Skadden

Privacy & Cybersecurity Update

New York Enacts Two Laws Expanding Consumer Protection for Data Breaches

On July 25, 2019, New York Gov. Andrew Cuomo signed two bills into law that enhance the rights of state residents in the event of a data breach.

New Yorkers will soon have increased rights if they find their personal information has been compromised. The Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)[1] expands the definition of personal information to which data breach reporting requirements apply and requires companies to use reasonable measures to protect private information. The second measure, known as the Identity Theft Prevention and Mitigation Services Act,[2] requires consumer credit reporting agencies that suffer a data breach involving Social Security numbers to provide five years of identity theft protection to affected consumers.

The SHIELD Act expands New York's current data breach notification law to add the following categories of information to the definition of "private information" to which notification requirements may apply in the event of a data breach:

- account number or credit or debit card number, in circumstances where such number could be used to access an individual's financial account without additional identifying information (*e.g.*, security code or password);
- biometric information; or
- user name or email address in combination with a password or security question and answer that would permit access to an online account.

The notification requirements now apply in the case of unauthorized access to private information in addition to cases where such information is acquired without authorization.

The SHIELD Act also expands the entities to which the data breach notifications apply. Under the prior version of the state's data breach notification law, any person or business that conducts business in New York and collects private information must notify any state residents whose private information was acquired in a data breach. Under the SHIELD Act, any person or business, regardless of where they conduct business, must

[1] A copy of the SHIELD Act may be found here.

[2] A copy of the Identity Theft Prevention and Mitigation Services Act may be found here.

notify affected New York residents in the event of a breach of such residents' private information, but the notice to affected residents is not required if:

- the exposure of private information was an inadvertent disclosure by persons authorized to access such information, and the entity reasonably determines such exposure will not likely result in the misuse of such information or harm to the affected state resident; such a determination must be documented and retained for five years, and if the incident affects over 500 state residents, the determination must be provided to the attorney general within 10 days after the determination; or
- notice of the security breach is made to affected New York residents pursuant to breach notification requirements under any other state or federal laws, including the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA).

Note that in the above cases, while notice to affected New York residents is not required, companies still must notify the state's attorney general, Department of State Division of Computer Protection and Division of State Police.

Finally, the SHIELD Act requires any person or business that maintains computerized private information of New York residents to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of such data, including its proper disposal. A person or business is deemed to be in compliance if it:

- is subject to, and in compliance with, the data security requirements under any other state or federal laws, including Gramm-Leach-Bliley and HIPAA; or
- implements a data security program that includes the following:
  - reasonable administrative safeguards, such as designating a security program coordinator; identifying reasonably foreseeable internal and external risks; assessing the sufficiency of safeguards to control such risks; training employees in the security program practices and procedures; selecting service providers capable of maintaining safeguards and requiring such safeguards by contract; and adjusting the security program in light of changes in circumstances;
  - reasonable technical safeguards, such as assessing risks in network and software design; assessing risks in information processing, transmission and storage; detecting, preventing and responding to attacks or system failures; and regularly testing and monitoring the effectiveness of key controls; and
  - reasonable physical safeguards, such as assessing risks of information storage and disposal; detecting, preventing and responding to intrusions; protecting against unauthorized access and use of private information; and disposing of private information within a reasonable amount of time after it is no longer needed by erasing electronic media.

Failure to comply with the data security provisions of the SHIELD Act may result in penalties assessed by the attorney general of up to $5,000 per violation. There is no private right of action.

The SHIELD Act takes effect on March 21, 2020.

Under the Identity Theft Prevention and Mitigation Services Act, any New York consumer credit reporting agency that experiences unauthorized acquisition of, or access to, a Social Security number must offer to each consumer whose number was breached, or is reasonably believed to have been breached, (1) reasonable identity theft prevention services and (2) if applicable, identity theft mitigation services, in each case for up to five years at no cost to the consumer, unless the agency determines after a reasonable investigation that the breach is unlikely to result in harm to the consumer.

The consumer credit reporting agency must provide all information necessary for consumers to enroll in such services, including information on how consumers can request a security freeze.

The Identity Theft Prevention and Mitigation Services Act takes effect 60 days from the date it was signed into law. It is applicable to any breach of the security systems of a consumer credit reporting agency that occurred within three years prior to the effective date.

Key Takeaways

Companies that collect personal information from New York residents should evaluate their data collection practices to determine whether they are subject to the new broader notification and data security requirements under the SHIELD Act and, if so,

begin implementing policies and procedures to be able to comply by March 21, 2020. In particular, companies subject to the data security requirements should determine whether their existing data security programs include the elements listed in the SHIELD Act and, if they do not, consider updating such programs to include any missing elements.

In addition, consumer credit reporting agencies should consider whether they have experienced data breaches within the past three years that are in violation of the Identity Theft Prevention and Mitigation Services Act, and take steps to prepare to offer identity theft prevention and mitigation services to affected consumers, as applicable.

Return to Table of Contents

Two DC Circuit Rulings Deepen Standing Split in Data Breach Cases

Two recent rulings in the D.C. Circuit held that increased risk of identity theft due to unauthorized disclosure of personal information may constitute an injury in fact, deepening the split between appellate courts on standing requirements in data privacy litigation.

On June 21, 2019, the D.C. Circuit decided in *National Treasury Employees Union v. Office of Personnel Management* that heightened risk of identity theft resulting from a cybersecurity breach is sufficient to establish standing at the pleading stage.[3] Shortly after, on July 2, 2019, the court held in *Jeffries v. Volume Services America Inc*. that a receipt printed by the defendant containing all 16 digits of a customer's credit card number in contravention of the Fair and Accurate Credit Transactions Act (FACTA) satisfied the plaintiff's standing requirement because the receipt in question increased the plaintiff's risk of falling victim to identity theft.[4] These decisions further deepen the divide between circuits on standing requirements in data breach cases that have been established by the Supreme Court in *Spokeo Inc. v. Robins*.

Background: Spokeo and the Circuit Split

In *Spokeo Inc. v. Robins*, the Supreme Court considered whether the Ninth Circuit properly granted the plaintiff standing against a "people search engine" that allegedly gathered and disseminated incorrect information about the plaintiff in violation of the Fair Credit Reporting Act. The Court vacated and remanded the decision because the Ninth Circuit only considered whether the injury in fact was "particularized" and failed to evaluate whether the injury was "concrete." While the Court stated that this requirement may be satisfied by a risk of real harm, it also stated that a plaintiff cannot satisfy the requirement by alleging a bare procedural violation.

Appellate courts have since split on how *Spokeo*'s concreteness requirement applies to data breach litigation. The Third, Sixth, Seventh and Ninth circuits have held that victims of data breaches can establish concreteness by showing a heightened risk of future misuse of their stolen information. The First, Second, Fourth and Eighth circuits have ruled that plaintiffs must show actual harm already has manifested. The courts' disagreements also have extended beyond cybersecurity failures to other forms of unauthorized disclosure. The Second, Third, Seventh and Ninth circuits have held that printing the first six digits of a credit card number on a receipt does not confer plaintiffs standing under FACTA, which prohibits merchants from printing "more than the last 5 digits of the card number ... upon any receipt provided to the cardholder." The Eleventh Circuit, however, has allowed plaintiffs to proceed with litigation after a merchant printed the first six and last four digits of customers' credit card numbers.

The DC Circuit On Data Breaches

In 2014, cyberattackers breached multiple U.S. Office of Personnel Management (OPM) databases, allegedly stealing the sensitive personal information — including birth dates, Social Security numbers, addresses and even fingerprint records — of more than 21 million past, present and prospective government workers.

In *National Treasury Employees Union v. Office of Personnel Management*, two consolidated complaints — one filed by the National Treasury Employees Union and three of its members, and another filed by the American Federation of Government Employees on behalf of several individual plaintiffs and a putative class

[3] The decision is available here.

[4] The decision is available here.

of others similarly affected by the breaches — alleged that OPM's cybersecurity practices were unlawfully inadequate. The district court dismissed both complaints for lack of Article III standing and failure to state a claim.

A three-judge panel on the D.C. Court of Appeals held both sets of plaintiffs cleared the "low bar" to establish standing at the pleading stage because the breach was "fairly traceable" to the defendant's cybersecurity practices and the stolen information left "no question that the OPM hackers ... have in their possession all the information needed to steal [plaintiffs'] identities." Indeed, some plaintiffs had suffered identity theft after the attack, supporting the inference that there was a "substantial — as opposed to a merely speculative or theoretical — risk of future identity theft."

While this holding ostensibly marks a split with the First, Second, Fourth and Eighth circuits, the D.C. Circuit distinguished one of these conflicting results. In *Beck v. McDonald*, the Fourth Circuit held that theft of a personal laptop and four boxes of pathology reports was too speculative to constitute an "injury in fact" because the plaintiffs failed to allege either that the thief "intentionally targeted" the information contained in the laptop or medical records, or that the information was subsequently used by the thief to commit identity theft. The D.C. Circuit pointed out that, in contrast to Beck, the plaintiffs in *National Treasury* alleged the intentional targeting of their information and subsequent misuse of that information. These allegations made the plaintiffs' claims comparatively concrete and were sufficient to establish standing in the context of a cybersecurity breach.

The DC Circuit On Credit Card Receipts

In *Jeffries et al. v. Volume Services America Inc. d/b/a Centerplate/NBSE et al*., Doris Jeffries alleged that Centerplate — a food and beverage company — provided her with a receipt containing all 16 digits of her credit card number, her credit card expiration date and her credit card provider. She claimed that she immediately recognized that the receipt contained her personal information and held onto it for safekeeping. She then filed a class action lawsuit against Centerplate alleging that the company violated FACTA, which contains a "truncation requirement" imposing liability on companies that willfully print more than five digits of the card number or the expiration date on a receipt. The district court granted Centerplate's motion to dismiss the case for lack of standing because Jeffries alleged that only she viewed the receipt containing her credit card information, making the harm hypothetical as opposed to *de facto*. In addition, the district court determined that the burden of safeguarding the receipt to prevent misuse of such information was not concrete enough to confer standing.

On appeal, the D.C. Circuit reversed the decision because FACTA measures liability at the point of sale and there was no way to know at that time whether Jeffries would catch Centerpiece's mistake or throw the receipt in the trash for any malicious third party to find. Because the inclusion of Jeffries's complete credit card information resulted in an increased risk of identity theft, she suffered a sufficiently concrete injury in fact to satisfy Article III's standing requirement.

The court distinguished the Third Circuit's opinion in *Kamal v. J. Crew Group*, which held that a plaintiff failed to establish standing when a merchant printed the first six digits of his credit card number on a receipt, noting that in *Jeffries* the inclusion of additional credit card numbers materially increased the risk of identity theft. Finally, the court stated that the risk of identity theft in the Jeffries case was not unacceptably conjectural because her claim did not rely on increased risk of future identity theft as her injury in fact. Rather, Jeffries' complaint was grounded in the invasion of her concrete privacy interest as protected by FACTA's truncation requirement.

Key Takeaways

The D.C. Circuit's pair of recent decisions results in two notable takeaways. First, the D.C. Circuit's attempt to distinguish potentially conflicting opinions issued by other circuits provides insight regarding the facts that may be relevant in future data breach cases. In the event of a data breach, the *National Treasury* opinion suggests that the case may turn on whether the plaintiff can plausibly allege that the thief intentionally targeted the stolen information, or can otherwise produce evidence of subsequent misuse of that information. With respect to a FACTA truncation claim, the D.C. Circuit indicates that the number of credit card digits matters, ostensibly ruling that 16 is too many.

Second, the deepening circuit split regarding standing in data breach litigation provides further impetus for the Supreme Court to clarify how *Spokeo* applies to data breach cases. At the time of writing, however, the Court declined to review any cases that might clarify this issue in the coming 2019 term. For now, the outcome of data breach litigation may depend in large part on the jurisdiction in which a case is filed.

Return to Table of Contents

Property Coverage Suit for Loss Caused by NotPetya Malware Attack Raises Questions About 'Act of War' Policy Exclusions

Snack-food company Mondelez International, Inc. (Mondelez) is challenging its property insurer Zurich American Insurance Company's (Zurich) reliance on an "act of war" exclusion in its policy to deny Mondelez coverage for losses resulting from the crippling NotPetya malware attack. The case, which is currently pending in Illinois state court, could be the first to determine whether an act of war policy exclusion applies to deny coverage for a cyber-related loss.

Background

On June 27, 2017, computers and servers at snack-food giant Mondelez were infected with the so-called NotPetya malware. The attack spread to thousands of the company's servers and laptops, halting company communications, rendering hardware useless and disrupting supply chains, which led to backlogs and unfulfilled product orders. All told, Mondelez claims that the malware infection caused it to incur losses in excess of $100 million.

According to U.S. officials, Mondelez was not the target of the NotPetya attack, which was part of a Russian campaign to destabilize Ukraine. Kremlin-affiliated hackers, using a cyber-weapon stolen from the U.S. National Security Agency, targeted a popular Ukrainian tax software company and its customers. NotPetya quickly spread, paralyzing government and industry in Ukraine and infecting global companies, including Mondelez. The U.K., Canada and Australia joined the U.S. in officially blaming Russia for the attack. The Kremlin adamantly denied responsibility.

Mondelez Claims Over $100 Million in Damages; Zurich Denies Coverage

Shortly after the NotPetya infection, Mondelez provided notice of loss under its "all risks" property insurance policy issued by Zurich. By letter dated June 1, 2018, Zurich denied coverage under Mondelez's policy based on an exclusion for "hostile or warlike action." That exclusion bars coverage for any 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."

On October 10, 2018, Mondelez brought suit against Zurich in the Cook County Circuit Court of Illinois for wrongful denial of coverage for the company's NotPetya malware loss.[5] Although Zurich has yet to answer the complaint, insurance industry players have taken a keen interest in the case and its implications. Two of the issues raised by this case are discussed below.

Should Legacy Exclusions Such as an Act of War Encompass Cyberattacks?

In its complaint, Mondelez alleges that act of war exclusions have never been applied to a malicious cyber incident and that invoking the exclusion for "anything other than conventional armed conflict" is "unprecedented." Indeed, the act of war exclusion is a legacy exclusion, crafted before insurers and policyholders anticipated modern acts of cyber warfare. As a result, interpreting the exclusion to apply to malware and ransomware attacks at least arguably could deprive policyholders of coverage they did not understand was excluded. On the other hand, courts have concluded that legacy policy provisions are applicable to previously unforeseen circumstances and new technologies. For example, in recent years, courts have applied various types of legacy policy language to digital privacy claims, data leaks and long-tail injury or damage claims.

What Evidence Suffices to Bring Cyberattacks Within the Ambit of Act of War Exclusions?

If the *Mondelez* court were to conclude that the act of war exclusion in the company's policy extends to the NotPetya attack, Zurich will face a critical hurdle: proving that the attack was carried out by a state actor. As noted above, applying the exclusion requires that the hostile or warlike action has been performed by a state, military arm of a state, or some agent or authority thereof. Tracing the source of a cyberattack, unlike many acts of conventional warfare, can be difficult, and it is unclear what kind of evidence the court will deem sufficient to demonstrate that the attack was carried out by a state actor. Although the U.S. intelligence agencies and several of its allies concluded that Russia was responsible for the NotPetya attack, marshalling evidence tracing the hack to its source could prove challenging. Nevertheless, it is conceivable that a court may conclude that the pronouncements of government and intelligence officials constitute sufficient proof of state action for Zurich to apply the exclusion.

[5] *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).

Key Takeaways

Industry players likely will continue to watch *Mondelez* closely for any rulings on the act of war exclusion. Although it is unlikely to be the final word on the topic, any ruling on the applicability of the act of war exclusion will have an impact on insurers' and policyholders' understanding of the scope of coverage for cyber-attacks under policies with act of war exclusions. Regardless of the outcome of this case, policyholders and insurers may want to consider clarifying policies' act of war exclusions, including with respect to their applicability to cyberattacks, whether the attackers can be both state and non-state actors, and the type of proof necessary for the exclusion to apply.

Return to Table of Contents

UK Data Protection Authority Responds to New Framework for Online Safety

In April 2019, the U.K. government published the Online Harms White Paper (the white paper) proposing a new legal and regulatory framework for online safety. The white paper outlined a new statutory duty of care, the implementation of new codes of practice and the creation of an independent regulatory body to enforce this framework. During the white paper's consultation period, which ended on July 1, 2019, the U.K.'s data protection authority, the Information Commissioner's Office (ICO), published a response, reinforcing the importance of regulation in this space and also pointing out key areas for improvement. The white paper now goes through the legislative process to determine whether it becomes law.

The White Paper

In April, the U.K. Department for Digital, Culture, Media & Sport and the secretary of state for the Home Department published a white paper on online harms, setting forth proposed legislative and non-legislative measures designed to keep British citizens safe from harms defined to include illegal, hostile or hurtful patterns of online behavior (*e.g.*, promulgating disinformation, cyberterrorism, hacking and cyberbullying) by individuals and organizations that target the safety and security of individuals.

The plan is designed to increase corporate responsibility and transparency with regard to users' safety online and proposes a new statutory duty of care for companies, requiring them to take "reasonable steps" to ensure users' safety (for instance, through easy-to-use online complaint functions that allow users to raise either concerns about specific pieces of harmful content or activity, or wider concerns about the company's compliance with its duty of care).

In addition, the white paper sets forth plans to create a new role for an independent regulator that will implement, oversee and enforce the new legal and regulatory framework, as well as oversee compliance by companies with the duty of care. The white paper also proposes a new media and digital literacy program designed to help users manage their own online safety.

The ICO's Response

As part of the consultation period, the ICO published its response, penned by U.K. Information Commissioner Elizabeth Denham. While Denham agreed with many of the proposed initiatives, she called for a broader understanding of internet harms, including those involving the use of personal data, which she emphasized cannot be positioned separately from the wider ecosystem of internet regulation. That is, any attempt to mitigate online harms must approach the problem holistically and across all government regulatory bodies to effectively use all existing regulatory tools and innovative new frameworks. Accordingly, Denham points out several gaps in the white paper, including the absence of an analysis of what is already regulated (and what is not) and "the lack of engagement … with the societal harm of electoral interference and the need for greater transparency in online political advertising and micro targeting."

As for who should enforce the white paper's initiatives, Denham explained that the role should be filled by an existing regulatory body that already has experience in data protection and content regulation. Denham stated that the regulator should take a cooperative and coordinated approach involving key U.K. regulators in the internet economy (*i.e.*, the ICO, the Competition and Markets Authority, the Electoral Commission and the Financial Conduct Authority). The white paper named the U.K. Office of Communications (Ofcom) as a candidate for the role, but only for an interim period during which a separate regulatory body would be set up. Denham noted that an interim approach would be difficult to execute in practice, as well as unnecessary given Ofcom's ability to develop capacity to support the role permanently.

Denham commented on the proposed duty of care, acknowledging that it was an "important part of the solution," but that it lacked the speed required to actively combat online harms. She proposed that the U.K. government also implement appropriate sanctions and powers that are comparable to those provided to the ICO under the General Data Protection Regulation (GDPR), including the power to compel information, carry out non-consensual audits, take cross-jurisdictional action and issue substantial fines.

Finally, Denham highlights one existing tension between privacy and security: the prevention of many online harms requires the monitoring of individual activities, a level of surveillance that could come into conflict with the ICO's mission to safeguard privacy. So far, insufficient definition has been given to the white paper's initiatives to determine whether any necessary surveillance would infringe on privacy rights.

Key Takeaways

From the ICO's perspective, the white paper's approach is only a starting point in the search for online safety, digital literacy and corporate accountability. In order to have the far-reaching effects the government intends, its approach must be holistic, collaborative and built on the efforts of existing regulators with effective enforcement powers. We will continue to monitor developments with respect to the white paper as it moves through the U.K. legislative process.

Return to Table of Contents

Equifax Reaches Largest-Ever Data Breach Settlement

In the largest settlement ever reached in a data breach case, Equifax has agreed to pay up to $700 million to settle claims arising from a breach that exposed the personal data of nearly 150 million people. It also agreed to spend $1 billion to improve its data security over the next five years. The global settlement resolves a nationwide, multidistrict class action litigation and investigations from the Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB) and nearly every state.

Background

Equifax, one of the country's three major credit reporting agencies, maintains a website where consumers can dispute information in their credit reports. The website ran on Apache Struts, an open source code. In March 2017, a vulnerability was discovered in the Apache software and a patch was issued. However, Equifax failed to properly apply the patch and the agency's scanning tool failed to identify the vulnerability. As a result, Equifax's systems were infiltrated in May 2017, more than two months after the Apache Struts patch was first made available. Between May 2017 and June 2017, Equifax's monitoring systems failed to detect the infiltration, and hackers were able to steal personal information from approximately 147.9 million American consumers, including names, dates of birth, Social Security numbers, addresses and other sensitive information. Equifax did not notify affected consumers until seven weeks after first learning of the breach.

More than 300 class actions were filed against Equifax arising from the breach and consolidated into a multidistrict litigation in the Northern District of Georgia.[6] The FTC, CFPB and every state, as well as the District of Columbia and Puerto Rico, also pursued action against Equifax. After nearly two years of negotiations, a global settlement was reached.

The Settlement

On July 22, 2019, the Northern District of Georgia granted preliminary approval to the nationwide class action settlement, which provides for monetary and injunctive relief.

Under the settlement, Equifax will pay $380.5 million into a non-reversionary fund to cover the settlement's benefits and costs, including attorneys' fees. Affected consumers may submit claim forms to receive compensation of $25 per hour (for up to 20 hours) for time spent taking preventative measures or dealing with identity theft. They also may receive reimbursement of up to $20,000 for (1) documented losses from the breach, such as the cost of freezing or unfreezing a credit file; buying credit monitoring services; or losses from identity theft or fraud; and (2) 25 percent of any money paid to Equifax for credit monitoring or identity theft protection subscriptions in the year before the breach. Equifax will pay an additional $125 million into the fund if needed to cover excess claims for out-of-pocket losses.

Class members will initially have six months to claim benefits. If money remains in the fund the claims period will be extended by four years, during which class members may recover for out-of-pocket losses and time spent rectifying identity theft that occurs after the end of the initial six-month claims period. The extended claim period reflects the fact that harm from a data breach may not materialize until years later because the hackers chose not to use the stolen data immediately, or because the stolen data

[6] *In re: Equifax Inc. Customer Data Security Breach Litigation*, No. 1:17-md-2800-TWT (N.D. Ga.)

standing alone does not suffice to effectuate an identity theft until later combined with other pilfered data.

The settlement also seeks to safeguard affected consumers from future harm and to restore their stolen identities. For four years, Equifax will provide three-bureau credit monitoring and identity protection services through Experian, and, for an additional six years, the agency will provide one-bureau credit monitoring through Equifax. It also will provide $1 million of identity theft insurance for four years. Those class members who already have credit monitoring or protective services in place will instead receive $125. For seven years, Equifax will provide identity restoration services to help class members victimized by identity theft, including access to a U.S.-based call center, assignment of a certified identity theft restoration specialist, and step-by-step assistance in dealing with credit bureaus, companies and government agencies.

Equifax also agreed to entry of a consent order requiring the company to spend a minimum of $1 billion on cybersecurity measures over five years. Among other things, the agency agreed to implement a comprehensive information security program; conduct vulnerability scanning; monitor and log security events, operational activities and transactions on its network; conduct incident response exercises; and engage in patch management. Equifax's compliance will be audited by independent experts and subject to the court's enforcement powers.

Equifax also has agreed to pay penalties of $100 million to the CFPB and $175 million to 48 states, as well as the District of Columbia and Puerto Rico. The only states not participating in the settlement are Massachusetts and Indiana, which have filed their own suits.

Key Takeaways

The Equifax breach resulted in a historic settlement requiring Equifax to pay up to $700 million in settlement money and fines, spend $1 billion in cybersecurity measures over the next five years, and be subject to oversight from auditors and the court. The breach may have been avoided by timely application of a patch to a known vulnerability on its webpage. As such, companies that process personal information should confirm that they have effective policies and procedures in place to identify and implement patches for known vulnerabilities.

Return to Table of Contents

UK ICO Issues New Guidance on Internet Cookies

On July 3, 2019, the U.K. ICO released, for the first time, guidance on the use of cookies and similar technologies (new guidance) in order to clarify the interplay between the GDPR and the U.K. Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (PECR). The new guidance comes in the lead-up to the proposed EU ePrivacy Regulation, which is intended to replace the Privacy and Electronic Communications (EC) Directive 2002/58/EC, upon which the PECR is based. Implementation of the EU ePrivacy Regulation has been delayed and is now expected in 2020 at the earliest.

Interplay Between GDPR and PECR

The PECR provides specific privacy rights in relation to electronic communications and applies to any technology that stores or accesses information on the user's device. This could include, for example, cookies and similar technologies, such as HTML5 local storage, local shared objects and fingerprinting techniques. Cookies assist in allowing a website to recognize a user's device and generally make websites work more efficiently. For example, they allow website providers to analyze website traffic and track users' browsing behaviors. Cookies often contain personal data, such as a user's location, IP addresses and/or website preferences.

Many of the areas of regulation that fall within the scope of the PECR also fall within the scope of the GDPR because the use of cookies typically involves processing personal data. The new guidance confirms that the key concepts of consent and transparency under the PECR must be interpreted in accordance with their definitions as enhanced under the GDPR. The new guidance therefore confirms that information provided about cookies on a website must be concise, intelligible and made available in an easily accessible form. In addition, where consent is obtained for the purpose of setting cookies, it must be freely given, granular and informed. The higher standard of consent means that implied consent would not constitute valid consent under the GDPR regarding the use of cookies or the processing of personal data. Accordingly, the new guidance clarifies that when companies send marketing messages or use cookies or similar technologies, they must comply with both sets of requirements under the PECR and the GDPR before doing so.

In particular, applying GDPR standards for consent has several implications, including the ban on pre-checked boxes and the use of "cookie walls." Cookie walls require users to "accept" the setting of cookies before they can access an online service's content and will often be non-compliant since they give users no choice but to accept the cookie. Cookie walls may only be permitted when falling under the specific exception in Recital 25 of PECR, which permits cookie walls so long as they are only used for specific website content, rather than general access, and facilitate the provision of online services requested by the user.

This is known as the strictly necessary exception, which applies where online collection of personal data is necessary in order to provide that particular online service. For example, companies may need a user's credit card information to process a transaction or a user's mailing address to ship a product. Outside of this exception, the use of cookie walls is likely to be in violation of the GDPR-enhanced consent requirement. The new guidance places a specific emphasis on analytics cookies, noting that these would not fall into this exemption.

Audits

The new guidance recommends that all website owners conduct a "cookie audit" to help ensure compliance with both sets of requirements under PECR and the GDPR. The ICO provides recommendations for these reviews, including:

- identifying cookies operating on or through the website;
- confirming the purpose of the cookies;
- confirming whether the cookies are linked to other data and might involve processing personal data;
- confirming whether cookies are "strictly necessary" or whether they will require user consent; and
- documenting findings and follow-up actions, while building in an appropriate review period.

Other Guidance

The new guidance covers a number of other topics, including an acknowledgment by the ICO that handling third-party cookies is one of the most challenging areas in which to achieve compliance with both PECR and the GDPR. Where a website sets third-party cookies, such as those on an advertising network, both the website owner and the third party have responsibility for ensuring that users are clearly informed and give consent. The ICO is committed to continuing to work with industries and other European data protection authorities to address the difficulties in finding workable solutions.

The new guidance does not clarify every point of uncertainty that arises within PECR. The proposed EU ePrivacy Regulation, an EU legislative instrument that is intended to replace the Privacy and Electronic Communications (EC) Directive 2002/58/EC (which is implemented through the PECR in the U.K.), may provide clarity on any remaining items of uncertainty. However, implementation of the EU ePrivacy Regulation has been delayed and is not expected until 2020 at the earliest.

Key Takeaways

The new guidance demonstrates that, in spite of a delay in the implementation of the EU ePrivacy Regulation, cookies are still a regulatory priority for EU member states. Other EU data protection authorities, including the French and Dutch authorities, also have published new guidance on cookies. The ICO and the other EU data protection authorities recommend that companies subject to the GDPR revisit their cookie usage policies and practices in light of the consent and transparency requirements under the regulation without waiting for the EU ePrivacy Regulation to come into force.

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

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

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