data breach resulting from the company's failure to patch a known vulnerability are prime examples of the regulatory damage a company could face.[8] In light of these factors, we expect the trend of organizations failing to implement effective patching measures to continue in 2020.

In many instances, ransomware attacks are directly tied to patching failures, as exemplified in the currency provider incident. According to reports published by cybersecurity companies McAfee Labs, Chubb and Emsisoft, there were significant increases in 2019 in the number of ransomware attacks against enterprises and government entities. Several reports also estimate that a substantial number of victims paid the ransoms, incentivizing attackers to continue using these types of attacks. As patching issues are not expected to dissipate in 2020, we also do not expect ransomware risks to decrease.

Key Takeaways

Organizations can mitigate the risks discussed above by taking steps to (1) protect against cyberattacks and (2) minimize the scope and impact of a successful cyberattack.

Protecting against cyberattacks is a broad task and involves several intersecting layers of controls. Companies should implement comprehensive cybersecurity policies and procedures detailing the controls in place to protect systems, networks and data. The implementation of these policies and procedures should regularly be reviewed and assessed. The specific assessment programs can vary based on the risks faced by the company, but typically include information security audits, internal and external vulnerability assessments, and penetration tests. A patch management program and cybersecurity training also are important tools in preventing attacks.

Minimizing the scope and impact of a successful cyberattack starts before an attack even occurs and continues until it is fully mitigated. Developing and implementing an incident response plan and identifying a dedicated internal governance team to respond to incidents and engage in tabletop training exercises can be some of the most important steps an organization can take. Additionally, business continuity and disaster recovery plans can help minimize business disruption from attacks. Backup systems should receive the same level of security consideration as production systems. It is in an attacker's interest to not only bring down a company's main information technology systems, but also render their backups useless so as to increase the damage inflicted and, in the case of ransomware, force the company to pay the ransom demanded.

Companies also should consider their vulnerability and how to respond if key vendors are attacked. Actions could include careful attention to critical vendors' cybersecurity preparedness, contractual commitments with respect to cybersecurity standards and assessing how the vendor will respond to — and allocate liability for — security breaches. Although not practical in many circumstances, companies should consider how they will respond if a vendor's services become unavailable because of an attack.

Return to Table of Contents

[8] In 2018, the Information Commissioner's Office issued a £500,000 fine to Equifax (the maximum it could for pre-GDPR infringement), and, in 2019, the credit bureau agreed to a settlement with the FTC, the Consumer Financial Protection Bureau, and 50 U.S. states and territories, under which the company could pay up to $700 million.

Privacy & Cybersecurity Update

Contacts

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

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

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

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

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

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

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

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

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

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

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

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

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

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

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

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

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

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000