Skadden

Privacy & Cybersecurity Update

European Data Protection Board Issues Opinions on Data Protection Impact Assessments

A key European data protection body has published opinions on the circumstances in which a company should carry out a data protection impact assessment under the GDPR. The opinions include specific requests to individual EU member states to update their own positions on these issues, creating an important test for the EU's efforts to harmonize GDPR enforcement across the member states.

On the October 3, 2018, the European Data Protection Board (EDPB) published opinions as to the circumstances in which a company should carry out a data protection impact assessment (DPIA),[1] recommending certain amendments to the guidance previously given by each member state on this topic. If implemented, the amendments could mean that mandatory DPIAs would be required in fewer instances than previously recommended in some member states, such as the U.K., but more frequently in others, such as Germany.

These EDPB opinions also draw attention to whether the GDPR will ever successfully achieve harmonization across the member states. DPIAs are just one example of differing GDPR approaches taken by member states, and it remains to be seen whether the EU can actually achieve one of the GDPR's key goals: consistency.

The Role of the European Data Protection Board

The EDPB is an independent European body based in Brussels that replaced the Article 29 Working Party (WP29) when the GDPR came into effect on May 25, 2018. It comprises representatives of the national supervisory authorities and the European Data Protection Supervisor (EDPS), as well as the supervisory members of the EEA EFTA states (Norway, Iceland and Liechtenstein), who are members with regard to GDPR-related matters but do not have capacity to vote or to be elected as chair or deputy chairs. The European Commission and the EFTA Surveillance Authority are able to participate in board meetings and activities but also lack a voting right.

[1] The EDPR opinions are available here.

The overriding aim of the EDPB is to contribute to the consistent application of data protection rules throughout the EU and promote cooperation between supervisory authorities. As opposed to the WP29 guidance, the general guidance issued by the EDPB (including guidelines, recommendations and best practices) is binding guidance. It also is worth noting that the EDPB has endorsed the WP29 guidance in relation to the GDPR issued prior to May 25, 2018.

Data Protection Impact Assessments

A DPIA is a process that helps an organization identify and minimize the data protection risks of any project involving new or amended data processing activities. As part of this assessment, organizations will need to describe the envisioned processing, to assess the necessity and proportionality of such processing in relation to the purposes, to assess the risks to rights and freedoms of the individuals concerned and to set out the measures that will be taken to address these risks.

A DPIA becomes mandatory when the level of risk is assessed to be of "high risk." Certain situations automatically are considered high risk under the GDPR when an organization plans to:

- use systematic and extensive profiling with significant effects;
- process sensitive (*e.g.* health data) or criminal offense data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

In addition, the GDPR requires supervisory authorities in each member state to publish lists of the other types of processing activities requiring a DPIA and, at their discretion, those for which no DPIA is required.

Though EDPB-endorsed guidelines (WP248 Guidance)[2] on how to assess a high-risk action are available, the lists put together by supervisory authorities providing practical examples on the type of processing activities requiring a DPIA differ significantly across the EU. The 22 opinions recently released by the EDPB advise how those DPIA lists should be amended for consistency purposes across the EU.

[2] The WP248 Guidance is available here.

Potential Changes to Member State Advice

The EDPB, which will impact a number of member states, clarifies that the lists prepared by supervisory authorities should state that they are not exhaustive, as scenarios that may qualify as high risk ultimately need to be assessed on a case-by-case basis. It also is good practice for an organization to conduct a DPIA prior to any critical project involving the processing of personal data. We highlight below the impact on Belgium, France, Germany and the U.K.

Interestingly, the EDPB seems to reference the list published by the Belgian Autorité de la Protection des Données (APD-DBA) when advising the other supervisory authorities on how to amend their lists, as the APD-DBA's list received far fewer requests for amendments than other member states. The EDPB did request a change to the list regarding the processing of health data with the aid of an implant to a matter that requires a DPIA, thereby adding a new scenario to the list of mandatory DPIAs in Belgium.

In relation to the processing of biometric, genetic or location data, the EDPB advised that such activity requires a mandatory DPIA only if another criterion requiring a DPIA also applies and therefore requested the U.K. Information Commissioner's Office (ICO) to amend its list accordingly.

Similarly, the EDPB required the French Commission Nationale de L'informatique et des Libertés (CNIL) to update its list (and to include the processing of location data). At the other end of the spectrum, the list of the German Budesbeauftragte und die Aufsichtsbehörden der Länder (BfDI) did not mention these types of processing activities at all, which prompted the EDPB to request that they be added in line with the advice given to the ICO and the CNIL.

In relation to the processing of personal data collected via third parties, the EDPB advises that the lists of all four supervisory authorities be amended to reflect that only where such processing is carried out in conjunction with at least one other criterion will it trigger the need for a mandatory DPIA. If the suggested amendments were followed through in such jurisdictions, this would add another type of processing activity requiring a DPIA.

In relation to processing using new or innovative technology, the ICO also was requested to amend its list to state that a DPIA only would be required when such processing is done in conjunction with at least one other criterion. This amendment would further restrict the ICO's current list in terms of mandatory DPIAs.

These four supervisory authorities, as with any other supervisory authority in the EU, are not obliged to amend their list in line with the EDPB opinion, but must justify their reasons if they elect not to do so.

Key Takeaways

We expect the DPIA lists of individual countries to evolve in light of the EDPB opinions. However, it is unclear if, and to what extent, the supervisory authority in each country will take the EDPB's suggested (but not required) changes into account. Where the guidance is not followed, it will be interesting to see the reasoning articulated as this may also point to potential future divergences from the EDPB.

Most importantly, how the supervisory authorities react to the EDPB's suggestions in relation to the DPIA lists represents one of the first real tests as to whether the GDPR is capable of being consistently applied across the EU. Given the existing discrepancies, it is quite possible that the supervisory authorities may not acquiesce to the EDPB's views, reflecting the different aims and agendas that each jurisdiction has concerning data protection. This recent development, therefore, demonstrates the distance between the current data protection framework and the more ambitious end goal of a greater level of harmonization across the EU.

Return to Table of Contents

Ohio Trial Court Holds That Bitcoin is Property, Not Money, Under a Homeowners Insurance Policy

An Ohio court recently concluded that a policyholder could pursue coverage for theft of bitcoin under his homeowners policy on the basis that bitcoin constituted "property" under the policy, and was not subject to the limits on coverage for "money" under the policy.

On September 25, 2018, the Franklin County Court of Common Pleas in Ohio ruled in *Kimmelman v. Wayne Ins. Grp.*, denying the defendant Wayne Insurance Group's (Wayne) motion for judgment on the pleadings in an insurance coverage action brought by the plaintiff, Wayne's insured, who was seeking to recover under his homeowners insurance policy for a bitcoin theft.[3] In ruling that bitcoin was "property" under the policy, rather than "money" that was subject to lower limits on recovery, the court may have set an important precedent for future claims for lost cryptocurrencies.

The Insurance Coverage Dispute

The dispute between the parties arose when the plaintiff submitted a claim for an approximately $16,000 bitcoin theft under his homeowners insurance policy issued by Wayne. After investigating the claim, Wayne paid the plaintiff $200 under the policy, concluding that bitcoin constituted "money" under the policy and therefore was subject to the policy's $200 sublimit for money loss. Disagreeing with Wayne's coverage determination, the plaintiff sued Wayne for breach of contract and bad faith.

Wayne moved for judgment on the pleadings, arguing that the plaintiff had no claim for breach of contract or bad faith because Wayne properly concluded that bitcoin constituted money under the policy and therefore was subject to a $200 money sublimit, which Wayne already paid to the plaintiff. In support of its contention that bitcoin constituted money, Wayne pointed to IRS Notice 2014-21, which refers to bitcoin as "virtual currency."

The trial court rejected Wayne's argument, reasoning that although the IRS Notice 2014-21 refers to bitcoin as virtual currency, the notice nevertheless treats bitcoin as "property" for federal tax purposes. The court thus denied Wayne's motion for judgment on the pleadings and concluded that the plaintiff could move forward with his breach of contract and bad faith claims.

Key Takeaways

The question of whether bitcoin is money or property appears to have been an issue of first impression for the Ohio trial court. However, as the use of bitcoin increases, the frequency of bitcoin-related insurance coverage issues is likely to increase. Given the lack of case law in this area, policyholders seeking coverage for cryptocurrency thefts are likely to cite the *Kimmelman* decision in support of coverage. In light of the *Kimmelman* decision and in order to avoid potentially costly coverage battles, insurers should clarify their policies to either expressly include or exclude coverage for bitcoin and other cryptocurrency loss.

Return to Table of Contents

[3] *Kimmelman v. Wayne Ins. Grp.*, Case No. 18-cv-001041, Doc. 0E337-P71 (Ohio Ct. Comm. Pl., Civ. Div. Sept. 25, 2018).

Florida District Court Holds That Policyholder is Not Covered Under CGL Policy For Data Breaches Publicized by Third-Party Hackers

A Florida federal court recently held that a policyholder was not covered under its commercial general liability (CGL) policy's "personal injury" coverage for a data breach where the data in question was publicized by the hackers rather than the policyholder.

On September 28, 2018, the U.S. District Court for the Middle District of Florida granted a motion for summary judgment in favor of St. Paul Fire and Marine Insurance Company (St. Paul), concluding that the insurer had no duty to defend its insured, the data security provider Rosen Millennium, Inc. (Millennium), under its CGL policy in connection with a credit card data breach caused by third-party hackers.[4]

The Data Breach and St. Paul's Coverage Action Against Millennium

Millennium provided data security services to its sister company Rosen Hotels & Resorts, Inc. (RHR). In February 2016, RHR learned of a potential credit card data breach at one of its hotels: malware had been installed on RHR's payment network which had been used to steal credit card information from RHR customers for up to a year-and-a-half. In December 2016, RHR emailed Millennium, stating its belief that the data breach was caused by Millennium's negligence and inquiring about Millennium's insurance coverage. Shortly thereafter, Millennium submitted a notice of claim to St. Paul under two consecutive CGL policies. St. Paul denied coverage and commenced suit against Millennium seeking a declaratory judgment that it had no duty to defend Millennium against RHR's claim.

In June 2018, St. Paul received a demand letter from Millennium in which RHR alleged that it was entitled to payment from Millennium as a result of the data breach. Although RHR had not filed suit against Millennium, St. Paul contended that the demand letter from RHR — together with Millennium's notice of claim — sufficiently created a case or controversy with respect to St. Paul's duty to defend. St. Paul therefore moved for summary judgment, arguing that it had no duty to defend Millennium because the allegations in the notice of claim and demand letter did not fall within the CGL policies' "personal injury" coverage. In response, Millennium contended that the claim fell squarely within both the personal injury and "property damage" coverages of the policies, thereby triggering St. Paul's duty to defend.

The District Court Granted Summary Judgment

Despite Millennium's argument that it was entitled to a defense under both the "personal injury" and "property damage" coverages, the court granted summary judgment for St. Paul, limiting its analysis to the personal injury coverage part only. The court reasoned that it was "confine[d] … to the allegations in the underlying claim" in determining whether St. Paul's duty to defend was triggered. Since a lawsuit had not been initiated, the relevant allegations are those in the demand letter and the notice of claim, with neither mentioning property damage. The notice of claim was "devoid of any substantive information," other than the fact of the data breach, while the demand letter tracked the policies' personal injury provisions with "no mention of, let alone a claim for, property damage." Accordingly, the court held that the issue of whether the policies covered any potential property damage was not ripe for determination and limited its coverage analysis to the policies' personal injury coverage.

The court then determined that the data breach was not covered by the policies' personal injury coverage. As relevant here, the policies defined a covered "personal injury offense" as "[m]aking known to any person or organization covered material that violates a person's right of privacy." The parties did not dispute that the credit card information at issue qualified as "covered material." At issue was whether the "making known" aspect had been satisfied. The court noted that the "making known" requirement was synonymous with "publication."

In reliance on another Middle District of Florida decision, *Innovak International, Inc. v. Hannover Ins. Co.*, the court held that the "making known" requirement was not satisfied because the third-party hackers, and not Millennium, had publicized the credit card information.[5] The court also reasoned that the policies require covered personal injuries to result from "[the insured's] business activities," and RHR's alleged injuries resulted from the actions of third-party hackers, not the business activities of Millennium. Accordingly, the court held that St. Paul had no duty to defend Millennium under the policies and granted summary judgment in favor of St. Paul.

[4] *St. Paul Fire & Mar. Ins. Co. v. Rosen Millennium, Inc.*, No. 617CV540ORL41GJK, 2018 WL 4732718 (M.D. Fla. Sept. 28, 2018).

[5] The case relied upon by the court is *Innovak Int'l, Inc. v. Hanover Ins. Co.*, 280 F. Supp. 3d 1340 (M.D. Fla. Nov. 17, 2017).

Key Takeaways

The District Court's decision highlights the complications that third-party hacking and malware play in the CGL insurance coverage arena. Although there are no bright-line rules in this context, a number of courts have found that there must be a "publication" by the insured — not a third-party hacker — in order to trigger a CGL policy's personal injury coverage. In light of the growing trend of data breaches at the hands of unknown hackers and CGL insurers taking the position that their policies do not cover cyber incidents, it is important for insureds to carefully negotiate coverage to extend to cyber incidents as needed.

Return to Table of Contents

UK Financial Conduct Authority Fines Tesco £16.4 Million for Failing to Protect Against Cyberattacks

The U.K. Financial Conduct Authority has levied a £16.4 million fine for failing to adequately protect against cyberattacks.

On October 1, 2018, the U.K. Financial Conduct Authority (FCA) announced that it would fine Tesco Personal Finance plc (Tesco) £16.4 million for failure to exercise due skill, care and diligence in protecting its account holders against a cyberattack that occurred in 2016, in which £2.26 million was stolen over 48 hours.

The Attack and Tesco's Response

The attackers exploited vulnerabilities in Tesco's process for issuing debit cards to customers, which enabled the attackers to generate authentic debit card numbers and engage in thousands of unauthorized transactions. Although Tesco's internal controls stopped almost 80 percent of the unauthorized transactions, the attack affected 8,261 out of 131,000 personal accounts.[6]

In its final notice to Tesco, the FCA described the sequence of events following the attack and described Tesco's inadequate response as a basis for the fine. According to the final notice, two hours after a 2:00 a.m. attack on a Saturday, Tesco's information security systems began sending automated text messages to affected account holders asking them to call Tesco regarding suspicious account activity. Staff at Tesco did not actually became aware of the attack until customers began calling in response to the text messages. It then took Tesco's internal financial crime operations team more than 21 hours to connect with the bank's fraud strategy team. Once the fraud strategy team identified the vulnerability that enabled the attack, the team put in place a rule to block the fraudulent transactions. However, Tesco failed to monitor the rule at first and therefore did not realize until several hours later that the rule failed to block the fraudulent transactions. The fraud strategy team eventually requested assistance from external experts who were able to identify the issue that caused the rule to fail and assist Tesco in implementing a new rule to block the fraudulent transactions by early Monday morning.

Determining the Fine

The FCA found that Tesco acted in breach of Principle 2 of the *Financial Conduct Authority Handbook*, which requires firms to conduct their business with due skill, care and diligence. Specifically, the FCA noted that Tesco distributed debit cards in a way that resulted in the circulation of sequential card numbers (which made it simpler for attackers to generate authentic debit card numbers), failed to address foreseeable risks that led to the attack and failed to respond to the attack in a sufficiently rigorous, skillful and urgent manner. Despite those failings, the FCA recognized that Tesco cooperated during the post-attack investigation, provided comprehensive redress to affected account holders and stopped a significant percentage of the unauthorized transactions. Tesco's agreement to enter into an early settlement also reduced the potential fine. Absent Tesco's early settlement and other mitigating actions, the FCA would have imposed a fine of £33,562,400.

In 2016, the U.K. Data Protection Act 1998 (DPA 1998) governed the imposition of penalties for inadequate cybersecurity practices, with the maximum fine under the DPA 1998 being £500,000. By contrast, the maximum penalty under the EU's General Data Protection Regulation (GDPR) as supplemented by the U.K.'s Protection Act 2018 is the higher of €20 million and 4 percent of annual worldwide turnover.

[6] The full text of the FCA's final notice to Tesco details the attack and is available here.

Key Takeaways

The FCA's decision to fine Tesco serves as a helpful reminder that companies should not only maintain appropriate incident response plans, but also should train those responsible for implementing such plans during a crisis. The FCA's decision to reduce the potential fine applicable to Tesco also should encourage companies to engage quickly and openly with relevant authorities to mitigate damages to their business and customers.

Return to Table of Contents

Vizio Settles Claims Relating to Data Collection Practices

Smart TV maker Vizio has agreed to pay $17 million to settle claims related to its data collection practices.

On October 4, 2018, Vizio, Inc. agreed to pay $17 million to settle multidistrict class action litigation arising from its data collection and tracking practices related to its smart TVs. The plaintiffs had argued that these practices violated federal and state privacy laws, as well as state consumer protection laws. The settlement is still subject to final court approval.

Background and Lawsuit

According to the lawsuit, Vizio, which manufactures internet-connected televisions (also known as smart TVs), used automatic content recognition software to collect information regarding the TV viewing choices and behavior of consumers and then shared that information with advertisers. These third parties could then use Vizio's viewing data to tailor advertisements on other devices connected to the same wireless network as the customer's smart TV. According to the lawsuit, Vizio failed to inform customers about its data-tracking practices and did not obtain consent from customers to collect and use such data. According to the plaintiffs, these actions violated state consumer protection and privacy laws and federal privacy laws, including the Video Privacy Protection Act and Electronic Communications Privacy Act. Vizio claimed that in using customer information, it never shared customers' names, addresses or other personally identifiable information.

The class action began as 20 separate class action lawsuits, each with similar claims, with the class including consumers who purchased a Vizio smart TV between February 1, 2014, and February 6, 2017. These lawsuits were consolidated in April 2016 in federal court in California and, since the consolidation, Vizio has unsuccessfully argued to dismiss the lawsuits on multiple grounds.

Prior FTC Settlement

Among other arguments, Vizio sought to dismiss the claims on the grounds that they were moot in light of Vizio's February 2017 consent decree with the U.S. Federal Trade Commission (FTC).[7] This decree resulted from an enforcement action brought by the FTC against Vizio, also based on the company's data collection and sharing practices. The FTC imposed $2.2 million in penalties on Vizio and prohibited the company from collecting viewer data without first disclosing its data collection and use practices and obtaining consumers' consent. The company had, in fact, revised its consumer-facing disclosures regarding data collection and use practices in December 2016, including by asking for consent from customers to use their data. In its motion to dismiss, Vizio argued that the plaintiff's request for injunctive relief was unnecessary because the FTC consent decree requires Vizio to disclose its data collection practices. This relief, according to Vizio, replicated what the plaintiffs sought. In July 2017, the U.S. District Court for the Central District of California denied Vizio's motion.

Settlement Terms

Under the settlement, in addition to paying class members a total of $17 million, Vizio must change how it discloses its data collection practices for new customers and delete the behavioral data it obtained during the class period. In addition to the changes already made in 2016, Vizio has agreed to make further revisions to its data collection and disclosure practices. For example, it will change the language of its opt-out mechanism from "agree/settings" — which was perceived as confusing consumers as to the options available to them — to "accept/decline."

[7] A discussion of the FTC case and related consent decree can be found in our February 2017 *Privacy & Cybersecurity Update*.

On December 7, 2018, the Central District of California plans to hold a hearing to consider the preliminary approval of the proposed settlement. In a motion for preliminary settlement approval, counsel for the consumers stated that the settlement is fair because it amounts to more than the revenue Vizio obtained from using class members' data during the class period. According to Vizio, the class could include roughly 16 million Vizio customers, each of whom can expect to receive between $13 and $31 depending on the claims submitted.

Key Takeaways

This class action lawsuit and proposed settlement (as well as the FTC enforcement action) is a reminder to companies, especially those manufacturing and distributing new technologies, to (i) conspicuously provide notice regarding their personal collection and use data practices, (ii) obtain clear, affirmative consent for any data collection and use, and (iii) comply with their stated privacy disclosures.

Return to Table of Contents

Anthem to Pay Record HIPAA Settlement for Data Breach

Anthem agreed to pay $16 million to the U.S. Department of Health and Human Services (HHS) and to undertake a corrective action plan following a 2015 cyberattack.

On October 15, 2018, HHS announced that Anthem, Inc. (Anthem) had agreed to pay $16 million to HHS to settle potential Health Insurance Portability and Accountability Act (HIPAA) violations resulting from cyberattacks in 2015 that led to the largest reported health data breach in the U.S. to date, with 79 million people's personal information accessed.[8] As part of the settlement, Anthem also agreed to undertake a corrective action plan to comply with applicable HIPAA requirements.

The Attacks

Anthem is an independent licensee of the Blue Cross and Blue Shield Association and is one of the largest health insurance providers in the United States. In January 2015, Anthem discovered that a targeted cyberattack had enabled access to its IT systems. In March 2015, Anthem filed a report with HHS detailing the attack and the resulting breach. An investigation found that a user at an Anthem subsidiary had opened a phishing email with malicious content, enabling the attackers to gain access to Anthem's IT systems. HHS revealed that between December 2, 2014, and January 27, 2015, the attackers stole the electronic protected health information (ePHI) of 79 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses and employment information.

Anthem paid $260 million for security improvements and remedial actions in response to the breach. The company also faced a civil class action lawsuit brought by its customers, which was settled for $115 million in June 2017, marking a record deal for private civil claims from data breaches. Additionally, Anthem agreed to provide two years of credit monitoring, to reimburse the out-of-pocket expenses customers incurred and to pay cash compensation to customers who had secured their own credit monitoring services.

The Anthem-HHS Settlement

HHS conducted an investigation into potential violations of HIPAA Privacy and Security Rules (HIPAA Rules) by Anthem in connection with the breach. In addition to the disclosure of confidential patient information, HHS's investigation indicated potential violations of HIPAA Rules due to Anthem's failure to conduct adequate risk analyses, implement sufficient information systems review procedures, identify and respond to detections of the security breach, and implement policies to limit access to customers' ePHI by non-authorized parties.

On October 15, 2018, HHS announced that Anthem agreed to pay $16 million to settle the alleged violations. Notably, the Anthem settlement is almost three times as high as what was previously the highest settlement paid to HHS for a data breach. As part of the settlement, Anthem agreed to comply with a corrective action plan aimed at addressing and ameliorating the deficiencies in its policies and procedures identified by HHS's investigation.

According to the director of HSS's Office for Civil Rights, Roger Severino, "The largest health data breach in U.S. history fully merits the largest HIPAA settlement in history." He also stated that "large health care entities are attractive targets for hackers, which is why they are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion or risk enforcement by [HHS's Office for Civil Rights]."[9]

[8] The full text of the settlement between Anthem and the HHS is available here.

[9] U.S. Department of Health and Human Services, "Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History," HHS.GOV (Oct. 15, 2018), can be accessed here.

Key Takeaways

The Anthem settlement highlights the costs of cybersecurity attacks. The settlement and HHS's statements confirm that HHS carefully investigates security and privacy breaches and potential HIPAA Rules violations, and that these violations could result in liability for companies. The settlement also highlights that companies must implement preventative strategies and safeguards to minimize the risk of cyberattacks, in addition to appropriate policies and procedures for responding to data breaches promptly and effectively. It is important that these measures are periodically reassessed and updated to ensure that cyberattack defenses remain robust and that a company is positioned as best as possible to deal with potential security breaches, therefore minimizing its potential liabilities due to a breach.

Return to Table of Contents

China Passes New Cybersecurity Regulations Pursuant to 2017 Cybersecurity Law

Chinese regulators have passed new regulations giving them broad authority to inspect the facilities, systems and data of companies operating in China.

New Chinese cybersecurity rules that will go into effect on November 1, 2018, grant Chinese regulators broad oversight to inspect companies' information technology systems and access their proprietary data and information. These new regulations have contributed to mounting concerns in the corporate world regarding protection of trade secrets.

China's 2017 Law and Reaction

China's primary cybersecurity law went into effect on June 1, 2017,[10] granting the Chinese government increased power to "ensure network security, to safeguard cyberspace sovereignty, national security and the societal public interest" according to language distributed by the government. Some key provisions of the law imposed the following requirements:

- Critical information infrastructure operators must store data in China. Since the law's enactment, certain major companies have begun the compliance process. For example, Apple has started building a data center in the southwest province of Guizhou.
- Network owners, managers and network service providers (a group which the law defines as "network operators") must adhere to social mores and commercial ethics and "accept supervision from the government and the public." In addition, network operators must provide technical support to public security officers. The 2018 regulations elaborated on this requirement, as described below.
- Network service and product providers must inform users and "competent departments" upon discovery of a security flaw or vulnerability. The recent regulations elaborate upon the general requirement that private corporations cooperate and assist Chinese cybersecurity officials in policing the internet.

When it was first passed, the law caused widespread concern among companies that would be subject to its new requirements — in part because of the vagueness of many provisions. Companies feared that the law could be used to force disclosure of trade secrets, including source code and other proprietary information.

2018 Regulations and Reaction

The 2018 regulations provide regulators with broad authority to inspect facilities, information technology systems and data to further the 2017 law's aims, while also requiring extensive cooperation with the government in monitoring and controlling content. Regulators have tried to address concerns over the misuse of proprietary information by indicating that "the information obtained by [cybersecurity officials] in fulfilling their duties of internet security supervision and inspection can only be used to maintain the needs of network security and must not be used for other purposes." However, because the new regulations take effect on November 1, 2018, and we have yet to see how vulnerable companies' proprietary data will be as they endeavor to comply with the rules, it is not yet clear whether and to what extent regulators will conform to that principle.

Some key provisions of the new regulations include:

- Chinese cybersecurity officials may conduct both physical and remote inspection and testing of a company's technology and security systems. Such inspection rights will allow Chinese officials to peruse a company's networks and information those networks contain so long as the inspection is in furtherance of Chinese national security, public safety, network security risks or social order.

[10] The new Chinese cybersecurity law is summarized at length in our June 2017 *Privacy and Cybersecurity Update*.

- Companies are responsible for policing the circulation of prohibited information online. This requirement reinforces provisions of the 2017 cybersecurity law which asks private actors to assist in censorship and surveillance efforts.
- Internet operators are required to cooperate with Chinese authorities conducting national security or criminal investigations. Failure to do so may result in legal liability of the internet operator itself.

Based on initial reactions, companies' greatest concerns with the new regulations are the rights of inspection and level of access that will apply broadly to proprietary systems and information. The regulations make it clear that Chinese authorities expect to receive access to technology and data within the country's borders. With this in mind, many fear that disclosure of such data will include trade secrets, source code and other proprietary information. Others, however, are embracing compliance as a cost of doing business. For example, Microsoft has opened what it calls a "transparency center" in Beijing where officials can test its products for security purposes.

Key Takeaways

The new regulations give regulators broad authority to inspect the facilities, systems and data for companies operating in China and do little to eliminate concerns surrounding the broad reach of China's cybersecurity law. As the new rules are implemented, the private sector may gain more insight into the practical consequences of doing business under the new cybersecurity regime.

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