Skadden

Privacy & Cybersecurity Update

EU Approves General Data Protection Regulation

The European Parliament formally approved a sweeping replacement of existing EU data protection laws. The new law will become effective in mid-2018.

Following its December announcement that a draft regulation had been completed, the European Parliament voted on April 14, 2016, to formally approve the EU General Data Protection Regulation (GDPR). The GDPR will replace and substantially expand the current data protection regime in the EU. This approval marks the beginning of a crucial implementation phase for any organization doing business with European residents.

Timing and Scope

The GDPR will go into full effect two years after it is published in the *Official Journal of the European Union* — or roughly mid-2018.[1] Until then, companies should, at a minimum, continue to comply with current EU data protection laws, while they prepare to comply with the GDPR. In particular, companies should consider the GDPR's requirements while developing new products, services, policies and procedures, and should examine their existing data practices to determine what will need to change under the new law.

Key Elements of GDPR

The GDPR contains sweeping reforms to data protection in the EU, and we provided a detailed summary of the GDPR in our December 2015 mailing.[2] Although the December summary was based on a non-final version of the law, the final law has not substantively changed from that version.

[1] Due to certain special status within the EU, the regulation only will apply to the U.K. and Ireland to a limited extent. Additionally, Denmark will make an individual decision within the next six months whether it will implement the GDPR into national law.

[2] Available online at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_December_2015.pdf.

More Information to Come

It remains to be seen what impact the GDPR will have on global commerce, but companies should not take lightly this monumental development. National Data Protection Authorities and the Article 29 Working Party are expected to issue guidelines and opinions over the coming months to assist companies in preparing for the regime shift, which we will report in this newsletter as available.

Return to Table of Contents

EU Data Protection Authorities Critique 'Privacy Shield'

The EU Article 29 Working Party has released a report that questions aspects of the recently negotiated "Privacy Shield" arrangement between the EU and U.S., throwing into question whether the EU will approve the proposed arrangement or require changes.

On April 13, 2016, the EU's Article 29 Working Party (WP29), a European data protection advisory body whose membership comprises representatives from the data protection authority of each EU member state, the European Data Protection Supervisor and the European Commission, released a report critiquing certain aspects of the proposed "Privacy Shield" recently negotiated by EU and U.S. representatives. Though the group noted that the Privacy Shield is a significant improvement over the now invalidated "Safe Harbor" program, it said that the Privacy Shield did not go far enough to protect the privacy of European residents. Since the WP29 only serves in a non-binding advisory capacity, its disapproval does not doom the proposed arrangement, but it may lead the EU and U.S. to make changes before the EU formally adopts it. However, U.S. negotiators have indicated that that they do not wish to change the proposed arrangement. If no changes are made, the report provides privacy advocates with a blueprint of areas where the Privacy Shield may fall short of EU data privacy requirements.

Background

EU data protection law forbids the transfer of personal information from an EU member state to a jurisdiction that does not — in the EU's view — provide "adequate" protections for that information. The EU has long viewed the United States as a jurisdiction that does not meet EU standards for data protection. In addition to certain other mechanisms to allow personal data to flow from the EU to the U.S., the EU and U.S. agreed on a "Safe Harbor" program, under which companies that self-certified to certain data protection standards could transfer personal information into the United States.

In October 2015, however, the Court of Justice of the European Union invalidated the Safe Harbor in *Schrems v. Data Protection Commissioner*[3] on the grounds that it did not adequately protect the interests of data subjects. The court's primary objections were the ability of the U.S. government to access personal data for national security purposes and the lack of recourse available to EU residents who felt their privacy rights had been violated fundamentally.[4] The *Schrems* decision threw into doubt the data practices of many companies, and EU and U.S. officials entered into negotiations to craft a replacement for the Safe Harbor. That replacement, the Privacy Shield, was released in February 2016.

The Privacy Shield consists of a series of key privacy principles with which companies must comply that are generally similar to those embodied in the Safe Harbor. In addition, U.S. government entities will undertake certain commitments regarding the use of data for national security purposes. The framework also provides new avenues of recourse for European residents who believe their data has been misused and adds more rigorous enforcement mechanisms.[5]

Before being formally adopted by the European Union, the Privacy Shield must be approved by a qualified majority of the Article 31 Committee, which is composed of EU member state representatives, after which the EU College of Commissioners must formally adopt the decision. This process is generally expected to be completed in June 2016.

Article 29 Working Party Review

The WP29 has reviewed the Privacy Shield and issued its advisory opinion on the arrangement.[6] Overall, the WP29's view was that the Privacy Shield was a significant improvement over the Safe Harbor arrangement, but the group expressed a number of concerns, including:

- The "purpose limitation," which limits how data can be used, is unclear and could allow for reuse of data for "very large purposes and transfers";
- Data retention issues were not adequately addressed;
- The various ways in which EU users can seek recourse for privacy issues is confusing and will be difficult for laypeople to navigate;
- The arrangement still would allow massive, indiscriminate surveillance for national security purposes — one of the very reasons the Safe Harbor was rejected;

[3] Case number C-362/14, in the Court of Justice of the European Union.

[4] For more on the *Schrems* decision, see our special October 7, 2015, edition of *Privacy and Cybersecurity Update*, available online at https://www.skadden.com/court-justice-european-union-declares-US-EU-safe-harbor-invalid.

[5] A more detailed discussion of the Privacy Shield can be found in our February 2016 edition of *Privacy and Cybersecurity Update*, available online at http://www.skadden.com/newsletters/Privacy_and_Cybersecurity_Update_February_2016.pdf.

[6] The full opinion is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

- There are insufficient guarantees that the proposed ombudsman — who will be responsible for processing requests relating to national security access to EU personal data that is transmitted to the U.S. — will be independent and have sufficient power to enforce the Privacy Shield's restrictions; and
- It is not clear how the Privacy Shield will interact with the new General Data Protection Regulation, which will take effect within two years.

US Response

Shortly after WP29 released its opinion, U.S. Undersecretary of Commerce for International Trade Stefan Selig — one of the lead negotiators for the U.S. — indicated that the U.S. would be wary of reopening the Privacy Shield negotiations at this stage. Selig expressed concern that changes at this stage could upset the "delicate balance" achieved in the Privacy Shield.

Next Steps

The Article 31 Committee still can issue a binding "adequacy decision" supporting the Privacy Shield, and the EU College of Commissioners may adopt the decision, each without doing anything to address WP29's concerns.

Whether or not any changes are made to the Privacy Shield before its adoption, a risk still remains that individual data protection authorities will be receptive to challenges to the Privacy Shield. Some suggest that even if changes are made, challenges by individual EU residents are inevitable. Any such challenges could result in a second *Schrems*-like decision invalidating the arrangement.

Binding Corporate Rules and Standard Contractual Clauses Remain Effective — For Now

WP29 has made clear that it views binding corporate rules and the EU-approved standard contractual clauses as valid mechanisms for companies transferring personal data from the EU to the U.S. for the time being. Even so, WP29 Chairwoman Isabelle Falque-Pierrotin has acknowledged the legal uncertainty surrounding these types of data transfers in light of potential *Schrems*-like challenges.

Return to Table of Contents

Nebraska Data Breach Statute Update

Nebraska has amended its data breach notification statute to expand the scope of covered information, require notice to the attorney general and clarify that data is not considered encrypted if the information needed to decrypt it also is accessed.

On April 13, 2016, Nebraska Gov. Pete Rickets signed LB 835 into law, amending the state's data breach notification statute. In amending its laws, Nebraska joins a growing number of states that have tightened their notification statutes.

The amendment expands the definition of "personal information" to include a username or email address that is associated with a password or security question and answer that allows access to an online account. The law now requires notification if such data is acquired by an unauthorized person. Nebraska is the fifth state — following California, Florida, Nevada and Wyoming — to require notification of a breach of account credentials.

The law also now requires notice of a data breach be made to the state's attorney general no later than notice is provided to state residents; such notices must be made "as soon as possible and without unreasonable delay."

Finally, the amendment also clarifies that data is not considered encrypted if the encryption key or confidential encryption method was or is reasonably believed to have been acquired as a result of the breach.

The changes take effect on July 20, 2016.

Return to Table of Contents

Seventh Circuit Allows Data Breach Class Action to Proceed Despite Lack of Financial Harm

The Court of Appeals for the Seventh Circuit has ruled that a class action arising out of a data breach can proceed, despite the plaintiffs' inability to show any actual out-of-pocket damages arising from the breach.

A Seventh Circuit panel ruled in mid-April in *P.F. Chang's* that customers affected by a data breach involving credit card information have standing to sue, despite not suffering any actual out-of-pocket financial harm, reversing the lower court's dismissal of a 2014 class action.[7] The succinct decision further advances concepts of "injury" underlying the Seventh Circuit's precedential 2015 ruling in *Remijas et al. v. Neiman Marcus Grp., LLC*.

[7] *See John Lewert v. P.F. Chang's China Bistro Inc.*, case number 1:14-cv-04787 (N.D. Ill. 2014), and *Lucas Kosner v. P.F. Chang's China Bistro Inc.*, case number 1:14-cv-04923 (N.D. Ill. 2014) (consolidated decision).

Background and Claim

In June 2014, P.F. Chang's China Bistro (P.F. Chang's) alerted customers that its computer system had been breached and credit- and debit-card information potentially compromised. At the time of its announcement, P.F. Chang's was uncertain about the extent of the breach, the length of time it had gone undetected and the number of restaurant locations affected. As a precautionary measure, the restaurant notified all of its customers, urging them to monitor their credit card statements. Certain individuals who had dined at a P.F. Chang's brought a putative class action suit, seeking damages resulting from the breach. The plaintiffs included among their claimed harms that fraudulent transactions were attempted (but not executed) using their stolen debit card numbers, and that the breach caused them to purchase credit monitoring services and expend time and effort monitoring their card statements.

District Court Decision

The district court found that the named plaintiffs failed to demonstrate "concrete and particularized injury" sufficient to established Article III standing, and that the plaintiffs' claimed harms were either non-existent or too abstract to qualify as "injuries" for purposes of standing. Specifically, the district court rejected the plaintiffs' argument that they were at an increased risk of identity theft as too speculative to meet their burden. Further, the court found that neither plaintiff suffered a present injury because no fraudulent charges were ultimately made on either's account, and, given the speculative nature of their "increased risk," the plaintiffs' mitigation efforts were not responsive to an imminent harm.

Seventh Circuit Reversal

The Seventh Circuit reversed the district court's decision, pointing to its recent ruling in *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015). In *Remijas*, plaintiffs brought a class action suit against Neiman Marcus, stemming from a data breach that potentially exposed the payment-card data of all customers who paid with a credit or debit card the previous year. The Seventh Circuit found that some of the plaintiffs' alleged injuries, both present and future, were sufficiently concrete and particularized to support standing. With respect to the future risk of fraudulent charges and identity theft, the court found that, rather than being overly speculative, these injuries were "objectively reasonabl[y]" likely to occur. Despite the fact that Neiman Marcus offered all affected customers a paid credit monitoring service, the court also found the time and money class members had spent resolving fraudulent charges, and mitigating future ones, to be injuries sufficient for standing, regardless of whether they were ultimately reimbursed. According to the *Remijas* court, because the data breach had already occurred, the risk of fraudulent charges and identify theft was sufficiently immediate to justify mitigation efforts.

The Seventh Circuit panel found that several of the injuries alleged in *P.F. Chang's* fit into those discussed in *Remijas*. First, the plaintiffs alleged sufficiently concrete, increased risks of fraudulent charges and identity theft stemming from the data breach. Additionally, they alleged sufficient facts to support standing based on present injuries, namely, their mitigation efforts: One plaintiff claimed he detected fraudulent charges and spent time and effort addressing them (including by purchasing credit monitoring), while another plaintiff, despite not identifying any suspect charges, expended time and effort monitoring his card statement due to his increased risk.

PF Chang's attempted to distinguish its case from *Remijas*, including by arguing that, unlike in *Remijas,* it is questionable whether the plaintiffs' data was actually compromised. Though P.F. Chang's announcement regarding the breach addressed customers of all P.F. Chang's locations, a subsequent internal analysis identified only a limited number of restaurants actually affected; the location where the plaintiffs dined was not among them. The Seventh Circuit rejected the argument as immaterial to the standing issue, though it remains available to P.F. Chang's to use as a defense in challenging the link between the breach and any fraudulent charges.

Key Takeaway

A major potential obstacle to class action suits against companies that suffer data breaches had been the plaintiffs' inability to establish standing because losses had been reimbursed or they were unable to link any harm to the specific incident. The Seventh Circuit's ruling suggests that plaintiffs may be able to overcome this obstacle, which may make it harder for companies that suffer data breaches to have these claims dismissed, potentially exposing them to damages. Companies may want to factor the possible difficulty of having these cases dismissed in their cybersecurity risk analysis.

Return to Table of Contents

Appellate Court Upholds Cybersecurity Coverage Under Traditional Liability Insurance Policy

While the procurement of standalone cyber policies is on the rise, a U.S. Appeals Court recently held that a cyber-based claim is covered by a traditional commercial general liability insurance policy, providing a useful reminder that insureds should consider all of their coverage lines when confronted with a cyber/privacy loss.

A recent decision from the U.S. Court of Appeals for the Fourth Circuit illustrates that insureds might be covered under their traditional commercial general liability (CGL) insurance policies for claims arising out of cybersecurity breaches. In *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, L.L.C.,*[8] the court held that Travelers must cover its insured, Portal, pursuant to the terms of two CGL policies, in a putative class action lawsuit arising out of an alleged data breach.

The underlying action alleges that Portal failed to adequately safeguard a server containing confidential medical records of patients of an upstate New York hospital that contracted with Portal for the electronic storage and maintenance of those records. According to the complaint, two of the patients discovered via Google that their medical records were publicly available online. Portal sought coverage for the underlying action under two CGL policies issued by Travelers, which, according to the district court's decision, obligate Travelers to pay all sums that Portal becomes legally obligated to pay as damages because of the electronic publication of material that, depending on the policy year, either "gives unreasonable publicity to a person's private life" or that "discloses information about a person's private life."

In July 2013, Travelers sued Portal in the U.S. District Court for the Eastern District of Virginia. seeking a declaration that Travelers has no duty to defend Portal on the basis that the complaint fails to allege a covered "publication." On the parties' cross motions for summary judgment on the duty to defend, the district court sided with Portal, holding that "exposing confidential medical records to online searching is 'publication' giving 'unreasonable publicity' to, or 'disclos[ing]' information about, a person's private life," which triggered coverage under the Travelers policies. In reaching its decision, the district court rejected Travelers' argument that there was no "publication" by Portal because no third party is alleged to have viewed the medical records, finding instead that the medical records were "published" the moment they became accessible to the public via the Internet, notwithstanding that no third party was alleged to have actually viewed the records.

In commending the district court for its "sound legal analysis," the Fourth Circuit first determined that the district court correctly applied Virginia's "eight corners" rule, which required it to compare the four corners of the Travelers policies with the four corners of the underlying complaint to resolve the duty to defend. Adopting the district court's reasoning, the Fourth Circuit then found that the underlying action "'at least potentially or arguably' alleges a 'publication' of private medical information by Portal," thereby triggering Travelers' duty to defend. In so holding, the Fourth Circuit reasoned that the alleged conduct "if proven, would have given 'unreasonable publicity to, and disclose[d] information about, patients' private lives,' because any member of the public with an internet connection could have viewed the plaintiffs' private medical records during the time the records were available online."

While companies across all industries are purchasing standalone cyber insurance on an increasing basis and prudently so, the Fourth Circuit's recent decision in *Travelers* demonstrates that the possibility of coverage for cyber incidents under traditional policies should not be overlooked.

Return to Table of Contents

FTC Issues Guidance and Compliance Tool for Mobile Health Apps

The FTC has issued guidance and a compliance tool for mobile health app developers. The guidance provides developers with the FTC's views on "best practices" with respect to privacy and security practices, and a tool to help developers understand what laws might apply.

On April 5, 2016, the Federal Trade Commission (FTC) released two guidelines to help mobile health app developers navigate data privacy and security matters: guidance on building privacy and security into mobile health apps and a web-based tool to help developers understand what federal laws and regulations might apply to their applications.

Guidance for Health Apps

The guidelines for mobile health app developers reflect the commission's views on "best practices" on data privacy and security practices for such applications. These include the following:[9]

- **Minimize Data**. Developers should minimize the amount of data they collect about individuals using their app, take reasonable steps to secure any data they do collect and delete it once they no longer have a legitimate purpose for retaining it. To help accomplish these goals, the guidelines provide information on keeping data in de-identified form and points to the Department of Health and Human Services' regulations requiring entities covered by HIPAA either to remove specific identifiers (*e.g.*, date of birth and zip code) from protected health information or to have a data security expert confirm that the risk of re-identifying the data is "very small."

[8] No. 14-1944, 2016 WL 1399517 (4th Cir. Apr. 11, 2016).

[9] The guidance is available online at https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.

- **Limit Access and Permissions**. Developers should limit access and permissions to ensure that the app does not access consumer information it does not need *(e.g.*, allowing users to select individual contacts to share information with, rather than requesting access to the user's entire address book).
- **Authentication and Passwords**. Developers should require multifactor authentication and complex passwords for users to log on and suggest using rate limiting to control the traffic sent to or received by a network to reduce the risk of automated attacks. The guidelines also emphasize the importance of developers storing the passwords securely and limiting access to the app's data to trusted clients or parties with a legitimate need to use the data.
- **Consider the Mobile Ecosystem**. If developers are using a mobile platform to protect sensitive data, they should thoroughly research different platforms and conduct security testing to confirm the protections they provide are adequate. The guidelines note that, even when using a software tool developed by another company, it is still the developers' responsibility to ensure it conforms to the app's privacy promises and consumer expectations.
- **Security by Design**. Developers should designate a dedicated staff member (or a team of people if the organization is large and/or complex) to be responsible for data security at the company. Developers also should run periodic testing to ensure the security measures hold up when challenged and implement "bug bounty" programs that offer rewards, such as cash or free products, to people who identify security vulnerabilities.
- **Notice to Consumers**. Developers should notify consumers of the app's privacy and security features, and the guidelines suggest best practices for doing so. Among these suggestions are that developers (i) inform users of sensitive or unexpected data the app will collect both when users first install the app and again when the app collects the data, (ii) maintain easily accessible and clearly worded privacy policies that don't use complicated jargon and (iii) be precise and clear regarding why the data is being collected (*e.g.*, rather than stating simply that "we want to know your location," explain that "we want to track your location to see how far you have run").
- **Awareness of Applicable Laws**. Developers should be aware of other federal laws that may apply. For more specific information about the laws that might apply to health apps, developers can use a new interactive tool that the FTC released (which we describe below). Additionally, the guidelines link to other laws that may apply, depending on the app's user base or functionality, such as the Children's Online Privacy Protection Rule and the Gramm-Leach-Bliley Act's Safeguards Rule and Privacy Rule, as well as state laws.

Guidance Tool

The guidance tool presents developers with a series of high-level questions about their applications to help them understand which federal laws and regulations might apply to their applications.[10] The FTC created the tool in conjunction with the Department of Health and Human Services' Office of National Coordinator for Health Information Technology, Office for Civil Rights and the Food and Drug Administration.

The guidance tool uses responses from those questions (which relate to, for example, the nature of the app, the data it collects and the services it providers to users) to determine which federal laws might apply and points developers toward more detailed information accordingly about those laws. These include:

- The FTC Act, which prohibits deceptive or unfair acts or practices in or affecting commerce, including those relating to privacy and data security and involving false or misleading claims about an apps' safety or performance;
- The FTC's Health Breach Notification Rule, which requires certain business to provide notification of breaches of personal health record information;
- The Health Insurance Portability and Accountability Act, which protects the privacy and security of certain health information and requires certain entities to provide notifications of health information breaches; and
- The Federal Food, Drug and Cosmetics Act, which regulates the safety and effectiveness of medical devices, including certain mobile medical apps.

Key Takeaways

The FTC's guidance and compliance tool reflect the commission's ongoing effort to help companies understand what the commission expects from developers with respect to data privacy and security matters. Though focused on health applications, much of the guidance and the compliance have broader application beyond the health field, so all developers should take them into account when developing products and services that collect personal information.

Return to Table of Contents

[10] The tool is available online at https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

Consumer Notice for Breach of Encrypted Data May Be Required Under Amended Tennessee Law

Tennessee has strengthened its existing data breach notification law, which now may require notification even if the compromised data was encrypted.

On March 24, 2016, Tennessee Gov. Bill Haslam signed into law S.B. 2005, which amends the state's data breach notification statute to impose increased and more specific notification requirements on individuals, state agencies and businesses that own or license computerized data that includes personal information. The amendment will go into effect on July 1, 2016.

Most significantly, there is some indication that the legislative intent was to remove the encryption safe harbor so that companies would have to report data breaches even if the personal information was encrypted. Nonetheless, it is unclear whether the amended law, as drafted, actually has this effect.

If, in fact, the legislature intended to remove the encryption exception, this would be a radical departure from what has become the federal and state norm on data protection. In every other state, and under all the applicable federal data breach notification laws, there is no obligation to disclose a data breach if the personal information was encrypted (except in some cases where the information needed to decrypt the data also was accessed).

Status of Encryption Exception Unclear

Statements by some Tennessee legislators — together with a summary of the amendment prepared by the legislature — suggest that the amendment was intended to remove the encryption exception to the notification obligations and instead require companies to disclose data breaches affecting encrypted personal information. Many commentators who have written on the changes to Tennessee's law have suggested that the amendment has this effect. A close reading of the amended statute, however, suggests that the encryption exception remains in effect, though this may simply be a drafting error in the revised law.

The confusion arises from the fact that the amendment removes the word "unencrypted" from two sentences in the existing statute:

- **Definition of Security Breach**: "'Breach of the security of the system' means unauthorized acquisition of *unencrypted* computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder;" (emphasis added)[11] and
- **Breach Disclosure Obligation**: "Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Tennessee whose *unencrypted* personal information was, or is reasonably believed to have been, acquired by an unauthorized person" (emphasis added).[12]

However, the amended statute did not modify the definition of "personal information," which would continue to limit the statute to cases where some or all of the compromised information was not encrypted:

> "Personal information" means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted
>
> (i) Social security number;
>
> (ii) Driver license number; or
>
> (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;[13]
>
> (emphasis added)

Based on this definition of "personal information" it would appear that if *both* the name and the data elements listed in the definition were encrypted, the compromised data would not be "personal information," and therefore not trigger notice under the statute.

Adding to the confusion, the Tennessee legislature's summary of the amendment explains that it specifies that "a breach of the security system includes the unauthorized acquisition of all computerized data, whether encrypted or unencrypted."[14] While this is true on its face, in order to constitute a "breach of the security of the system" as defined in the statute, the acquisition must materially compromise "personal information." If the name and the data elements were encrypted, then it would not constitute "personal information" under the statute, so there would be no "breach of the security of the system."

[11] Tenn. Code § 47-18-2107(a)(1) (prior to amendment).

[12] Tenn. Code § 47-18-2107(b) (prior to amendment).

[13] Tenn. Code § 47-18-2107(a)(3)(A).

[14] The legislature's summary is available online at http://wapp.capitol.tn.gov/apps/Billinfo/default.aspx?BillNumber=SB2005&ga=109.

Similarly, Sen. Ketron, one of the amendment's sponsors, commented during a legislative session that the amendment "addresses encrypted and unencrypted information, because current law includes only unencrypted information." This statement suggests his intent was to remove the encryption exception.

The legislature's and the amendment sponsor's statements suggest that the inconsistency with the plain text of the statute is the result of a drafting error. If this error is not corrected, there may continue to be ambiguity on the exception's status.

Other Changes in Tennessee Law

The amendment also requires notification to Tennessee residents affected by a data breach "immediately" and at least within 45 days after discovery of the breach (absent a delay requested from law enforcement). The law previously required disclosure "in the most expedient time possible and without unreasonable delay" but, like the majority of states, did not provide a specific time frame. In imposing this specific time limit, Tennessee joins the growing number of states that have set specific time frames for notifying affected individuals.

Finally, the amendment expands the definition of "unauthorized person" for purposes of triggering notification obligations to include employees of the information holder who the information holder discovers has obtained personal information and used it for an unlawful purpose.

Key Takeaways

Regardless of whether or not the encryption exception was removed entirely, encrypting the data may still provide a defense against the obligation to disclose a breach in Tennessee. Under the statute, as amended, unauthorized access to data only qualifies as a "breach of the security of the system" if it "materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder." If the data were encrypted, a company that has experienced a security breach could argue that the security, confidentiality and integrity of personal information remains intact.

Controversy over the status of the encryption exception aside, the changes to Tennessee's law reflect a growing trend among state legislatures to tighten their data breach notification laws. Companies with information on residents of multiple states should continue to monitor these changes to ensure compliance.

Return to Table of Contents

Congress Considers the Role of Cyber Insurance in Managing Cybersecurity Risks

To assist congressional review of the role of cyber insurance in managing cybersecurity risks, North Dakota Insurance Commissioner Hamm testified on the state of the cyber insurance market and state regulators' commitment to promoting a working regulatory framework.

On March 22, 2016, North Dakota Insurance Commissioner Adam W. Hamm testified alongside other professionals before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on behalf of the National Association of Insurance Commissioners (NAIC) at a hearing titled "The Role of Cyber Insurance in Risk Management."[15] The hearing addressed the state of the market for cyber insurance and its use to effectively manage cyberrisk. Hamm testified from a regulatory perspective, emphasizing state insurance regulators' commitment to the promotion of an optimal regulatory framework with respect to cyber insurance and the key hurdles they face in effectively regulating an evolving market.

Hamm began his testimony by noting the "unprecedented" demand for cyber insurance, which he indicated is driven by an increased risk of cyberattacks. While threats to data privacy are not new, Hamm testified that the opportunities for cyber terrorists to inflict damage on businesses and the public increase exponentially as society becomes more reliant on electronic communication and as businesses collect personal data about their customers on a more granular level. Due to the lack of standardization in the marketplace, however, procuring a cyber insurance policy continues to be a nuanced process, and coverage can vary widely.

In discussing the regulatory challenges facing the cyber insurance market, Hamm testified that although insurance regulation is conceptually straightforward, in practice, "the regulation of an increasingly complex insurance industry facing constantly changing risks and developing new products to meet risk-transfer demand becomes challenging very quickly." Nevertheless, he testified, insurance regulators "take very seriously [their] responsibility to ensure the entities [they] regulate are both adequately protecting customer data and properly underwriting the products they sell" and cyber insurance policies "are scrutinized just as rigorously as other insurance contracts."

[15] The testimony of Hamm and the other witnesses is available at https://homeland.house.gov/hearing/the-role-of-cyber-insurance-in-risk-management/.

Hamm also noted that the lack of actuarial data has made it difficult to quantitatively assess cyberrisk, which in turn has potential implications for the ongoing regulation of the cyber insurance market and the promotion of best practices. If insurers price cyber policies too low, for instance, they risk being left without the financial means to pay out claims. Conversely, if insurers price their policies too high, businesses will opt instead to self-insure against cyberrisks, which, Hamm pointed out, limits the ability of the insurance industry to drive cybersecurity best practices. In the absence of quantitative data, insurers have resorted to qualitative assessments of applicants' cyberrisk profiles, which, in practice, results in customized policies at higher costs, Hamm noted.

Hamm then discussed a number of enhancements to the insurance industry's regulatory framework designed to improve cyberrisk management. He testified that, in 2015, the NAIC made specific improvements to its *Financial Examiner's Handbook* pertaining to the review of insurers' cybersecurity protocols. State insurance regulators also have heightened their expectations of insurers' chief risk officers and boards of directors with respect to knowledge and management of cyberrisk. Additionally, new reporting requirements are being imposed on insurers in 2016 to enable regulators to more accurately report on the size of the cyber insurance market and to better understand the market as it grows and matures, according to Hamm. The new NAIC-developed reporting form will be attached to insurers' annual financial reports and requires all insurers writing either identify theft or cyber insurance policies to report to the NAIC on their claims, premiums, losses, expenses and in-force policies covering either risk.

Hamm's testimony also addressed initiatives led by the NAIC and state insurance regulators to enhance data security expectations among insurers. Most recently, the NAIC Cybersecurity Task Force introduced a new *Insurance Data Security Model Law* for public comment, the purpose of which is to establish standards for data security, investigation and notification of a breach applicable to insurance licensees. The NAIC and state insurance regulators also work in collaboration with the federal government to identify and protect against cybersecurity threats.

In his concluding remarks, Hamm emphasized that the cyber insurance market remains in early stages of development and that insurance regulators are well-positioned to lead initiatives to optimize the cyber insurance market. "Insurance has a long history of driving best practices and standardization by creating economic incentives through the pricing of products, and the underwriting process can test the risk management techniques and efficacy of a policyholder making a broader range of businesses secure."

Hamm's testimony underscores the importance of understanding and managing cyberrisks in today's world of heightened cyber vulnerabilities. Cyber insurance is a key market-driven method to improve security and manage cyberrisks and, as Hamm's testimony suggests, the demand for cyber insurance will only continue to grow as cyberrisks develop and the cyber insurance market matures.

Return to Table of Contents

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

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

James R. 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

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

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

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

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

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

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

Gregoire Bertrou
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@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

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