Skadden

Privacy & Cybersecurity Update

1 European Commission Publishes Second Annual Review of EU-US Privacy Shield

2 Department of Commerce Addresses Impact of Brexit on the Privacy Shield

2 Conference Adopts Declaration on Ethics and Data Protection in Artificial Intelligence

4 Annual Joint Review of the EU-US Privacy Shield Reveals Few Complaints From European Data Subjects

5 Company Seeks Coverage From Property Insurer for $100 Million Loss Resulting From Malware Attack

6 Financial Stability Board Publishes New Standardized Lexicon to Help Mitigate Cyber Threats

European Commission Publishes Second Annual Review of EU-US Privacy Shield

The European Commission's second annual report on the EU-U.S. Privacy Shield (Privacy Shield) featured a generally positive review of the transborder data flow program.

As 2018 drew to a close, the European Commission issued its second annual review of the performance of the 2016 EU-U.S. Privacy Shield, the negotiated framework that allows U.S. companies who have self-certified to import data from the European Economic Area (EEA) in compliance with European data protection laws.[1]

The report was generally very positive, with the commission noting that the Privacy Shield continues to ensure an adequate level of protection for personal data transferred from the EEA to Privacy Shield-compliant companies in the U.S. The commission also noted that the U.S. had taken steps in 2018 to address recommendations made by the commission in its 2017 report, such as having the Department of Commerce conduct compliance "spot checks" and look for false claims of compliance.

The commission also praised the Federal Trade Commission (FTC) for taking a more proactive approach to enforcement, including by issuing administrative subpoenas to request information from self-certifying companies.

The commission also noted that it expects the U.S. to nominate a permanent ombudsperson by the end of February 2019 to replace the current acting ombudsperson. Under the Privacy Shield, the ombudsperson is responsible for ensuring that complaints regarding access to personal data by U.S. authorities are addressed.

Key Takeaways

Although many privacy advocates have criticized the Privacy Shield as inadequate, arguing that U.S. enforcement is weak, the commission's second annual review provides an important endorsement of the Privacy Shield. The commission encouraged the U.S. to adopt a comprehensive data protection law, an issue that is likely to garner significant attention in 2019.

[1] The text of the report can be found here.

Department of Commerce Addresses Impact of Brexit on the Privacy Shield

The Department of Commerce has added a new Frequently Asked Questions section to its Privacy Shield site to address the impact of Brexit.

The Department of Commerce has provided companies who self-certify to the Privacy Shield with some guidance on how to handle United Kingdom-based data in light of the U.K.'s intended withdrawal from the European Union on March 29, 2019, commonly referred to as Brexit. Given the general uncertainty surrounding Brexit, the agency outlined two potential scenarios:

- **Scenario (1) "Transition Period":** The U.K. and EU preliminarily have agreed that there will be a transition period from March 30, 2019, to December 31, 2020, during which EU law, including EU data protection law, will continue to apply in the U.K. During this period, the Privacy Shield will continue to apply to data transfers from the U.K. to U.S. Privacy Shield participants. No additional action will be required of Privacy Shield participants during this period, although companies should begin to implement plans for the post transition period outlined below.
- **Scenario (2) "No Transition Period":** If there is no transition period, then the steps outlined below need to be in place by March 29, 2019 (assuming no delay in the Brexit date).

Steps that will be required to import U.K. data under the Privacy Shield:

- All public commitments regarding the Privacy Shield explicitly must state that personal data received from the U.K. is in reliance on the Privacy Shield. Human resource policies also must be updated if HR data is imported from the U.K. in reliance on the Privacy Shield. Through this commitment, a company participating in the Privacy Shield will be ruled to have complied with the U.K. Information Commissioner's Office with regard to personal data received from the U.K. in reliance on Privacy Shield. The Department of Commerce has provided the following model language:

  (INSERT your organization name) complies with the (INSERT EU-U.S. Privacy Shield Framework [and the Swiss-U.S. Privacy Shield Framework(s)]) (Privacy Shield) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the (INSERT European Union ***and the United Kingdom*** *and/or Switzerland, as applicable) to the United States in reliance on Privacy Shield. (INSERT your organization name) has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.*
- Unchanged from current requirements, organizations must continue to maintain a current Privacy Shield certification, recertifying annually.

Return to Table of Contents

Conference Adopts Declaration on Ethics and Data Protection in Artificial Intelligence

A group of data protection commissioners issued an edict outlining measures to preserve human rights as the development of artificial intelligence (AI) technology becomes more prevalent.

On October 23, 2018, the 40th International Conference of Data Protection and Privacy Commissioners (the conference) adopted the Declaration on Ethics and Data Protection in Artificial Intelligence (the declaration).[2] The declaration endorses six guiding principles to ensure the protection of human rights in conjunction with the development of AI. The conference also established a permanent working group on Ethics and Data Protection in AI, which will be in charge of setting common governance principles on AI at an international level.

[2] The Declaration on Ethics and Data Protection in Artificial Intelligence can be read here.

Background

The declaration was written by the European Union's independent data protection authority (the European Data Protection Supervisor, or EDPS), the French and Italian national supervisory authorities (the French Commission Nationale de l'Informatique et des Libertés and the Italian Garante per la protezione dei dati personali) and was sponsored by another 14 privacy regulators worldwide.

The announcement at the conference triggered an official public discussion on digital ethics and its place in regulating the use of AI.

Human Rights and Artificial Intelligence

The declaration recognizes the significant benefits that AI may have for society while also highlighting the corresponding risks. It acknowledges that the rights to privacy and data protection are increasingly challenged by the rapid development of AI and that the collection of personal information has the potential to impact human rights more broadly, most notably involving the right to not be discriminated against and the right to freedom of expression and information.

One example of this direct impact is that AI systems have been found to contain "inherent bias." This can occur as a result of the initial configuration of AI models, which may not include an exhaustive or representative list of parameters or use cases, and may accordingly generate prejudiced results. As such, this may lead to unfair discrimination against certain individuals or groups in areas such as credit scoring by potentially restricting the availability of certain services or content.

The Six Guiding Principles Endorsed by the Conference

The principles outlined by the declaration are:

1. AI and machine learning technologies should be designed, developed and used in respect of fundamental human rights and in accordance with the fairness principle. The conference suggested this might be achieved by considering the collective impact that the use of AI may have, and ensuring that systems adhere to their original purposes, while making certain that the data they generate is used in a way that is compatible with such original purposes.
2. There should be continued attention and vigilance through actions such as promoting accountability of all relevant stakeholders. The principle encourages documented governance structures and processes to ensure collective and joint responsibility involving the whole chain of stakeholders at the outset of any AI project.
3. Improvement in the transparency and intelligibility of AI systems remains necessary. For example, by providing adequate information on purpose and effects of such systems, individual users of the technology can manage their expectations and increase their level of control over AI systems.
4. An "ethics by design" approach should be adapted, focusing on responsible design and fair use of AI systems, thereby implementing the newly codified principles of "data protection by design and by default" set out in the General Data Protection Regulation (the GDPR).
5. Echoing the greater transparency requirements set out in the GDPR, empowerment of every individual should be promoted, which can be achieved through communicating information and ensuring that individuals are aware of their rights. In the context of AI solutions, which may be relying on solely automated decision-making processes, individuals can exercise their right to challenge any such decision in line with GDPR requirements.
6. Unlawful biases or discriminations that may result from the use of data in AI should be reduced or mitigated, including by issuing specific guidance to acknowledge and address any such bias or discrimination-related issues.

Overall, the six principles aim to promote a use of AI that is fair and transparent, and to ensure greater accountability for failure to meet this standard, in compliance with the principles applicable to the processing of personal data under the GDPR.

Going Forward

The conference also established a permanent working group on Ethics and Data Protection in Artificial Intelligence, which will promote understanding and respect for the six guiding principles and encourage the establishment of international principles on AI. In this vein, the conference calls for common governance principles on AI that, due to the breadth of issues raised by the widespread use of AI worldwide, only can be achieved on the basis of concerted cross-sectoral and multi-disciplinary efforts.

The declaration, which was authored by two EU supervisory authorities and the EDPS and featured the United Kingdom's Information Commissioner's Office as a co-sponsor, is likely to be an ongoing focus in the EU. The declaration also has been endorsed by 42 organizations and 185 individuals, many of whom are non-European, indicating that the intersection of ethics and AI is a topic of increasing concern worldwide.

Other parties also have signalled their interest in this area, including the European Commission, which revealed plans to draft its own ethical guidelines on AI in April 2018. In addition, a group of German data protection commissioners recently called for public bodies to ensure protections on algorithms and AI transparency.

Key Takeaways

Ethical considerations and data protection in AI is an area in which we are likely to see considerable development. The declaration also suggests a renewed focus by regulators on ethics. In light of recent scandals regarding certain uses of personal data, companies may now be expected to concentrate on ethics in addition to complying with applicable laws and regulations, including the GDPR. Areas such as AI, where statutory regulation may not be able to keep up with rapid technological development, may be particularly suited to regulation through ethical principles. Companies that use machine learning and AI should monitor the effects that the declaration (and other AI-focused regional or worldwide standards and practices) might have on their operations and compliance mechanisms.

Return to Table of Contents

Annual Joint Review of the EU-US Privacy Shield Reveals Few Complaints From European Data Subjects

In October 2018, officials including U.S. Secretary of Commerce Wilbur Ross and European Commissioner Vera Jourová met for the second annual joint review of the EU-U.S. Privacy Shield. This year's review revealed that few European data subjects have filed complaints with data protection authorities regarding noncompliance with the Privacy Shield.

Overview of the Privacy Shield

The Privacy Shield replaced the Safe Harbor Privacy Principles, which were invalidated by the European Court of Justice in 2015, and provides a mechanism for organizations to transfer personal data from the European Union and three EEA member states to the United States in accordance with EU data protection law. To transfer personal data of EU and EEA residents to the U.S. under the Privacy Shield, a company must self-certify to the U.S. Department of Commerce that it complies with the principles set forth in the Privacy Shield. If a company represents to the public that it complies with the Privacy Shield but fails to maintain compliance in practice, the U.S. Federal Trade Commission (FTC) may bring an enforcement action under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices.

The Privacy Shield sets forth dispute resolution mechanisms to resolve data protection-related complaints from data subjects. Among other requirements, organizations that self-certify under the Privacy Shield must respond to data subjects within 45 days of receiving a complaint and provide an independent recourse mechanism to investigate unresolved complaints at no cost to the data subject.

As reported in the July 2018 edition of our *Privacy & Cybersecurity Update*, in July the European Parliament passed a nonbinding resolution calling on the European Commission to suspend the Privacy Shield, citing the recent Cambridge Analytica scandal and certain failures by the Department of Commerce to enforce

certification requirements as evidence of the Privacy Shield's inadequacy as a data protection mechanism. In light of these and other criticisms of the Privacy Shield, the results of this year's review are being closely watched by data protection stakeholders.

Few Complaints Under the Privacy Shield

During this year's joint review, representatives from the Department of Commerce revealed that fewer than 40 complaints had been filed by European data subjects across all independent recourse mechanism providers in connection with the Privacy Shield. Although representatives from the EU raised questions regarding the procedures used by such independent recourse mechanism providers, the very limited number of complaints raised a more significant question as to whether European data subjects are utilizing the protections under the Privacy Shield at all. There is some speculation that European data subjects are simply not aware of, or are not inclined to use, the somewhat complex independent recourse mechanisms available to them under the Privacy Shield. It also is possible that most U.S. companies receiving data under the Privacy Shield do so as data processors, rather than data controllers. As such, if a data subject has a complaint about the use of his or her data, it is likely directed to the data controller with which the data subject may be more familiar.

Key Takeaways

The Privacy Shield remains one of the primary mechanisms by which companies can lawfully transfer personal data from the EU and EEA to the U.S. Although there have been only a few complaints filed by European data subjects, companies should bear in mind that the FTC can bring enforcement actions against companies that self-certify and then fail to comply with the Privacy Shield. The joint press statement issued by Secretary Ross and Commissioner Jourová regarding the review reiterated the Department of Commerce's commitment to revoking the certification of companies that do not comply with the Privacy Shield. The European Commission is expected to publish its conclusions drawn from the review by the end of the year. We will continue to monitor developments stemming from the official report when it is released.

Return to Table of Contents

Company Seeks Coverage From Property Insurer for $100 Million Loss Resulting From Malware Attack

Property insurer Zurich American Insurance Company (Zurich) is facing a new lawsuit by one of its policyholders, snack food company Mondelez International, Inc. (Mondelez), challenging Zurich's denial of coverage for losses resulting from the 2017 NotPetya malware attack.

On October 10, 2018, Mondelez filed a complaint against its property insurer Zurich in Cook County Circuit Court of Illinois alleging that Zurich wrongfully denied coverage, in reliance on the policy's "Hostile or Warlike Action" exclusion, for losses stemming from Mondelez's exposure to the 2017 malware attack commonly known as NotPetya.[3] U.S. intelligence officials later determined that the NotPetya malware initially was launched against Ukraine by the Russian military.

Malware Attack and Denial of Coverage

According to Mondelez's complaint, on June 27, 2017, the company fell victim to the NotPetya malware, which infected computer systems of many businesses around the world. The malware initially infected two of Mondelez's servers before spreading to other servers, stealing the credentials of numerous users and ultimately rendering approximately 1,700 of Mondelez's servers and 24,000 of its laptops "permanently dysfunctional." The complaint alleges that as a result of the malware attack, Mondelez suffered property damage, commercial supply and distribution disruptions, unfulfilled customer orders, reduced margins and other losses in excess of $100 million.

Prior to the malware attack, Zurich sold Mondelez a property insurance policy providing coverage for "all risks of physical loss or damage," including "physical loss or damage to electronic data, programs or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction." The policy also provides time element coverages for losses incurred during a defined period after the loss "resulting from the failure of the Insured's electronic data processing equipment or media to operate."

[3] *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-11008, complaint filed, 2018 WL 4941760 (Ill. Cir. Ct., Cook Cty., Oct. 10, 2018).

Mondelez alleges that it promptly notified Zurich of the loss under its property insurance policy.

According to the complaint, Zurich thereafter disclaimed coverage in reliance on the policy's "Hostile or Warlike Action" exclusion. That exclusion bars coverage for loss resulting from a "hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any: (i) government or sovereign power (*de jure or de facto*); (ii) military, naval, or air force; or (iii) agent or authority of any party specified in i or ii above." Zurich subsequently rescinded its disclaimer and committed to a $10 million partial payment toward the claim. However, after negotiations failed to resolve the claim, Zurich sent a final letter to Mondelez reasserting its disclaimer of coverage.

Mondelez Files Suit Against Zurich

Thereafter, Mondelez commenced a lawsuit against Zurich based on its alleged wrongful disclaimer of coverage for the malware attack. Mondelez alleged that the "Hostile or Warlike Action" exclusion was inapplicable because the malware attack did not constitute a "hostile or warlike action," nor was Mondelez's loss caused directly or indirectly by "hostile or warlike action." The company also claimed that such an exclusion has never been applied to a malicious cyber incident and invoking the exclusion for "anything other than conventional armed conflict" is unprecedented. In the alternative, Mondelez alleged that the exclusion is vague and ambiguous with respect to whether it extends to cyber incidents "and therefore must be interpreted in favor of coverage." Mondelez is seeking an award of damages in the amount of at least $100 million. As of publication of this *Privacy & Cybersecurity Update*, Zurich has not yet responded to the complaint.

Key Takeaways

Regardless of how this coverage dispute is resolved, this case illustrates that, depending on the circumstances and terms and conditions of a policy, traditional coverage lines, such as property insurance, may cover cybercrime and other cyber-related losses. This case also serves as an important reminder to insurers and insureds alike that it is vital to have a clear understanding of the scope of such coverage in their policies, including which exclusions may be implicated, taking into account that cyber-related losses, such as those suffered by many companies as a result of NotPetya, can stem from government-backed actions.

Return to Table of Contents

Financial Stability Board Publishes New Standardized Lexicon to Help Mitigate Cyber Threats

The Financial Stability Board (FSB) has issued a standardized lexicon of cybersecurity terms in an effort to encourage better communication and cooperation among financial institutions regarding cyber threats.

On November 12, 2018, the FSB, an international body focused on monitoring and making recommendations about global financial systems, published a "Cyber Lexicon" comprised of over 50 terms related to cybersecurity in the financial sector. With cyber incidents increasing for financial services firms, the lexicon is intended to ensure that stakeholders have a common terminology to reference cybersecurity matters. The FSB regards the Cyber Lexicon as a preventative measure to help combat a cybersecurity landscape that is increasingly risky for financial institutions, many of which have faced significant security incidents in the past several years. In connection with its issuance of the Cyber Lexicon, the FSB highlighted the 2016 attack on the Bangladesh Bank (which resulted in $81 million in losses), the 2017 WannaCry ransomware attack (which infected over 250,000 systems in over 150 countries) and the 2017 Equifax hack (which compromised the personal information of over 146 million individuals).

In issuing the Cyber Lexicon, the FSB noted that several factors have led to the increased exposure of financial firms, including evolving technologies, improved interconnections among firms and heavier reliance on cloud computing. Moreover, the FSB has pointed to the rising attractiveness of financial institutions as hacking targets and the lagging regulation of financial technology providers. Given the increasing complexity of the ways in which hackers are targeting financial institutions, the FSB and other regulators worldwide are looking for equally sophisticated measures to help mitigate cyber vulnerabilities facing financial firms.

The call for the Cyber Lexicon arose from several key meetings in 2017, including the FSB's meeting with finance ministers and central bank governors in Washington, D.C. and the G20 Finance Ministers and Central Bank Governors meeting in Baden-Baden, Germany. To help develop the standardized list of cyber terms, the FSB formed a working group of experts, which was chaired by the U.S. Federal Reserve Board and staffed by representatives from governmental authorities, private sector participants

and a collection of standard-setting bodies, including the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures, the International Association of Insurance Supervisors and the International Organization of Securities Commissions.

According to the FSB, the new Cyber Lexicon embodies four chief objectives, including:

1. creating a cross-sectoral common understanding of relevant cyber security and cyber resilience;
2. increasing the ability of the FSB to assess and monitor financial stability risks of cyber risk scenarios;
3. contributing to appropriate information sharing across jurisdictions; and
4. providing the FSB with the ability to provide guidance related to cybersecurity while reducing the risk of duplicative and potentially conflicting regulatory requirements.

The FSB's new Cyber Lexicon includes terms such as "cyber resilience," which is defined as the ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents, and "cyber risk," which is defined as the combination of the probability of cyber incidents occurring and their impact.

Key Takeaways

While the immediate goal of the Cyber Lexicon is to aid the work of the FSB, standard-setting bodies and governmental authorities, the lexicon also is aimed at private sector participants and financial institutions to create greater transparency in a sector that is facing increasingly complex cyber risks. The Cyber Lexicon, which was delivered at the G20 Leaders' Summit in Buenos Aires, Argentina, on November 30, 2018, signals that financial institutions should familiarize themselves with the Cyber Lexicon.

Return to Table of Contents

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
213.687.5381
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

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@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

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

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