Skadden

Privacy & Cybersecurity Update

October is National Cyber Security Awareness Month, initiated by the U.S. Department of Homeland Security and the National Cyber Security Alliance, an opportune time for companies to reassess their cybersecurity training, policies and procedures.

Adviser to European Court of Justice Says US-EU Safe Harbor Should Be Declared Invalid

An advisory opinion issued by the advocate general to the European Court of Justice states that the U.S.-EU Safe Harbor should be declared invalid because of U.S. intelligence access to data stored in this country.

For some 15 years, thousands of U.S. companies have relied on the U.S.-EU Safe Harbor Framework to transfer personal data from the European Union to the U.S. in a manner that meets the requirements of the EU Data Protection Directive. In recent years, the Safe Harbor has come under increasing attack from EU privacy officials who have argued that the Safe Harbor no longer provides adequate protection for the personal information of EU citizens. Now, the Safe Harbor faces what might be its greatest challenge to date. An adviser to the European Court of Justice has concluded in a report regarding a pending case that the Safe Harbor should be declared invalid.

Background

Under the EU Data Protection Directive, personal information about EU citizens can only be transferred from the EU to countries with adequate data protection. Only a handful of countries satisfy this requirement, and the U.S. is not one of them. The EU provides a few mechanisms for companies to conduct such transfers if they are not located in a country that meets the adequacy requirement. In the U.S., one of these mechanisms is the Safe Harbor, which was negotiated between the European Commission and the U.S. Department of Commerce, and went into effect in 2000. To join the Safe Harbor, a company must self-certify to the Department of Commerce that it complies with specified EU privacy standards. As a general matter, the Federal Trade Commission (FTC) has enforcement powers if companies violate the Safe Harbor or state they are certified when, in fact, they are not.

Recently, a number of EU privacy officials have attacked the Safe Harbor. In some cases, these attacks have questioned whether the FTC provides adequate enforcement, and in other cases, have asserted that the right of the U.S. intelligence community to access data vitiate the protections offered by the Safe Harbor.

Schrems v. Data Protection Commissioner

In *Schrems v. Data Protection Commissioner*,[1] the plaintiff alleged that Facebook's Irish subsidiary transferred data to the U.S. under the Safe Harbor but then participated with the National Security Agency's (NSA) PRISM program, which allowed the NSA unrestricted access to his data. The PRISM program became public as a result of documents leaked by former NSA contractor Edward Snowden. Schrems filed the complaint with Ireland's Data Protection commissioner, but the Irish authority rejected the complaint given that the European Commission had already determined that the Safe Harbor ensured an adequate level of data protection. Schrems appealed to the Irish High Court, which then referred the case to the European Court of Justice.

The European Court of Justice requested an advisory opinion from Advocate General Yves Bot. Bot's opinion harshly critiqued the Safe Harbor as a means to protect the privacy rights of EU citizens and said it should be declared invalid. Bot's focus was on the right of U.S. government agencies, particularly the intelligence community, to access such data "without any requirement that the persons concerned represent a threat to national security" and without any right for an individual to challenge the intelligence community's decision to access his or her data. BOT noted that the FTC, which is the enforcement body for the Safe Harbor, does not provide a means for an individual to challenge access by U.S. intelligence services to personal data transferred from the EU. According to Bot, "such mass, indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with [EU privacy rights]. Bot suggests that while the Safe Harbor may, back in 2000, have provided adequate protection, new circumstances — such as the PRISM program — render the Safe Harbor invalid.

Of equal significance is Bot's statement that despite the European Commission's acceptance of the Safe Harbor, the data protection authorities of individual member states could nonetheless find that the Safe Harbor should not be applied in individual cases. In Bot's view, an "essential component" of protecting the privacy rights of individual citizens is for the data commissioners to be able to make their own determination. Bot goes so far as to say that the European Commission or an individual member state could find that a third country, such as the U.S., does not provide an adequate level of data protection. As a result, Bot concluded that the Irish data commissioner should not have rejected Schrems' complaint.

Impact of Bot's Report

Bot's opinion is not binding on the European Court of Justice; however, there has been a strong trend for the court to adopt such opinions. Moreover, as seen by the European Court of Justice's decision upholding the "right to be forgotten," the court is willing to take a hard-line position on data privacy even when it has a direct impact on companies outside the EU.

In the event the court were to adopt Bot's opinion and strike down the Safe Harbor, or simply find that individual state data protection authorities can challenge its application in individual cases, the current framework of transferring data from the EU to the U.S. could be thrown in disarray. If that were to happen, companies would still have options to transfer data under the EU Data Protection Directive. The EU today allows companies to use so-called "model contracts" which are essentially form agreements that require adherence to certain fundamental EU data privacy principles, but allow the signatories to transfer data from the EU to the U.S. Since a model contract is required between each pair of companies transferring data, it can be far more cumbersome than Safe Harbor certification. The European Court of Justice's opinion is likely to be issued in the coming weeks.

Return to Table of Contents

SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach

The SEC has fined a broker-dealer for inadequate cybersecurity measures, possibly signaling the start of greater SEC enforcement activity.

On September 22, 2015, the Securities and Exchange Commission (SEC) announced that R.T. Jones Capital Equities Management, an investment adviser, agreed to settle charges that it "failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients."

The SEC's ruling is premised on Rule 30 of Reg. S-P, which provides:[2]

> Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to:

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

[2] 17 CFR § 248.30.

(1) Insure the security and confidentiality of customer records and information;

(2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

(3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

According to the SEC, R.T. Jones violated this rule over a four-year period, from September 2009 to July 2013, by "fail[ing] entirely to adopt written policies and procedures reasonably designed to safeguard customer information." During that period, the firm "failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cybersecurity incidents."

In July 2013, a hacker gained access to the personal information records of 100,000 individuals, including thousands of R.T. Jones' clients, that was stored on a web server hosted by a third party. R.T. Jones provided notice of the breach to every individual whose PII may have been compromised and offered free identity theft monitoring through a third-party provider. In addition, there was no evidence that any individual suffered any financial harm as a result of the attack. Nonetheless, the SEC found R.T. Jones had violated Rule 30. Without admitting any liability, R.T. Jones agreed to cease and desist from committing any future violations of Rule 30, and to pay a $75,000 penalty.

Marshall S. Sprung, co-chief of the SEC Enforcement Division's Asset Management Unit, stated in the SEC's press release that "Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."

Practice Points

The announcement of this enforcement action follows on the heels of guidelines issued by the SEC's Division of Investment Management (IM) in April 2015 for registered investment companies (funds) and registered investment advisers (advisers), and of the announcement on September 15, 2015, by the Office of Compliance Inspections and Examinations (OCIE) of its initiative to examine registrants, including advisers, for cybersecurity preparedness. Noting the increased reliance by funds and advisers on information technology and the importance of "protect[ing] confidential and sensitive information," IM staff outlined a number of measures for funds and advisers to consider taking to protect themselves against cyberattacks. Those measures fell under three broad categories: (1) conducting periodic risk assessments, (2) creating a strategy to "prevent, detect and respond" to threats, which could include setting up firewalls, managing access rights, storing data in protected servers and developing an incident response plan, and (3) implementing these strategies through written policies and procedures, and by training employees. With the Enforcement Division highlighting the absence of these measures as the basis for its action against R.T. Jones, it now appears that the measures identified in the IM's April 2015 guidelines — which are essentially derived from pronouncements in the National Institute of Standards and Technology's (NIST) Cybersecurity Framework — are not simply suggestions for conduct. Rather, they are actions that the SEC and other regulatory authorities will expect registrants to take in order to properly comply with existing regulations for safeguarding customer information and other data, such as Regulation S-P.

Return to Table of Contents

CNIL Determines 'Right to Be Forgotten' Deletions Must Be Applied Globally

In May 2014, the European Court of Justice decided that EU citizens have a "right to be forgotten" by having certain search engine hits removed from the Internet. The French data protection authority has extended this right to searches done from non-EU domains.

As reported in our May 2014 *Privacy & Cybersecurity Update*, in a case brought against Google, the European Court of Justice decided that month that an EU citizen has the right, with certain public interest exceptions, to demand that a search engine remove results that are generated when his or her name is searched. This so-called "right to be forgotten" was widely seen as favoring the fundamental right of privacy of EU citizens over the right of free speech. After the ruling, the president of the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), put Google on notice that it needed to proceed with such delistings on all of the search engine's domain names. Google delisted results on European extensions of its search engine (.fr, .es, .co.uk, etc.), but not on google.com or other geographical extensions. Google filed an informal appeal with the CNIL seeking to clarify that its actions were appropriate, and that the European Court of Justice ruling only applied to searches conducted from EU domains. On September 21, 2015, the CNIL president rejected Google's appeal, finding that a search engine must delist results regardless of where the search originated or which domain was used.

The CNIL president stated that if the right to be forgotten was limited to certain geographic extensions, it could easily be circumvented (*i.e.*, a user looking for information about someone who had been delisted would simply have to conduct a search using a geographic extension where delisting had not been implemented). This would convert the right to be forgotten simply into a right not to be searchable in certain countries.

The CNIL president also rejected Google's argument that its ruling would adversely impact the public's right to information, since delisting is not available to public persons. Finally, the president also rejected Google's argument that the decision amounts to applying French law extraterritorially. According to the CNIL, "It simply requests full observance of European legislation by non European players offering their services in Europe."

Google has not yet indicated how it plans to proceed in light of the CNIL's decision.

Return to Table of Contents

SEC Issues Cybersecurity Initiative for Broker-Dealers and Investment Advisers

The SEC has issued a risk alert announcing that the OCIE will be conducting a new Cybersecurity Examination Initiative. The alert highlights the areas of concern for the SEC.

On September 15, 2015, the SEC issued a risk alert release announcing that the OCIE will be conducting a new Cybersecurity Examination Initiative (the Initiative).[3] Through the Initiative, the OCIE will undertake a second round of examinations of registered broker-dealers and investment advisers' cybersecurity preparedness in light of recent breaches and continuing threats against financial services firms. The release highlights a number of areas of focus that the OCIE will cover when conducting its examinations.

Background

In March 2014, the SEC invited industry representatives to a cybersecurity roundtable to underscore the importance of cybersecurity to the integrity of the market system and customer data protection.[4] In April 2014, the OCIE published a risk alert announcing the examination of more than 50 registered broker-dealers and investments advisers, focusing on areas related to cybersecurity risks and preparedness.[5] A summary of OCIE's finding was published in February 2015, reflecting the legal, regulatory and compliance issues relating to cybersecurity.[6] OCIE announced a renewed focus on cybersecurity compliance and controls as part of its 2015 Examination Priorities and issued its most recent risk alert release to elaborate on the guidelines by which it will conduct its next round of examinations.[7]

Areas of Focus

In an effort to ensure that firms can adequately protect broker-dealer customer and investment adviser client information, OCIE will examine various cybersecurity-related controls and test implementation of those controls. The Initiative is designed to build on OCIE's prior cybersecurity examinations and will involve more testing to assess implementation of firm procedures and controls. The Initiative will focus on the following areas, many of which are consistent with areas of focus of other regulators:

- **Governance and Risk Assessment.** Examiners may assess whether registrants have cybersecurity governance and risk assessment processes in the areas set out below and whether those controls and processes are evaluated regularly and adequately tailored.
- **Access Rights and Controls.** Examiners will look at how firms control access to various systems and data via management of user credentials, authentication and authorization, including controls associated with remote access, customer logins and passwords.
- **Data Loss Prevention.** Examiners will assess how firms monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads. This also will include an assessment of how firms monitor for unauthorized data transfers and how firms verify the authenticity of a customer request to transfer funds.
- **Vendor Management.** Examiners will study firm practices and controls related to vendor management, such as due diligence in selecting a vendor, monitoring and oversight of vendors and contract terms.
- **Training.** Examiners will focus on how training is tailored to specific job functions and designed to encourage responsible employee and vendor behavior, and will review procedures for responding to cyber incidents under an incident response plan.
- **Incident Response.** Examiners will assess whether firms have established policies, assigned roles, assessed system

[3] OCIE, NEP Risk Alert, "OCIE's 2015 Cybersecurity Initiative" (September 15, 2015).

[4] Skadden, "SEC Holds Roundtable on Cybersecurity" (March 28, 2014).

[5] OCIE, NEP Risk Alert, "OCIE Cybersecurity Initiative" (April 15, 2014). *See also* our April 2014 *Privacy & Cybersecurity Update*.

[6] OCIE, NEP Risk Alert, "Cybersecurity Examination Sweep Summary" (February 3, 2015). *See also*, Skadden, "SEC Issues Cybersecurity Guidance for Investment Companies and Advisers" (May 6, 2015).

[7] OCIE, "Examination Priorities for 2015" (January 13, 2015).

vulnerabilities and developed plans to address possible future events.

The Initiative includes a sample request for information and documents.

Conclusion

In light of the OCIE's continued interest in promoting the Cybersecurity Examination Initiative, it would be prudent for broker-dealers and investment advisers to reflect on their cybersecurity policies and preparedness. Skadden's Privacy and Cybersecurity Group has the experience to assist clients in meeting these requirements.

Return to Table of Contents

Ninth Circuit Finds No Private Right of Action for Violations of Video Privacy Protection Act

The Ninth Circuit has joined two other federal appeals courts in finding that individuals do not have a private right of action under the Video Privacy Protection Act if their data is stored for longer than the act allows.

In *Rodriguez v. Sony Computer Entertainment America, LLC*,[8] the U.S. Court of Appeals for the Ninth Circuit joined the Sixth and Seventh circuits in finding that there is no private right of action for violations of the data retention provision of the Video Privacy Protection Act (VPPA).

Background

Rodriguez sued Sony Computer Entertainment America LLC (Sony Computer), alleging that the company stored his movie and rental purchase history beyond the one-year time limit permitted under the VPPA. Rodrigues also sued Sony Network Entertainment International, LLC (Sony Network) on the grounds that Sony Computer and Sony Network impermissibly shared his personal information with each other.

The Court's Ruling

The district court dismissed Rodriguez's claim because the VPPA did not provide a private right of action for retention of information, and because disclosure of personal information between the related Sony corporate entities in the ordinary course of business is permitted under the VPPA.

Consistent with the reasoning of the Seventh Circuit in *Sterk v. Redbox Automated Retail*[9] and the Sixth Circuit in *Daniel v. Cantrell*,[10] the Ninth Circuit concluded that Section 2710(c) of the VPPA created a private right of action only for the unlawful disclosure of personal information, not for unlawful retention. This is because the statute is structured so that the private right of action section of the act appears after the disclosure prohibition section rather than after all the provisions in the section, creating the impression that the private right of action is only for disclosure prohibition. Furthermore, the language of the unlawful retention statute was directed to the entity being regulated rather than the party seeking relief. In so ruling, the court also observed that awarding damages or other forms of relief would be illogical for unlawful retention because no injury would occur absent disclosure.

The court also affirmed the district court's dismissal of Rodriguez's unlawful disclosure claim pursuant to the VPPA's exemption for disclosures made "incident to the ordinary course of business of the video tape service provider." In his first complaint, Rodriguez alleged that Sony Computer "shared, sold, and/or transferred" his personal information to Sony Network after Sony Network "took over" the PlayStation Network. However, the VPPA expressly includes "transfer of ownership" in its definition of "ordinary course of business." Rodriguez then amended his complaint to allege that Sony Network assumed management and not ownership of the PlayStation Network. The Ninth Circuit held that the amendment was "unconvincing" because it completely contradicted Rodriguez's earlier pleading. The Ninth Circuit further held that intra-corporate disclosures are allowed under the VPPA because they were intended to support the videotape service providers' provision of services. Thus, even accepting Rodriguez's allegations that Sony Network assumed only the management of PlayStation Network, that service still falls into the "order fulfillment" or "request processing" exemptions of the VPPA.

Practice Points

This is the first time the Ninth Circuit has considered the VPPA as it relates to the retention of customer information. Prior to this decision, in 2012, Netflix settled for $9 million a class action lawsuit largely based on allegations that Netflix retained users' financial information and viewing history even after they canceled their accounts. Going forward, the *Rodriguez* decision substantially narrows plaintiffs' abilities to extract such settlement payments from video providers based on data disclosure and data retention claims, and further admonishes plaintiffs that courts do not have to accept amended pleadings with allegations that are factually inconsistent with their earlier pleadings.

Return to Table of Contents

[8] No. 12-17391 (9th Cir. Sept. 4, 2015).

[9] 672 F.3d 535 (7th Cir. 2012).

[10] 375 F.3d 377 (6th Cir. 2004).

Illinois Governor Vetoes Bill Expanding State's Privacy Law

The Illinois governor has vetoed a bill that would have expanded the state's data breach notification requirement to geolocation and consumer behavior data, and would have required companies to post a privacy policy.

Although many states have looked to expand their privacy and data breach notification laws, Illinois Gov. Bruce Rauner has issued an amendatory veto to Illinois' state data breach notification law — the Illinois 2005 Personal Information Protection Act (PIPA) — stating that the proposed amendment, Senate Bill 1833 (SB 1833), "goes too far, imposing duplicative and burdensome requirements that are out-of-step with other states." The amendment would have, among other changes, (1) expanded the definition of "personal information" to include geolocation information and consumer marketing (*e.g.*, browsing and purchasing history), and (2) required all websites and online services processing Illinois residents' PII to post a privacy policy.[11]

According to Rauner, consumer marketing and geolocation information do not pose the same degree of risk to consumers that justifies the notification burdens PIPA imposes and should not be included within PIPA's definition of personal information.[12] The governor also stated that including these categories is economically unjustifiable and out-of-step with other states' data privacy laws.

Rauner also challenged PIPA's requirement that entities draft and make public privacy policies. Since California already has such a law, Rauner said that imposing such a requirement in Illinois is duplicative for national large businesses that must already comply with the California requirement. Moreover, for small businesses, the cost of complying with the requirement is burdensome and potentially prohibitive — particularly because no other state makes similar requirements. According to Rauner, the law illustrates how overregulation has created a "hostile economic environment" in Illinois, and he would like to correct this by encouraging economic expansion — including by narrowing the proposed bill's breadth.

[11] *See* full text of Rauner's address to the Illinois Senate.

[12] As proposed, consumer marketing information refers to "information related to a consumer's online browsing history, online search history, or purchasing history, including, but not limited to, consumer profiles that are based upon the information" not held by a data collector with a direct relationship with the consumer. Geolocation information is defined as "information generated or derived from the operation or use of an electronic communications device that is stored and sufficient to identify the street name and the name of the city or town in which an individual is located and the information is likely to enable someone to determine an individual's regular pattern of behavior." For more, see Illinois Senate Bill 1833.

Practice Points

Rauner's challenge to the proposed PIPA expansion is atypical in a year that has seen several states, including Connecticut, Montana, Nevada and North Dakota, adopt more rigorous data breach notification policies. However, none included SB 1833's identification of marketing and geolocation data as "personal information." Rauner's opposition to the bill were echoed by advertising and other trade groups. Declaring that the types of information contained within geolocation data and consumer marketing information are unlikely to be used to perpetrate fraud, the groups wrote to the Illinois Senate that "[n]o other state has defined 'consumer marketing data' and 'geolocation' as 'personal information.' This radical definition would put Illinois far outside the mainstream of responsible and effective state breach notification laws, while failing to help Illinois residents defend themselves against fraud borne of a data breach."[13] Given the prevalence of marketing and geolocation information, and their integration into everyday social and economic life, the conflict indicates that marketing and geolocation data may present the next major area of dispute in defining what is personal information.

Return to Table of Contents

EU and US Enter Into Data Protection 'Umbrella Agreement'

The EU and U.S. have entered into an umbrella agreement to enhance law enforcement capabilities in the face of increasing cyberattacks.

On September 8, 2015, the EU commissioner for justice announced that the EU and United States had "finalized negotiations" on a so-called "umbrella agreement" aimed at establishing a data protection framework for EU-U.S. law enforcement cooperation. The EU Commission has not released a copy of the agreement; the outline below is therefore based on information the EU Commission has disclosed.

Procedural History

In March 2009, the European Parliament called for an EU-U.S. agreement that would ensure adequate protection of civil liberties and personal data protection.[14] On December 2009, the European Council invited the European Commission to propose a recommendation on this matter, and the commission

[13] *See* "Ad Industry Opposes Illinois Data Breach Bill."

[14] European Parliament Resolution of March 26, 2009, on the state of transatlantic relations in the aftermath of the U.S. elections.

proposed a draft mandate for negotiating an agreement with the United States in May 2010. On this basis, the EU justice minister approved the start of EU-U.S. talks in December 2011, and negotiations officially began on March 29, 2011.[15]

This was not the first time that the EU and the United States had entered into negotiations and reached an agreement with respect to personal data.[16] However, the negotiations on the umbrella agreement have been hindered by the diplomatic climate and, in particular, the U.S. surveillance scandal involving the NSA from 2013 to 2015, as well as the difficult, parallel discussion on the Transatlantic Trade and Investment Partnership (TTIP).

Purpose

The umbrella agreement's objectives are to (1) facilitate EU-U.S. law enforcement (police and judicial) cooperation, (2) harmonize and strengthen safeguards and guarantees of lawfulness for data transfers, in particular with regard to fundamental rights, and (3) ensure equal treatment between European and U.S. citizens in this matter. It covers all personal data (*e.g.*, names, addresses, criminal records, etc.) exchanged across the Atlantic for the purpose of prevention, detection, investigation and prosecution of criminal offenses, including — but not limited to — terrorism.[17] Transfers for purposes other than criminal matters, *e.g.*, commercial purposes, are not covered by the agreement.

The main features announced are (1) clear limitations on data use, (2) consent by the country of origin's competent authority before transferring data to non-U.S./non-EU states, (3) maximum data retention periods, (4) right to access and rectification, and (5) notification mechanism of data security breaches to competent authorities and data subjects.

Judicial Redress

The umbrella agreement would allow EU citizens not residing in the U.S. to have the right to seek judicial redress where U.S. authorities (1) denied them access or rectification or (2) disclosed their personal data. On the contrary, U.S. citizens already have the option to seek for redress before European courts.

Final Adoption

The final adoption of the umbrella agreement remains subject to political uncertainty. On the European side, the commission will propose the agreement to the council, and the council will adopt it after obtaining the European Parliament's consent. On the U.S. side, the agreement may only be signed after the adoption of the Judicial Redress Bill, which is the key hurdle. The 2015 Judicial Redress Act, which would extend the scope of the 1974 U.S. Privacy Act's remedies to EU citizens, was introduced on March 18, 2015. This bill would allow the U.S. attorney general (with the concurrence of the Departments of State, Treasury and Homeland Security) to designate countries whose citizens may — as U.S. citizens are able to — bring a civil action before the U.S. District Court for the District of Columbia against an agency and obtain civil remedies for:

(1) disclosure of their personal information in violation of their rights. For EU citizens, such right would be expressly limited to intentional or willful disclosures; or

(2) failure to comply with a request to gain access to — but not a request to amend — their record or any stored personal information.

The bill would not allow EU citizens to sue companies for privacy breaches that take place in the U.S. However, such right would be subject to the same exemptions as the one applying to U.S. citizens, which protect many enforcement agencies. These exemptions include, among others, information (1) compiled in reasonable anticipation of a civil action or proceeding, (2) maintained by the CIA, (3) maintained by an agency which performs as its principal function any activity pertaining to the enforcement of criminal laws and for the purpose of identifying individual criminal offenders and alleged offenders, and consisting only of identifying data and notations of arrests, (4) compiled for the purpose of a criminal investigation, (5) classified under an executive order in the interest of national defense or foreign policy, or (6) required by statute to be maintained and used solely as statistical records. Given these exemptions, it remains to be seen whether the Judicial Redress Bill, even if passed, would be sufficient to satisfy EU officials.

Return to Table of Contents

China Adopts Privacy and Cybersecurity Criminal Law

China has amended its criminal law to address the growing issue of cybercrimes in that country.

On August 29, 2015, the National People's Congress, China's legislature, adopted the Ninth Amendment to the Criminal Law, which will become effective on November 1, 2015. The amendment introduces significant developments on privacy and cybersecurity in the following five areas:

[15] IP/10/609; MEMO/10/216; IP/10/1661; MEMO/11/203.

[16] In November 2000, the EU and U.S. Department of Commerce agreed on the Safe Harbor principles to regulate the way that U.S. companies handle European citizens' personal data. (The U.S. is not recognized by the European Commission as a country with "adequate" levels of protection for personal data.) The Safe Harbor arrangement is currently being renegotiated.

[17] MEMO/15/5612 (Q&A).

1. Enhanced Protection of Personal Information

Prior to the amendment, criminal sanctions for illegally selling or providing personal information only applied to employees in certain selected industries where employees were likely to have access to personal data, including government, finance, telecommunications, transportation, education and health care. The amendment removes the industries limitation and simply provides that anyone who sells or provides personal information to third parties in violation of the law is subject to criminal sanction if the circumstances of the violation are considered "serious." (This term is not defined.)

Previously, a serious violation was punishable by a fine and/or imprisonment (or detention) of no longer than three years. The amendment further introduces the concept of a "particularly serious" violation (this term also is not defined), where the violator may be subject to imprisonment for three to seven years, plus a fine. In addition, if the information illegally sold or provided was obtained during the conduct of duties or provision of services to a third party, the violator will be punished at the harsher range of the penalty.

2. Network Service Providers' Obligations to Ensure Network Security

The amendment adds a punishment for network service providers who fail to fulfill network security administration obligations required under relevant laws and regulations if such failure results in (1) widespread dissemination of illegal information, (2) a leak of users' personal information that have serious consequences, (3) loss of evidence for a criminal claim, and the circumstances are considered serious, or (4) other serious circumstance. The penalties include imprisonment (or detention or surveillance) of up to three years and/or a fine.

3. Criminal Liabilities for Facilitating Illegal Activities Via Information Networks

The amendment adds a new provision imposing criminal liabilities on anyone who facilitates illegal activities via information networks, including by establishing websites or communication groups, or publishing information for or with respect to illegal activities, and who knowingly provides technology support or other advertisement, marketing, payment or clearance services therefor, if the circumstances are considered serious. The penalties include imprisonment (or detention) of up to three years and/or a fine.

4. Criminal Liabilities for Fabricating and Disseminating Information Harmful to National Security

Under the amendment, anyone who fabricates and knowingly disseminates false information relating to emergencies, epidemics, disasters or other incidents threatening public security over information networks or mass media, which seriously disrupts the public order, faces imprisonment (or detention or surveillance) of up to three years. If the action leads to serious consequences, the penalty increases to three to seven years' imprisonment.

5. Government Assistance in Evidence Collection

The amendment also allows a court to require the public security authority to provide assistance in collecting evidence from an information network if there is a complaint of criminal defamation through that network.

Return to Table of Contents

Senators Request Updated Information From Auto Industry Regarding Cybersecurity

Two U.S. senators have sent new requests to the auto industry asking for information on how the industry protects vehicles from cyberattacks.

U.S. Sens. Edward Markey, D-Mass., and Richard Blumenthal, D-Conn., continue to lead the effort to push automakers into increasing cybersecurity and privacy protections in vehicles. On September 16, 2015, Markey and Blumenthal sent a letter to 18 automakers, including Ford Motor Company, Lamborghini and Tesla, requesting that they provide updated information regarding the vehicles' technological capabilities as well as the companies' efforts to protect consumer privacy and safety. The senators' letter follows up on their December 2013 request for similar information. At that time, Markey collected the responses to the letter and in February 2015 published a report detailing the risks consumers face due to inadequate security measures automakers had taken. The September 2015 request aims to gather updated information regarding 2015 and 2016 vehicles as well as any changes the automakers have made in their approach to cybersecurity and data privacy in the intervening years.

In the September 2015 letter, the senators highlight recent studies and incidents as evidence that vulnerable vehicles pose a risk to consumers' personal information and safety. Specifically, the letter points toward two highly publicized reports by Andy Greenberg of *Wired* magazine. In July 2015, Charlie Miller and Chris Valasek demonstrated that they could remotely hack of a Jeep Cherokee and control the vehicle's radio, transmission, brakes and steering.[18] In August 2015, a group of researchers at the University of California San Diego led by Stefan Savage

[18] Read the article here.

demonstrated they could hack a 2013 Corvette by sending specifically designed text messages which allowed the hackers to activate windshield wipers and disable a vehicle's brakes.[19]

Markey and Blumenthal have sponsored legislation that seeks to require automakers to meet cybersecurity standards for vehicles. In response to the February 2015 report, the Alliance of Automobile Manufacturers and the Association of Global Automakers have released a set of voluntary privacy standards. The senators note that these actions are a "step in the right direction"; however, they call on automakers to do more because the voluntary guidelines fail to address the issues. Responses to the letter are due on October 16, 2015.

Further details regarding auto-hacking can be found in our August 2015 *Privacy & Cybersecurity Update*.

Return to Table of Contents

US Prosecutor to Be Posted at Europol to Support Cybercrime Investigations

The U.S. has agreed to post a prosecutor at Europol to help prosecute cybercrimes, including by resolving jurisdictional issues that often arise in these cases.

U.S. Attorney General Loretta Lynch has announced that the U.S. will post a prosecutor at Europol, Europe's police agency, to enable closer cooperation on international cybercrime investigations. Lynch referenced resolving jurisdictional issues in an ongoing investigation as one example of how such a prosecutor would help. Europol's expectation is that the presence of a U.S. prosecutor will facilitate cooperation by U.S.-based technology companies in international cybercrime investigations.

Return to Table of Contents

[19] Read the article here.

FBI Issues Warning on the Security of the Internet of Things

The growing popularity of Internet-enabled devices such as wearable fitness trackers has created cybersecurity concerns. The FBI has issued an alert on the potential harm and what consumers should be doing to minimize their risks.

As we have reported in previous newsletters,20 the "Internet of Things" — physical objects or devices that connect to the Internet and automatically send and/or receive data, such as wearables — present enormous benefits but also new types of cybersecurity risks.

On September 10, 2015, the FBI weighed in on this issue with a warning on the cybersecurity risks these devices present and offered tips on how consumers and businesses can protect themselves.

The FBI noted that weak security capabilities as well as difficulties in patching vulnerabilities make these devices welcome targets for hackers. The main risks, according to the FBI, are:

- Exploiting the Universal Plug and Play protocol (UPnP) — the process through which a device remotely communicates on a network automatically without authentication — to gain access to devices;
- Exploiting the default passwords used on many devices to send malicious emails and spam, or to steal personally identifiable or credit card information;
- Compromising a device to cause physical harm;
- Overloading a device to render it inoperable; and
- Interfering with business transactions.

Such attacks can allow hackers to access individuals' personal, health and financial information and interfere with business operations.

[20] For earlier reports on the Internet of Things, see our January 2015, March 2015 and May 2015 *Privacy & Cybersecurity* updates.

The FBI has offered a number of steps that users of such devices can take to minimize the risk of a cyberattack, including:

- Isolating devices on their own protected networks;
- Disabling UPnP on routers;
- Purchasing devices from manufacturers with a track record of providing secure devices;
- Installing security patches when they become available; and
- Changing default passwords to strong passwords and only operating the device on a home network with a secured Wi-Fi router.

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

Cyrus Amir-Mokri
Partner / New York
212.735.3279
cyrus.amir-mokri@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 A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

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

Anastasia T. Rockas
Partner / New York
212.735.2987
anastasia.rockas@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