Skadden

Privacy & Cybersecurity Update

1 First EU-US Privacy Shield Review Signals Support for the Privacy Framework

2 FTC Brings Actions Against Companies for Violating the Privacy Shield

3 Ninth Circuit Affirms Google's *Cy Pres* Privacy Settlement

4 Eighth Circuit Weighs in on *Spokeo*'s Effects on Standing in Data Breach Cases

5 Illinois District Court Decision Applies Expansive View of the State's Biometric Law

6 European Court Rules on EU Employee Rights of Privacy in Workplace Emails

7 UK Government-Backed Terrorism Reinsurer to Cover Cyberterrorism

First EU-US Privacy Shield Review Signals Support for the Privacy Framework

The first annual review of the EU-U.S. Privacy Shield resulted in a short but supportive statement by U.S. and EU regulators regarding the program.

Privacy Shield Review

On September 18 and 19, 2017, U.S. and European Union (EU) officials conducted the first official review of the EU-U.S. Privacy Shield Framework, a mechanism that allows for transborder data flow from the EU and the European Economic Area (EEA) to the United States under the EU Data Directive. This joint review is required on an annual basis under the Privacy Shield. Following the review, EU Justice Commissioner Vera Jourová and U.S. Secretary of Commerce Wilbur Ross issued a joint press statement summarizing the nature of the review, stating that the "Privacy Shield raised the bar for transatlantic data protection by ensuring that participating companies and relevant public authorities provide a high level of data protection for EU individuals."[1] This fairly benign pronouncement put at ease a number of companies and Privacy Shield proponents who were concerned about the potential of a much harsher statement from EU officials.

Background on the Current Privacy Framework

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 EEA member states — Norway, Liechtenstein and Iceland — to the U.S.[2] Under the EU Data Protection Directive, personal data about EU citizens can only be transferred to countries with "adequate" data protection laws

[1] For the full text of the press statement, see here.

[2] For more detailed information about the Privacy Shield and its specific obligations on companies, see our July 2016 *Privacy and Cybersecurity Update*.

in place. Notably, only a few countries satisfy this standard, and the U.S. is not one of them. However, under the Privacy Shield Framework, 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 adequately protect the privacy of EU citizens, mainly due to the U.S. government's ability to access personal data for national security purposes.[3] 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*.[4]

Support for the Privacy Shield

The two-day review of the Privacy Shield, which took place in Washington, D.C., marked the first opportunity for U.S. and EU regulators to analyze its efficacy. As the review was underway, The Future of Privacy Forum, a think tank and privacy advocacy group, published a study of the 2,400 companies enrolled in the Privacy Shield program that highlighted the framework's positive impact on EU companies and employees. According to the study, 114 European-headquartered companies are active participants in the Privacy Shield Framework, many of which rely on the program to transfer data to U.S. subsidiaries and key vendors. In addition, nearly one-third of Privacy Shield companies use the program to transfer and process human resources data. The Future of Privacy Forum also pointed out that the termination of the Privacy Shield could harm employees and possibly lead to reduced global hiring by U.S. companies.[5]

The joint press release issued by Commerce Secretary Ross and the European Commission indicates that there will be continued official support for the Privacy Shield. According to the statement, the "review examined all aspects of the administration and enforcement of the Privacy Shield, including commercial and national-security related matters." The statement concludes by stating that the U.S. and EU "share an interest in the framework's success and remain committed to continued collaboration to ensure it functions as intended."

Return to Table of Contents

FTC Brings Actions Against Companies for Violating the Privacy Shield

The Federal Trade Commission (FTC) brought actions against three companies for erroneously claiming they were Privacy Shield-certified, possibly signaling increased FTC enforcement in this area.

A major criticism from the EU regarding the U.S.-EU Safe Harbor Framework was that the FTC was lax in its enforcement of that agreement. Recently, some privacy advocates have noted that the FTC seemed to have taken a similar approach with respect to the Privacy Shield. However, this month the FTC brought actions against three companies for falsely claiming to be certified to the Privacy Shield. But it remains to be seen whether this signals future FTC enforcement in this area or if the agency simply wanted to bring actions prior to the Privacy Shield review (see preceding article).

The FTC Enforcement Actions

On September 8, 2017, the FTC initiated three separate enforcement actions, the first since the Privacy Shield's inception. Previous actions under the Safe Harbor program tended to address companies' noncompliance with annual self-certification, such as an August 2015 settlement with 13 companies that were alleged to have violated the FTC Act by falsely claiming to have current certifications. In contrast, the new actions under the Privacy Shield emphasize how each company misrepresented initial Privacy Shield compliance.

The actions targeted three companies' allegedly false claims concerning their respective Privacy Shield participations. The companies — Decusoft, LLC, a New Jersey software company; Tru Communication, Inc., a California printing corporation; and Md7, LLC a California company that assists with wireless companies' real estate dealings — were alleged to have disseminated false and misleading privacy policies and statements. The FTC complaints against the three companies alleged they

[3] For a description of the Court of Justice's decision in *Schrems v. Data Protection Commissioner*, see our *Privacy and Cybersecurity Update* from October 7, 2015.

[4] For more information regarding criticism of the Privacy Shield, see our April 2017 *Privacy and Cybersecurity Update*.

[5] See additional details about the study's results and methodology.

had violated Section 5(a) of the FTC Act by falsely representing themselves as participants in the EU-U.S. Privacy Shield Framework. Although the companies had initiated applications for Privacy Shield certification, they never completed the certification process. The FTC complaints found these companies' Privacy Shield compliance claims to constitute false and deceptive acts or practices. All three have received proposed settlement orders from the FTC.

Key Takeaway

The FTC has instructed companies to remove any false Privacy Shield claims from public documents until they complete the self-certification process, and has stated that the agency will be more vigilant and proactive in ensuring Privacy Shield compliance.

Return to Table of Contents

Ninth Circuit Affirms Google's *Cy Pres* Privacy Settlement

In *In re Google Referrer Header Privacy Litigation*, the U.S. Court of Appeals for the Ninth Circuit approved a $8.5 million *cy pres* class action settlement of privacy claims against Google, Inc., where nearly all the money went to the plaintiffs' lawyers and charitable organizations. The decision marks a notable departure from other courts that have become increasingly wary of *cy pres* awards.

On August 22, 2017, the U.S. Court of Appeals for the Ninth Circuit approved Google's $8.5 million class action settlement stemming from the privacy claims of three Google search users who challenged the company's practice of disclosing users' search terms to third-party websites. A split panel of the Ninth Circuit approved the *cy pres* award — in which nearly all the money went to plaintiffs' lawyers and charitable organizations — despite the objections of class members that Google and the plaintiffs' lawyers had prior relationships with many of the charitable groups. The *cy pres* doctrine permits a court to distribute unclaimed or non-distributable portions of a class action settlement fund to the "next best" class of beneficiaries for the indirect benefit of the class. Although courts frequently award damages to *cy pres* charitable groups that represent the interests of plaintiffs, courts have become increasingly wary of such awards because of the potential for abuse and lack of benefit to consumers. As such, the Ninth Circuit's decision cuts against this trend.

Background and Claims

In October 2010, three Google search users sued Google in the U.S. District Court for the Northern District of California, claiming the company's practice of disclosing users' search terms to third-party websites without their knowledge or permission violated Google's privacy policy, in addition to federal privacy law and California law. The plaintiffs alleged that as part of the "referrer header" information Google shared with owners of third-party websites, the company also included the URL of the last website a user visited before clicking into the current website. As a result, when the last website a user visited was a Google search results page, the user's private search terms were embedded within the URL that then became available to the owners of third-party websites.

In March 2014, the district court preliminarily approved a *cy pres* settlement between the parties in which Google agreed to pay $8.5 million: $3.2 million for attorney fees, incentive payments to the named plaintiffs and administrative costs, and the remaining $5.3 million to six *cy pres* nonprofit recipients that promised to use the funds to promote internet privacy protections. The recipients included AARP, Carnegie Mellon University, Chicago-Kent College of Law, Harvard University, Stanford University and the World Privacy Forum. As part of the settlement, Google also agreed to inform its users about how search terms are shared with third parties.

Five members of the class objected, arguing the settlement was inappropriate because Google and its counsel had pre-existing relationships with the *cy pres* recipients. Specifically, Google had donated to several of the recipients, and the plaintiffs' counsel had attended three of the universities receiving awards. The five objectors also argued the settlement award should have instead been distributed to a large class through a random lottery. In March 2015, the district court rejected these arguments and approved the *cy pres* settlement,[6] which the objectors appealed.

[6] See *In re Google Referrer Header Privacy Litig.*, 87 F. Supp. 3d 1122 (N.D. Cal. 2015).

The Ninth Circuit's Ruling

In a 2-1 decision, the Ninth Circuit panel held the district court had not abused its discretion and the settlement agreement was appropriate. The court determined that the settlement fund could not have been distributed as the objectors proposed because, after attorneys' fees and other costs, the remaining settlement fund was only $5.3 million, which could not be distributed to an estimated 129 million class members. The class members would each recover only a *de minimis* amount of money and the cost of sending such small payments would exceed the benefit obtained by the class.

The court also dismissed concerns about Google's and the plaintiffs' lawyers' pre-existing relationships with the *cy pres* recipients. The court wrote that district courts should consider a number of factors in determining whether a *cy pres* recipient is appropriate, including the nature of the relationship between the recipient and the parties, the timing of the relationship, the merits of the recipient and the circumstances of the selection process. The court held that there was no allegation of fraud or collusion between the recipients and the parties, and the universe of qualified recipients was small, noting that "[g]iven the burgeoning importance of internet privacy, it is no surprise that Google has chosen to support the programs and research of recognized academic institutes and nonprofit organizations."

Additionally, the court stated that the argument that the settlement is "taint[ed]" because the plaintiffs' lawyers were alumni of universities that received awards under the settlement "can't be entertained with a straight face." The court held that class counsel had no ongoing relationships with their alma maters. However, Judge John Wallace dissented on this issue. He noted that courts should carefully scrutinize any *cy pres* awards to the plaintiffs' counsel's alma maters, such as by holding an evidentiary hearing. Judge Wallace believed that such connections raise red flags about the appropriateness of *cy pres* awards.

Key Takeaway

Cy pres settlement awards are a mechanism used in privacy class actions to indirectly benefit class members when a class settlement includes unclaimed or undistributed funds. Such awards are generally the exception, rather than the rule. Courts have become increasingly wary of *cy pres* awards because they may fail to provide a benefit to harmed consumers and have the potential for abuse. However, the court's decision in *In re Google Referrer Header Privacy Litigation* sends a clear message that such awards are not viewed with disfavor in the Ninth Circuit.

Return to Table of Contents

Eighth Circuit Weighs in on *Spokeo*'s Effects on Standing in Data Breach Cases

In a pair of decisions[7] delivered nine days apart, the Eighth Circuit joined the Second, Fourth, Sixth, Seventh and D.C. Circuits in applying *Spokeo, Inc. v. Robins*[8] in data breach cases, deepening the growing divide among the circuits regarding how to satisfy *Spokeo*'s standing requirements.

The Courts' Rulings

In *Kuhns v. Scottrade*, which stemmed from the theft of more than 4.6 million Scottrade customers' personally identifiable information (PII), the panel addressed whether a plaintiff's claim that he overpaid for security services confers Article III standing. Plaintiff Matthew Kuhns alleged that his contract with Scottrade included a promise to provide security services to protect his PII. By failing to provide adequate security, he argued, the company breached the contract and caused him to overpay for services that were not provided. This failure, the court held, resulted in an actual injury to Kuhns: the diminution of the value of his bargain. Although the court subsequently dismissed the case for failing to state a claim, it held that the allegations demonstrated a sufficiently concrete harm to secure Article III standing.

By contrast, in *In re SuperValu, Inc., Consumer Data Security Breach Litigation*, which involved the theft of thousands of customers' credit card information from SuperValu and Albertsons grocery stores, the panel found that the threat of fraud from the breach of credit card information fell short of the standing requirements. These claims, the court held, did not meet *Spokeo*'s requirements that an injury be "concrete and particularized and actual or imminent."[9] The court, following similar precedent from the Second and Fourth Circuits,[10] held that the mere theft of a consumer's credit card information without more information, such as actual evidence of fraudulent charges, did not create a case or controversy under Article III.

[7] The opinions and orders may be found here and here.

[8] 136 S. Ct. 1540 (2016).

[9] *Spokeo, Inc.*, 136 S. Ct. at 1548.

[10] See *e.g.*, *Beck v. McDonald*, 848 F.3d 262, 274–75 (4th Cir.), cert. denied sub nom. *Beck v. Shulkin*, 137 S. Ct. 2307 (2017) (holding that the threat of identity theft from a breach at a hospital was too speculative to constitute an injury in fact); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 91 (2d Cir. 2017) (holding that plaintiff's risk of future identify fraud from the theft of her credit card information did not rise to the level of an injury in fact).

Notably, the *SuperValu* panel cited the several out-of-circuit cases that came "to differing conclusions" on whether an increased risk of future identity theft constitutes an injury in fact. The panel declined to "reconcile" this precedent, concluding instead that the specific facts before the court dictated the outcome. In particular, the panel focused on the fact that the data breach at issue involved only credit card information and not stolen personal information that could be used for identify theft or medical harm.[11] Consequently, the court held that only those plaintiffs who had actually suffered fraudulent charges on their accounts could assert Article III standing.

Key Takeaways

Despite the suggestion that no case directly conflicted with its holding, the Eighth Circuit's opinion in *SuperValu* stands in tension with Seventh Circuit precedent. In a pair of pre-*Spokeo* cases, the Seventh Circuit held that a breach involving credit card information alone creates an actionable injury.[12] Although it remains unclear whether the two cases remain good law in light of *Spokeo*, the circuits remain split about how to assess the actual risk of identity theft in a given case.

At the same time, in *Scottrade*, the Eighth Circuit demonstrated its willingness to find standing where plaintiffs can point to an actual contract underlying their data breach claim. When companies promise a certain level of security in their contracts with customers — even if the value of that security would otherwise appear *de minimis* — courts appear willing to hold them at their word. Thus, in light of *Scottrade*, companies should carefully review their contacts with customers to ensure their security measures comply with their promises.

The divergent analysis, and the growing circuit split over how to plead an actionable injury following a data breach, illustrate the continuing difficulty courts at all levels have had interpreting and applying *Spokeo*. As courts continue to wrestle with these issues, it seems ever more likely the Supreme Court may weigh in on the subject again soon.

Return to Table of Contents

[11] See *e.g.*, *Attias v. CareFirst, Inc.*, __ F.3d __ (D.C. Cir. August 1, 2017).

[12] *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690 (7th Cir. 2015).

Illinois District Court Decision Applies Expansive View of the State's Biometric Law

On September 15, 2017, an Illinois district court denied a motion to dismiss a putative class action that accused Shutterfly, Inc. (Shutterfly) of violating the Illinois Biometric Information Privacy Act (BIPA) by storing facial geometry scans, holding that BIPA covers biometric data derived from photographs and does not require consumers to allege actual damages.[13]

Background

The plaintiff, Alejandro Monroy, alleged that Shutterfly collected and stored his biometric information without his consent, in violation of BIPA. Monroy had never used Shutterfly's services, but a friend of his uploaded a photograph and tagged him in it. When a photo is uploaded to its website, Shutterfly creates a map of the person's face and stores the template in its database. Monroy alleged that a template of his face was created and stored without his consent, in violation of the statute.

BIPA requires private entities to obtain written consent prior to collecting, capturing or otherwise obtaining certain kinds of biometric data, including retinal scans, fingerprints and facial geometry scans. Under BIPA, companies also must notify individuals if they gather biometric data and develop publicly available written guidelines for permanently destroying such data within a specific time period. Companies also are prohibited from collecting and storing a person's biometric data without first obtaining an executed written release.[14]

Shutterfly filed a motion to dismiss the class action complaint, arguing that (1) BIPA applies only to facial scans or face prints derived from in-person scans, not photographs; (2) the suit requires an impermissible extraterritorial application of the statute; and (3) Monroy had not pled actual damages, as required by the statute.

[13] A copy of the decision is available here.

[14] The text of BIPA may be found here.

The Court's Decision

The court first examined Shutterfly's contention that BIPA applies only to in-person facial scans and not data extracted from a photograph. The statute expressly excludes photographs from the definition of "biometric information," and the definition of "biometric identifier" (which includes retina or iris scans, fingerprints, voiceprints, face or hand geometry scans, and biometric information) excludes "information derived from items or procedures excluded under the definition of 'biometric identifiers.'" Shutterfly argued that biometric data obtained from photographs was thus outside the scope of BIPA. The court noted that, "[t]his reading of the statute seems sensible enough at first blush, but it begins to unravel under scrutiny," however it pointed to earlier BIPA cases involving Google and Facebook that rejected this argument. The court also noted that there was no textual support for Shutterfly's contention that a "scan of face geometry" could only mean an in-person scan. Rejecting Shutterfly's argument that the other terms included in the definition of "biometric identifier" (*e.g.*, retina or iris scans, fingerprints, voiceprints and hand scans) all involved in-person processes, the court pointed out that both fingerprints and retinal scans can be obtained from images or photographs. Additionally, the decision notes that legislators "clearly sought to define the term 'biometric identifier' with a great deal of specificity… [i]f the legislature had intended a 'scan of face geometry' to refer only to scans taken of an individual's actual face, it is reasonable to think that it would have signaled this more explicitly." Furthermore, Shutterfly's interpretation would "leave little room for the law to adapt and respond to technological development."

The court also rejected Shutterfly's position that the plaintiff's complaint should be dismissed because the suit would require the court to apply the statute extraterritorially or in a way that would violate the U.S. Constitution's dormant commerce clause. With regards to the extraterritorial issue, the court noted that it was unable at this juncture to determine whether the circumstances of the plaintiff's claim occurred "primarily and substantially in Illinois" without a fuller understanding of how the Shutterfly facial recognition technology operates (*e.g.*, where the actual scan of Monroy's face geometry took place and where the scan was stored). The court also found that at this time there was no basis for concluding that applying BIPA in this case would entail control over out-of-state conduct in violation of the dormant commerce clause (as the suit and the class are confined to individuals whose biometric data was obtained from photographs uploaded to the Shutterfly website from Illinois and applying the statute would not entail regulation of Shutterfly's collection or storage of biometric data outside the state). However, the decision notes that upon further development of the factual record and a better understanding of how Shutterfly's technology works, it is conceivable that this conclusion might change.

Finally, the court decision rejected Shutterfly's contention that Monroy failed to allege actual damages as required under BIPA. The court noted that while the question was a "close one," a showing of actual damages is not necessary in order to state a claim under BIPA. The language in BIPA, while not defining actual damages, allows plaintiffs to recover the greater of either liquidated damages or actual damages. The court concluded that a showing of actual damages was therefore not required.

Additionally, although the issue of Article III standing was not raised by Shutterfly in its pleadings, the court noted in a footnote that Monroy had adequately alleged injury-in-fact under *Spokeo*[15] by credibly alleging that Shutterfly violated his right to privacy. The decision distinguished other BIPA cases where courts had found no standing because unlike the plaintiffs in those cases, Monroy had not voluntarily provided or consented to provide his biometric information to Shutterfly.

Key Takeaways

The court's ruling highlights the privacy concerns surrounding facial recognition software and suggests that the broadly drafted BIPA could create issues for companies that collect or store biometric information in the state of Illinois. The court's expansive view on damages and standing also might pave the way for additional suits. In addition to BIPA, Texas and Washington each have biometric privacy laws. We expect that as technologies utilizing biometric information increase, we are likely to see a growing number of state, or even federal laws.

Return to Table of Contents

European Court Rules on EU Employee Rights of Privacy in Workplace Emails

A European human rights court overruled an earlier decision involving the privacy rights of an employee in the workplace, finding that the original court had not struck a fair balance between the employer's interest in enforcing its IT policy and the employee's interests.

On September 5, 2017, the Grand Chamber of the European Court of Human Rights (ECHR) found on appeal in *Barbulescu v. Romania* that a Romanian employer had violated an employee's right to privacy, pursuant to Article 8 European Convention of Human Rights (Article 8), when it monitored personal messages sent on his work-related Yahoo Messenger account. In

[15] Further background on the *Spokeo* case can be found in our May 2016 *Privacy & Cybersecurity Update*. A copy of the decision is available here.

doing so, the ECHR overruled an earlier decision[16] which ruled that the employer's actions in the context of disciplinary proceedings had been a proportionate interference with his rights.

The employee, Bogdan Barbulescu, had been dismissed for inappropriate internet use at work in breach of his employer's IT policy. When investigating the employee's internet use, the employer had discovered private exchanges with the employee's family and fiancée on a Yahoo Messenger account. The employee, a sales engineer, had been encouraged to use the account to deal with customer enquiries.

The ECHR ruled that monitoring employees' communications is not inevitably in breach of the Article 8 right to privacy, but that organizations should take a number of factors into account before they do so. In particular:

- internet messaging is a form of "correspondence" and therefore within the ambit of Article 8;
- there is a distinction between monitoring use of an employer's systems and the extent of communication versus the content of that communication;
- employers need a legitimate reason to justify monitoring communications;
- whether it is possible to use less-intrusive methods to obtain the information required — this had not been considered in this case;
- employers should ensure that clear and explicit advance notice is given before employee communications are monitored. In this case the employer's IT policy alluded to the fact that communications could be monitored, but did not explicitly state that the content of the communications might be reviewed or give notice of the nature and extent of the monitoring that in fact took place. This was a key factor in the ECHR's decision; and
- the potential damage to the employee (here, the employee's dismissal).

Key Takeaway

The ECHR focused on the requirement of domestic authorities in Europe (in this case the Romanian court) to ensure that measures introduced to monitor correspondence include adequate safeguards to prevent an abuse of employee privacy. The original court had not struck a fair balance between the employer's interest in enforcing its IT policy and the employee's interests.

Return to Table of Contents

[16] See our January 2016 *Privacy & Cybersecurity Update* for our discussion of this case.

UK Government-Backed Terrorism Reinsurer to Cover Cyberterrorism

The British government recently granted government-backed terrorism reinsurer Pool Reinsurance Company Limited tentative permission to move forward with its plan to extend coverage to physical losses caused by cyberterrorism.

According to several news outlets, the British government-backed terrorism reinsurer Pool Reinsurance Company Limited (Pool Re) has reached an agreement in principle with the U.K. Treasury to cover physical damage resulting from cyberterrorism, a major step towards combatting the evolving threat of terrorism and closing the terrorism insurance coverage gap.

About Pool Re

Pool Re was established in 1993 in cooperation with the British government following the 1992 bombing of London's Baltic Exchange by the Irish Republican Army (IRA) and a series of other terrorism incidents in England related to the situation in Northern Ireland at the time. The formation of Pool Re became necessary because of the significant costs of these terrorist incidents and the lack of a reliable method to estimate future loss experience, which led reinsurers to withdraw from the U.K. terrorism coverage market.

Pool Re, which currently underwrites more than £2 trillion ($2.7 trillion) of exposure in commercial property to terrorism risks across the U.K. mainland, covers loss resulting from an "Act of Terrorism," as defined in the enabling Act of Parliament, the Reinsurance (Acts of Terrorism) Act of 1993. Pool Re is owned by its members — which comprise the vast majority of U.K. commercial property insurers — but is secured by a commitment from Her Majesty's Treasury to step in and pay legitimate claims in the event that Pool Re is without sufficient resources to do so. Pool Re pays a premium to the treasury for this backstop and must repay all money loaned to pay claims.

Since its inception, Pool Re has been involved in claims arising from 13 terrorism incidents and has covered more than £600 million ($810 million) in losses without seeking recourse from U.K. taxpayers. The single-largest payout was £262 million ($353 million) in connection with the 1993 IRA bombing of Bishopsgate in London.

Pool Re's Expansion to Cyberterrorism Coverage

The contemplated expansion of the Pool Re scheme to cover physical damage caused by cyber perils will mark the first major change to the scheme in roughly 15 years. Initially, the Pool Re scheme was limited to providing coverage for property damage and business interruption arising from fire and explosion that was proximately caused by an act of terrorism. It was unnecessary at the time for Pool Re to provide broader coverage because commercial reinsurers were still willing to reinsure other types of terrorism risks.

However, following the attacks of September 11, 2001, commercial reinsurers were no longer in a position to cover terrorism risks, and it became necessary to expand the Pool Re scheme. Accordingly, the Pool Re scheme was broadened to provide terrorism coverage on an "all risks" basis and a then-existing exclusion for chemical, biological, radiological and nuclear terrorism was deleted. The scheme continued to exclude coverage for cyberterrorism.

Recognizing that terrorism has evolved to include cyberthreats, and that such threats can cause physical damage, Pool Re initiated talks with the U.K. government approximately two years ago with the goal of expanding the Pool Re scheme to include incidents of cyberterrorism. The contemplated expansion of the Pool Re scheme will amend the cyberterrorism exclusion such that coverage for physical damage caused by cyberterrorism, such as remote digital interference by terrorists, will be available to Pool Re's members. It is unclear whether the new Pool Re scheme also will cover business interruption resulting from physical damages caused by cyberterrorism.

According to reports, Pool Re is working on final details with the U.K. government, with a goal of issuing underwriting guidelines by the end of September 2017. Pool Re's members will then have until April 2018 to implement the new cyber-related guidelines into their insurance policies.

Key Takeaway

While Pool Re is working on closing other terrorism coverage gaps — most notably, the non-physical damage business interruption coverage gap — the addition of coverage for cyberterrorism losses will be a significant coverage enhancement and should go a long way to protecting businesses in the wake of a cyberterrorism attack.

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