Skadden

Privacy & Cybersecurity Update

EU Advisory Group Critiques Privacy Shield

The Article 29 Data Protection Working Party released a report challenging the adequacy of the EU-U.S. Privacy Shield and setting forth a series of recommendations for future personal data transfers.

On November 28, 2017, the Article 29 Data Protection Working Party — an advisory body made up of representatives of the data protection authority of each EU member state, the European data protection supervisor and the European Commission — issued an advisory report on the adequacy of the EU-U.S. Privacy Shield. The report accompanies the European Commission's first annual joint review of the Privacy Shield, conducted with several U.S. federal agencies. In its review, the commission stated that the Privacy Shield continues to provide a valid mechanism for organizations to transfer personal information from the EU to the U.S. By contrast, the Article 29 Working Party's report strongly critiqued the current regime and provided a set of aspirational recommendations for personal data transfers moving forward. The Article 29 Working Party stated that it would take appropriate action — including petitioning the European national courts to refer a challenge on the adequacy of the Privacy Shield to the Court of Justice of the European Union — in the event that its concerns are not addressed by the European Commission's second annual joint review. Although the Article 29 Working Party maintains only an advisory role, the report raises issues that create some uncertainty regarding the continued viability of the Privacy Shield.

Background on the EU-US Privacy Shield

In 2016, the United States and the European Commission adopted the EU-U.S. Privacy Shield, a self-certification framework designed to enable companies to transfer personal data from the EU and the three European Economic Area member states — Norway, Liechtenstein and Iceland — to the U.S. Under the EU Data Protection Directive, EU citizens' personal data can be transferred only to countries with "adequate" data

protection laws in place. The U.S. does not meet this standard. However, under the Privacy Shield, companies that self-certify their adherence to seven broad data privacy principles may transfer personal data outside of the EU to the U.S.

The Privacy Shield replaced the previous framework between the EU and U.S. known as the Safe Harbor Privacy Principles, which the Court of Justice of the European Union invalidated in October 2015 in the *Schrems v. Data Protection Commissioner* case. In the *Schrems* decision, the court found that the Safe Harbor failed to protect the personal data of EU citizens, mainly due to the U.S. government's ability to access personal data for national security purposes. The Privacy Shield aimed to remedy the inadequacies of the Safe Harbor. However, after the Privacy Shield's adoption, many privacy advocates criticized the replacement framework for failing to address the government's surveillance concerns raised in *Schrems*.

European Commission's First Annual Review of the Privacy Shield

As we discussed in our October 2017 mailing, in its first annual joint review of the Privacy Shield, the commission concluded that "the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the [European] Union to organizations in the United States." The commission also lauded the Department of Commerce's more robust oversight of self-certified companies in the U.S., the improved availability of mechanisms for EU individuals to obtain redress from companies that violate European data protection law and a satisfactory self-certification process. Although the commission noted some areas for improvement — and, notably, did not state whether the Privacy Shield provided protections sufficient to meet the more stringent requirements of the General Data Protection Regulation (GDPR) — the commission's review provided some short-term comfort to affected companies regarding the adequacy of the Privacy Shield.

Article 29 Working Party's Report

The Article 29 Working Party made the following critiques of the Privacy Shield in the report it released after the commission's first annual joint review:

- **Lack of guidance for companies from the U.S. Department of Commerce:** The Article 29 Working Party explained that companies should be in a position to assess their compliance with the Privacy Shield on the basis of clear guidance from the Department of Commerce on how the substance of the Privacy Shield's requirements and principles should be implemented in practice. For example, the report noted the lack of clarity regarding what qualifies as "HR data" and the confusion surrounding cross-border transfers of such data.
- **Insufficient oversight of Privacy Shield self-certified companies:** The report noted that the Federal Trade Commission (FTC) and Department of Commerce should conduct periodic investigations of Privacy Shield-certified companies to ensure that they continue to meet the principles and requirements of the framework. This echoes a long-standing concern that the Article 29 Working Party had regarding FTC oversight of the Safe Harbor.
- **Inadequate protections against automated decision-making:** Recognizing that predictive analytics can significantly impact individuals without their knowledge, the report called upon the commission and U.S. agencies to consider specific rules concerning automated decision-making.
- **Improper collection of personal data by U.S. agencies:** Based on the information made available to the Article 29 Working Party during the commission's first annual joint review, the report called for further evidence or legally binding commitments to substantiate assertions by U.S. authorities that they do not collect personal information in an indiscriminate and generalized manner.
- **Ineffective redress for EU individuals:** The report critiqued the "standing" requirement in U.S. courts as an insurmountable barrier to judicial redress for individuals who wish to challenge surveillance by U.S. agencies and otherwise allege violations of their right to privacy.

The Article 29 Working Party concluded the report by stating that if the commission and U.S. agencies do not address the concerns raised in the report by next year, the Article 29 Working Party will support a legal challenge of the Privacy Shield.

Key Takeaways

The Article 29 Working Party's report suggests that the Privacy Shield may face challenges in the future. Although there is currently no reason for companies to stop using the Privacy Shield, those who have self-certified should be aware of the critiques that have been raised, and those who are considering whether to self-certify should take note of this report.

Return to Table of Contents

Sixth Circuit to Rule on Scope of Computer Fraud Coverage in Insurance Dispute Over Social Engineering Fraud Loss

The U.S. Court of Appeals for the Sixth Circuit will consider the issue of whether computer fraud coverage under a traditional crime policy extends to a loss sustained by a manufacturer that was tricked into wiring payments to email fraudsters posing as one of the manufacturer's overseas vendors.

In November 2017, Michigan-based tool and die manufacturer American Tooling Center, Inc. (ATC) filed an appeal to the Sixth Circuit regarding a decision holding that ATC was not covered under the computer fraud coverage part of its crime policy issued by Travelers Casualty and Surety Company of America (Travelers) for over $800,000 in fraudulent transfers that resulted from a social engineering scheme known as "spoofing."[1] The Sixth Circuit's decision will add to the expanding and varied body of jurisprudence on coverage for social engineering-related losses under traditional crime policies.

The Fraudulent Transfers and ATC's Insurance Claim

As part of its business, ATC outsourced certain manufacturing work to a Chinese vendor, Shanghai YiFeng Automotive Die Manufacturers Co. Inc. (YiFeng). ATC paid YiFeng in stages via wire transfer when it completed certain milestones. In mid-2015, fraudsters impersonating YiFeng emailed ATC from an address closely resembling YiFeng's and requested payment of over $800,000 in legitimate outstanding invoices to a new bank account that, unbeknownst to ATC, was controlled by the fraudsters. After confirming that YiFeng had met requisite milestones — but without verifying the new banking information — ATC wired payment to the new fraudster-controlled bank account. By the time ATC detected the fraud, the money could not be retrieved.

ATC filed a claim under its Travelers crime policy, which provided computer fraud coverage for any "direct loss" that was "directly caused" by "Computer Fraud" — defined in part as "[t]he use of any computer to fraudulently cause a transfer." Travelers denied the claim on the basis that ATC's loss was not a direct loss that was directly caused by the use of a computer, and litigation ensued.

The District Court's Decision

The U.S. District Court for the Eastern District of Michigan agreed with Travelers' interpretation of the policy's computer fraud coverage and granted summary judgment in its favor, holding that ATC's loss was not covered under the policy. It reasoned that "[g]iven the intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds" — ATC's verification of milestones and authorization and initiation of the transfers without verifying bank account information — "it cannot be said that ATC suffered a 'direct' loss 'directly caused' by the use of any computer." The court relied on Sixth Circuit precedent stating that "direct" is defined as "immediate" without any intervening events, and other district court decisions declining to extend computer fraud coverage to scenarios where an email is merely incidental to a fraudulent transfer.

ATC's Appeal to the Sixth Circuit

In November 2017, ATC filed an appeal to the Sixth Circuit seeking reversal of the district court's decision. ATC contended that it suffered a "direct loss" because the wire transfers to the fraudsters' bank account came directly from ATC's account, and the transfers were "only initiated because of the fraudulent spoofed emails sent via computer to ATC." Moreover, ATC argued, the fraudsters used a computer to hack into ATC and/or YiFeng's email server, intercept legitimate emails, create fake email domains and send spoof emails to ATC that were intentionally designed to look like legitimate emails. Therefore, the loss was caused by computer fraud because "[t]he use of a computer was an integral and indispensable part of the fraud committed on ATC."

In its appellate brief filed this month, Travelers countered that ATC's loss did not constitute computer fraud because a computer was not used to fraudulently cause the transfers. In order to trigger the policy's computer fraud coverage, Travelers wrote, "a computer must fraudulently cause the transfer. It is not sufficient to simply use a computer and have a transfer that is fraudulent." In the present scenario, a computer did not fraudulently cause any transfer. "ATC simply received an email communication that provided it with false information. Rather than use a computer to fraudulently cause a transfer, the third party merely used a computer to provide ATC with false information more quickly than it could through the United States mail." Further, Travelers argued, even if there was computer fraud, it did not directly cause any loss in light of "the numerous intervening events" between the allegedly fraudulent emails and the wire transfers.

[1] *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017).

Key Takeaways

Regardless of how the Sixth Circuit resolves the coverage issue in *American Tooling Center v. Travelers*, both policyholders and insurers should be cognizant of the fact that courts throughout the country have reached varying results on the issue of coverage for social engineering fraud under traditional crime policies. Given the increasing frequency of social engineering fraud losses and the uncertainty of coverage under traditional crime policies, insurers have introduced coverage specifically geared to social engineering scams perpetrated by fraudsters posing as vendors, clients, employees and the like. Businesses should evaluate their risk profiles and consult with their insurance broker and coverage counsel to determine whether it would be beneficial to purchase this additional coverage.

Return to Table of Contents

The Top Privacy and Cybersecurity Stories of 2017 and What to Look for in 2018

This past year saw a number of significant developments in the privacy and cybersecurity area that will likely have repercussions for 2018 and beyond. We recap some key stories from 2017 below.

The Approaching GDPR

The EU GDPR will take effect on May 25, 2018, replacing the current Data Protection Directive 95/46/EC that was designed to harmonize data privacy laws across Europe. Amongst the most significant changes is the extension of EU privacy laws to all companies that process personal data of EU data subjects regardless of the company's location, as well as strengthening the requirements to be able to rely on a user's consent. Fines under the GDPR can be significant for material violations of up to the greater of 4 percent of a company's annual global turnover or €20 million.

Although the effective date is only a few months away, much uncertainty surrounds how certain provisions will be interpreted and enforced. In 2017, the EU's Article 29 Working Party shed some light on how issues like the new data breach notification requirement, as well as the limits on profiling data subjects and using automated decision-making, will be enforced.

We believe that 2018 will yield a fair amount of uncertainty in this space with certain provisions becoming clearer as enforcement actions are brought. It also remains to be seen whether individual countries will choose to enact additional requirements that adversely impact the goal of creating a more unified EU approach to data privacy since the GDPR permits some limited country-specific customization. For example, in July 2017, German Parliament passed a new version of the country's Federal Data Protection Act (also known as Bundesdatenschutzgestz or BDSG), making Germany the first EU member state to adopt national legislation in response to the GDPR, and the first to take advantage of the leeway permitted in the opening clauses in areas such as how employee data and sensitive data will be handled.

Companies who control or process personal data about EU subjects will need to carefully monitor this evolving area of the law in 2018.

Standing in Data Privacy Breach Class Actions

One of the greatest risks that companies face in the aftermath of a data breach are plaintiff class action lawsuits. A key gating factor in these cases to date has been whether plaintiffs have sufficient cognizable injury to bring such cases, particularly when the alleged injury is merely the possibility of future identity theft. In 2017 courts continued to take differing views on this issue, laying the groundwork for continued battles in this space in 2018. For example, in *In re SuperValu, Inc., Consumer Data Security Breach Litigation*, which involved the theft of credit card information from SuperValu and Albertsons grocery stores, the Eighth Circuit found that the threat of fraud from the breach of credit card information fell short of the standing requirements that an injury be "concrete and particularized and actual or imminent." This is consistent with similar rulings in the Second and Fourth Circuits, but contrasts with certain rulings in other circuits. For example, also in 2017, the D.C. Circuit found in a case involving a breach at CareFirst that it used "experience and common sense" to find a substantial risk of financial identity theft arising out of hackers' access to "Social Security numbers and credit card information in addition to names, birth dates, email addresses and policy subscriber numbers." The court found there to be substantial risk that an individual could "impersonate the victim and obtain medical services in her name," even if the impostor only had access to the victim's non-financial information. These substantial risks of harm exist, according to the circuit court, "simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."

Ransomware and Other Cyberattacks

As expected, the amount and types of cyberattacks showed no signs of slowing down in 2017, a trend we expect will continue into 2018 and beyond as regulators also took note of this development. For example, in May 2017, the Office of Compliance Inspections and Examinations, the arm of the SEC charged with monitoring risks and improving compliance among market participants through the agency's National Exam Program, released a cybersecurity risk alert in the wake of the widespread "WannaCry" ransomware attacks that had affected organizations in over 100 countries in the preceding days. The alert highlights certain deficiencies in cybersecurity practices across financial firms (as identified in recent examinations) and identifies risk management considerations in order to encourage market participants to strengthen cybersecurity preparedness across the industry. We expect regulators to continue to be proactive in this area as global attacks such as "WannaCry" proliferate.

New FTC Approach to Privacy?

The appointment of Joe Simons to chair the FTC, replacing Edith Ramirez, suggests that the FTC may be limiting its enforcement activity against companies that may have misused personal data. For example, when the FTC and the New Jersey Attorney General's Office settled a privacy action against Vizio, Inc. regarding the company's practice of gathering television viewing data from certain users of its smart TVs, then Acting FTC Chairwoman Maureen K. Olhausen reiterated that the FTC's enforcement actions in the privacy area should be grounded in whether "substantial injury" to consumers is likely to occur, a higher standard than the FTC applied under Chairwoman Ramirez. As such, Simons' appointment signifies that relying on this standard may limit the number of privacy cases brought by the FTC under the Trump administration.

Return to Table of Contents

Contacts in the Cybersecurity and Privacy Group

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
213.687.5381
david.eisman@skadden.com

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

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

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

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

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

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

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

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

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

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@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

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

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

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

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