Skadden

PRIVACY & CYBERSECURITY UPDATE

APRIL 2014

CONTENTS

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 14, or your regular Skadden contact.

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

Four Times Square
New York, NY 10036
212.735.3000

DECISION IN WYNDHAM CASE PROVIDES FTC WITH SIGNIFICANT VICTORY

In a much-anticipated decision with potentially broad implications, a district court denied Wyndham Hotels and Resorts, LLC's motion to dismiss a Federal Trade Commission enforcement action alleging that Wyndham had violated Section 5 of the Federal Trade Commission Act as a result of a cybersecurity attack. Judge Esther Salas' April 7, 2014, decision in *FTC v. Wyndham Worldwide Corporation, et al.*,[1] addresses the scope of the FTC's authority over cybersecurity at a time when it is taking a greater enforcement role in such incidents and privacy more generally.

BACKGROUND

Between April 2008 and January 2010 Wyndham suffered three separate cyberattacks in which intruders gained unauthorized access to Wyndham computers that stored customers' personal information. According to the FTC's complaint, the three data breaches resulted in the compromise of over 619,000 consumer payment card account numbers, many of which were exported to a domain registered in Russia, resulting in fraudulent charges and more than $10.6 million in fraud loss.

In June 2012, the FTC filed suit against Wyndham alleging that the hotel chain had engaged in unfair and deceptive acts by failing to provide reasonable and appropriate security for the personal information it collected and maintained, by engaging "in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft" and by making statements in its privacy policy that it used industry standard measures to protect customer information. The FTC also alleged that Wyndham had failed to take appropriate actions to prevent further compromises once it became aware of the initial breaches.

The FTC's action against Wyndham was consistent with the position it has taken in other cases. In general, the FTC has claimed that inadequate security measures resulting in harm to consumers can violate Section 5 of the FTC Act's, which prohibits "unfair" business practices. Further, in some cases, the FTC has argued that a company violates Section 5's ban on "deceptive" business practices when it falsely claims to take adequate or reasonable steps to protect the customer's data.

Wyndham moved to dismiss, asserting that the FTC lacked authority to bring such an action, focusing in particular on the FTC's efforts to punish "unfair" business practices.

THE COURT'S DECISION

The court rejected each of Wyndham's arguments, and in doing so, gave wide latitude to the FTC's enforcement powers in the areas of privacy and cybersecurity.[2]

---

[1] *Federal Trade Commission v. Wyndham Worldwide Corp. et al.*, No. 2:13-cv-01887-ES-JAD, 2014 BL 94785 (D.N.J. Apr. 7, 2014).

[2] Wyndham has submitted a motion for interlocutory appeal, requesting that Judge Salas permit Wyndham to seek an immediate appeal to the Third Circuit on the issues raised in its motion.

SCOPE OF THE FTC'S AUTHORITY

Wyndham asserted that the FTC lacked broad sweeping authority in the area of cybersecurity since: (a) Congress instead had settled on a "less extensive regulatory scheme" by passing narrowly tailored privacy legislation such as the Children's Online Privacy Protection Act and the Gramm-Leach-Bliley Act; (b) Congress recently had proposed a number of bills giving the FTC broader cybersecurity authority, thereby proving that such authority did not currently exist; and (c) the FTC itself had disclaimed its authority to regulate data security through recent public statements seeking broader powers in this area and suggesting that the agency's existing authority generally was limited to deceptive, as opposed to unfair, practices.

The court disagreed, holding that specific privacy laws only served to complement, not preclude, the FTC's broad authority to enforce privacy and cybersecurity. With respect to the FTC's own statements about the scope of its authority, Judge Salas found that these statements were not resolute or unequivocal enough to warrant a data security exception to the FTC's general authority to regulate unfair practices.

ABSENCE OF FTC SECURITY RULES

Wyndham argued that to satisfy fair notice and due process principles, the FTC was required to publish formal rules, regulations or other guidelines regarding appropriate data security practices before it could file a Section 5 unfairness claim. The court disagreed, holding that the FTC had discretion to proceed by rulemaking or by individual adjudication, especially in areas that were not reasonably foreseeable like cybersecurity. Judge Salas also noted that accepting Wyndham's argument would require the FTC to issue formal regulations prior to acting in any context, which would contradict years of jurisprudence in which the FTC brought unfairness actions where there were no preexisting regulations. Perhaps most importantly, the court held that the FTC's informal guidance, through best practice publications and the body of existing FTC complaints and consent orders, provided sufficient notice of the FTC's position on cybersecurity.

PRESENCE OF CONSUMER INJURY

Wyndham also brought various challenges regarding the sufficiency of the FTC pleadings, including with respect to causation and the scope of injury to consumers. For example, Wyndham asserted that consumers could not suffer substantial injury from a breach of their credit card information since major credit card brands generally limit or even waive a consumer's liability for fraudulent charges. The court rejected Wyndham's arguments, finding that Wyndham effectively was arguing for a heightened pleading standard beyond the "unfairness" standard codified in Section 5. The court also refused to find as a matter of law that financial injury from payment card theft could never be substantial. Finding the financial harm pleaded by the FTC, accepted as true for purposes of the motion, sufficient by itself, Judge Salas did not rule on whether non-monetary injury, such as time spent mitigating harm caused by fraudulent charges, is cognizable as a matter of law under Section 5.

In summary, the court found that:

- the FTC has general authority to regulate cybersecurity as an unfair trade practice under Section 5, even though there are no specific cybersecurity laws or regulations granting the commission this general authority;
- the FTC does not need to promulgate rules or regulations regarding cybersecurity standards before it can bring a Section 5 claim; and
- despite the protection offered by credit card companies against fraudulent charges, the FTC alleged sufficient potential injury to consumers to support a Section 5 claim.

It is also important to note that the court's decision did not establish that Wyndham had violated Section 5. Whether Wyndham engaged in unfair practices still needs to be litigated unless the case is now settled.

IMPACT OF THE COURT'S DECISION

The case marks the first time a court has explicitly upheld the FTC's regulatory authority over cybersecurity under the FTC Act and its right to sue companies under Section 5 for not maintaining reasonable data security safeguards. While Judge Salas noted that her decision "does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked," the court's broad findings will make it difficult for future defendants to challenge the FTC's authority in this area. The case also leaves open exactly what types of cybersecurity practices are required to withstand a Section 5 unfairness claim.

The case may serve to embolden the FTC to be more aggressive in pursuing companies that have suffered cybersecurity attacks. However, many have noted that the case merely supported the FTC's practice to date and does not broaden its authority. Moreover, the FTC has, to date, gone after companies where, most would agree, the security lapses were egregious. Indeed, in the *Wyndham* case, the FTC alleged in part that Wyndham failed to employ firewalls; permitted "storage of payment card information in clear readable text"; and permitted Wyndham-branded hotels to use servers with outdated operating systems that could not receive security updates.

PRACTICE POINTS

The court's decision in *Wyndham* effectively requires companies to monitor FTC enforcement activity so they can draw conclusions as to what practices the FTC has deemed "unfair." The challenge companies face in undertaking this exercise is that such enforcement actions are often heavily fact-dependent, making it difficult to draw broad conclusions. Companies also should pay particular attention to any informal guidance issued by the FTC, such as booklets or statements, and keep abreast of general industry standard practices. The challenge here is that the FTC statements are often very general, and industry standard practices in the area of cybersecurity are continuously evolving. Nonetheless, by monitoring these various sources, companies should be able to compile a general best practices checklist to guide their policies in this space and avoid an FTC enforcement action.

SEC ANNOUNCES CYBERSECURITY INITIATIVE

On April 15, 2014, the staff of the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert announcing a Cybersecurity Initiative to conduct cybersecurity-focused examinations of more than 50 registered broker-dealers and registered investment advisers. The Risk Alert is the latest in a series of SEC communications related to cybersecurity. The National Exam Program Examination Priorities for 2014 included cybersecurity preparedness as an examination priority,[3] and at an SEC-sponsored Cybersecurity Roundtable on March 26, 2014, Chair Mary Jo White commented on the "compelling need for stronger partnerships between the government and the private sector" in addressing cyber threats. The Risk Alert provides securities industry participants with more detailed information relating to the OCIE's Cybersecurity Initiative.

The Cybersecurity Initiative is designed to assess cybersecurity preparedness in the securities industry and to collect information from securities industry participants relating to their recent

[3] The National Examination Priorities for 2014 are available at http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf.

experiences with cybersecurity threats. The examinations generally will focus on cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.

The OCIE will request copies of all relevant policies such as written information security policies, written business continuity of operations plans, written data destruction policies and written cybersecurity incident response policies. It also will be inquiring into each firm's risk assessments to identify cybersecurity threats, vulnerabilities and business consequences and physical security threats, including the frequency of such assessments.

Pursuant to the request, firms will need to:

- identify a chief information security officer (or similar position);
- disclose whether the firm maintains cybersecurity insurance;
- provide detailed information as to how they protect their networks;
- provide information as to whether they conduct risk assessments of vendors and business partners with access to their networks or information;
- detail practices used to detect unauthorized activity on networks and devices;
- disclose whether they have updated their procedures to reflect the Identity Theft Red Flag Rules; and
- provide details as to all cybersecurity breaches and incidents, such as information theft or unauthorized use of information.

Registered broker-dealers and registered investment advisers should review or prepare their cybersecurity policies, procedures and preparedness in light of the issues.

HEARTBLEED BUG GENERATES SIGNIFICANT SECURITY CONCERNS

In late March and early April , software engineers at Google and Codenomicon, a small cybersecurity firm in Finland, independently identified a serious security flaw, dubbed the Heartbleed bug, in certain versions of OpenSSL — an open source encryption software widely used in common network services, including email, instant messenger/chat services, web servers, virtual private networks (VPNs) and other applications. The servers of many companies reportedly were affected, including OKCupid, Box, Dropbox and Yahoo (Google and Facebook stated that they patched the vulnerability on their systems before the flaw was disclosed publicly).

In the weeks that have followed, the Heartbleed bug continues to make headlines due to the seriousness of the flaw, which potentially disclosed encrypted communications — including passwords, credit card numbers and other sensitive data — across the Internet since June 2012. Security experts have determined that the security hole potentially can be used to reveal a web server's private encryption key, thus rendering all future communications with that server vulnerable until the hole is patched. While a fix is now available, the full ramifications of the Heartbleed bug remain unclear, as companies, regulators, and individuals continue to monitor the situation.

IMMEDIATE EFFECTS

Thus far, there have been few reports of the Heartbleed bug being used to compromise systems or steal data. For example, on April 10, 2014, the Canadian Revenue Agency (CRA) temporarily shut down access to its online services in light of the Heartbleed vulnerability, and a few days later announced that the Social Insurance Numbers of approximately 900 taxpayers were compromised. The following day, a 19-year-old Canadian was arrested for his alleged role in the breach of the CRA website. More recently, according to the cybersecurity firm Mandiant, an attacker was able to leverage the Heartbleed vulnerability to hijack multiple active VPN user sessions.

While there have been few reports of Heartbleed attacks, an unfortunate aspect of the bug is that a successful exploit leaves no trace of the incursion. As a result, we may never know if cybercriminals, government-backed espionage groups or others were aware of, and used, the flaw to their advantage prior to the public announcement on April 7, 2014. Undoubtedly in light of the 2013 Edward Snowden revelations, the U.S. federal government and the NSA to disclaim publicly any knowledge or use of the bug.[4]

Regardless of how hackers leverage the Heartbleed bug, the short-term costs to companies and individuals are sure to be high. Companies are spending many man-hours ensuring that their servers are no longer vulnerable; contacting customers to ensure that they are aware of the issue and update their passwords; and taking additional steps to scan their systems for potential security breaches or suspicious activity.

LONG-TERM EFFECTS

While the short-term effects of the Heartbleed bug may be difficult to measure, the long-term effects are likely to be more significant. As with any security breach that impacts multiple organizations, there is the potential for an increase in identity theft and similar crimes. Some have cautioned that if an organization is able to decipher that the Heartbleed bug was the cause of its breach, it cannot argue that the compromised data was encrypted (and therefore notice to consumers is not required), since the very essence of Heartbleed is to break through a site's encryption.

In addition, many have highlighted the fact that the affected OpenSSL software was developed and maintained by a small group of programmers. Heartbleed has therefore focused on the many pieces of open source software that are critical to the operation of the Internet and cybersecurity, but that are maintained by small groups. Whether this has a negative effect on open source software generally, or at least its use for critical services or systems, remains to be seen. Critics of open source software point out that submissions to open source projects can be made by anyone, regardless of their level of competency, and the review process is ultimately only as good as the reviewers who volunteer their time to the projects.

While the Heartbleed bug is unlikely to spell the demise of the open source software movement, companies relying on open source for IT security or other critical systems might consider an independent audit of the quality of such code on an ongoing basis. Companies might also consider participating in the maintenance and review of such code, thereby benefiting not only themselves, but also the community at large. To that end, it is noteworthy that a group of technology companies, including Microsoft, Facebook, Google and IBM, have committed to provide $100,000 a year for a minimum of three years as part of the Core Infrastructure Initiative. The funds, which already amount to $3 million, will support projects that improve open source software and might be used to pay developers to work on new projects, to fund

---

[4] See Official Statement, Office of the Director of National Intelligence, available at http://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew.

security audits or to improve computing infrastructure. Not surprisingly, the first project that might be funded will be OpenSSL.

PRACTICE POINTS

General Guidelines. The FTC recommends that anyone running a vulnerable version of OpenSSL take the following steps:

- update to the newest version of OpenSSL and reboot servers;
- generate new encryption keys;
- obtain a new SSL Certificate; and
- notify employees and customers that they should change their passwords on the affected system and any other accounts for which the same password is used.

The FTC also recommends that individuals monitor their bank and credit card accounts, especially over the next few weeks.

Public Companies. Companies vulnerable to Heartbleed should work expeditiously to patch their systems and alert customers about any potential harms. Affected public companies also should consider whether the vulnerability warrants disclosure in its public filings or with their applicable regulators.

Financial Institutions. For financial institutions, regardless of whether their servers were affected by the Heartbleed bug, the Federal Financial Institutions Examination Council (FFIEC) suggested taking the following actions, as appropriate:

- ensure that third party vendors that use OpenSSL on their systems are aware of the vulnerability and take appropriate risk mitigation steps;
- monitor the status of the vendors' efforts;
- identify and upgrade vulnerable internal systems and services; and
- follow appropriate patch management practices and test to ensure a secure configuration.

The FFIEC alert also suggests that financial institutions consider replacing private keys and X.509 encryption certificates after applying the patch for each service that uses the OpenSSL library and requiring users and administrators to change passwords after applying the OpenSSL patch.

FTC AND DOJ ANNOUNCE POLICY REGARDING THE SHARING OF CYBER THREAT INFORMATION

Law enforcement officials and cybersecurity experts have long said that sharing cyber threat information is a critical component in preventing cyberattacks. Many companies, however, are concerned that sharing information with competitors might constitute an antitrust violation. Congress has recognized this issue and proposed legislation such as the Cyber Intelligence Sharing and Protection Act of 2013 that would allow companies to share cybersecurity information and with the government notwithstanding laws that might prohibit such exchanges. However, given the low probability that any such legislation would be enacted, and to address concerns regarding the sharing of cyber threat information, the FTC and the DOJ released a joint statement on April 10, 2014, addressing their policy with respect to private entities sharing such information and its implications for antitrust concerns.

In their statement, *Department Of Justice And Federal Trade Commission: Antitrust Policy Statement On Sharing Of Cybersecurity Information*,[5] the two agencies acknowledged that an important way to protect against cyber threats in the U.S. is for companies to share information such as incident reports, alerts, indicators and threat signatures. The FTC and DOJ emphasized that antitrust laws do not, and should not, restrict private entities from sharing such information. As the agencies explained, information sharing agreements generally are analyzed under a "rule of reason analysis," which considers the overall competitive effect of an agreement. Under such an analysis, antitrust concerns are lower when the information being shared is not competitively sensitive. The two agencies note that cybersecurity information is unlikely to include information such as pricing, output data and business plans, and therefore is less likely to violate the rule of reason analysis. The information critical to preventing cyber threats is "very technical in nature and very different" than competitively sensitive information and highly unlikely to lead to a reduction in competition.

The agencies' statement builds on the DOJ's previous guidance of October 2000 in which, in a business review letter to the Electric Power Research Institute, Inc., the DOJ confirmed it would not bring an enforcement action against the company in response to the company's proposal to share real-time cyber threat and attack information. The joint statement represents another important step in the government encouraging information sharing to combat cybersecurity and to increase the security and integrity of the nation's information systems.

PRACTICE POINT

Although the DOJ and FTC statement provides the means through which companies can share cyber threat information, communications with competitors always raise concerns. Companies should consult with counsel before engaging in such information.

KEY DEVELOPMENTS IN STATE DATA BREACH NOTIFICATION LAWS

In April, four states took steps to introduce or strengthen their data breach notification laws. Kentucky passed a data breach notification law, making it the 47th state to do so. Iowa passed a bill that strengthened its data breach notification law, and lawmakers in Florida and California recently introduced legislation that would toughen data breach notification requirements. These actions are further proof that states are continuing to shape the data breach notification landscape in the absence of a national data breach law.

KENTUCKY

On April 10, Kentucky passed a data breach notification law that requires businesses to notify consumers if a security breach might have resulted in the unauthorized acquisition of consumers' personally identifiable information.[6] Like the majority of states, the statute defines data breach such that notice is only required when malicious conduct is known or suspected, not for inadvertent breaches. Notifications must be delivered "in the most expedient time possible and without unreasonable delay," but companies may delay notification if required by law enforcement or to determine the extent of the breach and restore system integrity. Although the scope of the law is generally consistent with other states' data breach notification laws, it contains one unique provision that is aimed at protecting the data of K-12 students stored in the cloud. The law prohibits cloud providers from processing such student data for any purpose other than providing cloud computing services, unless it has received express parental

[5] Available at http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf
[6] H.B . 232, 2014 Leg., Reg. Sess. (Ky. 2014).

permission. The passage of a data breach law in Kentucky leaves Alabama, South Dakota and New Mexico as the only three states without such laws.

IOWA

Iowa took steps to strengthen its existing data breach notification laws. On April 3, Governor Terry Branstad signed into law an amendment to the state's data breach notification law that now requires notice be sent to the Office of the Attorney General within five business days of consumer notification for breaches affecting more than 500 people.[7] The amended law also expands the definition of "breach of security" to include personal information transferred from a computer to any medium, including paper. It previously limited a breach to simply unencrypted computerized data, which meant that breaches of personal information in paper form would not have constituted a breach requiring notice. The new law also adds credit and debit card expiration dates when combined with the credit or debit card number to the list of "personal information" subject to breach notification requirements.

FLORIDA

On April 23, the Florida Senate passed a bill that would replace the state's existing data breach law.[8] The proposed law would require businesses and government entities to notify consumers of a breach within 30 days and provide notice to the attorney general's office when the breach affects more than 500 individuals. Failure to notify the attorney general would subject an entity to civil penalties of up to $500,000. The proposed bill also requires commercial and government entities that maintain, store or use personal information to take measures to protect and secure personal information stored in an electronic format. They are also required to dispose of such personal information through "reasonable methods" when the information is no longer required.

CALIFORNIA

In California, the first state to enact a data breach notification law, legislation has been introduced that would toughen data protection standards.[9] The proposed legislation would prohibit business who sell goods and services to California consumers from storing payment-related data, except as expressly permitted by a payment data retention and disposal policy that limits (a) the amount of data stored and (b) the time that data is retained. In the latter cases, data may be retained only to the amount and time required for explicitly documented business, legal or regulatory purposes. Businesses also would be prohibited from storing sensitive authentication data (even if it is encrypted) after authorization, including full credit or debit card number, PIN numbers, social security numbers or driver's license numbers. In addition, the bill would require businesses that suffered a data breach to reimburse card issuers for the cost of providing replacement cards and to offer identity theft prevention mitigation services to affected customers at no cost. Finally, the bill also would require businesses that maintain but do not own the data, such as cloud services providers, to alert those affected by a data breach within 15 days. The assemblymen who introduced this bill pointed to the Target and Niemen Marcus data breaches as evidence of a need for stricter standards.

---

[7] S.F. 2259, 85th. Gen. Assemb. (Ia. 2014).
[8] S.B. 1524 2014, Reg. Sess. (Fl. 2014).
[9] A.B. 1710, 2014. Leg., Reg. Sess. (Ca. 2014).

EU COURT OF JUSTICE STRIKES DOWN DATA RETENTION DIRECTIVE

In an important new development in the EU's attempt to strike a balance between security and privacy, the European Court of Justice declared on April 8, 2014, that the EU's 2006 Data Retention Directive[10] is invalid. The court ruled that the directive, which requires communications services providers to retain data for six to 24 months, entails "a particularly serious interference with those fundamental rights" of respect for private life and the protection of personal data. As a result, it "is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[11]

The decision was adopted following requests from Ireland's High Court and Austria's Constitutional Court, which asked the European Court to examine the validity of the directive in light of two fundamental rights guaranteed by the EU's Charter of Fundamental Rights, the right to respect for private life and the right to the protection of personal data.[12] The court carried out a proportionality analysis and found that the EU legislature had interfered with those rights beyond what was proportional in light of the legislators' security and crime-fighting objectives.

The court cited five main factors having led to this conclusion:

- **Overbroad data collection.** Although the directive does not impose the retention of the contents of conversations, it nevertheless covers all individuals, all means of communication and all traffic data, without tailoring such collection to law enforcement goals.[13]
- **Insufficient limits on government use of data.** The directive does not lay down objective criteria to determine when authorities may access an individual's data, leaving it up to each EU member state to define what "serious crime" justifies such interference with a person's fundamental rights.[14]
- **Overbroad data retention periods.** The directive requires each EU member state to define one blanket retention period between six months and two years, making no distinctions according to categories of data, persons concerned and the potential usefulness of the data.[15]
- I**nsufficient safeguards against abuse.** The directive does not provide sufficient protection against unlawful access and use of the data retained.[16]
- **Insufficient privacy protection for retained data.** The directive does not require data to be retained within the EU. As a result, it does not fully ensure compliance with EU data protection laws.[17]

This decision could affect the EU data privacy and law enforcement landscape in several ways. First, EU member states may alter their domestic laws transposing the directive. As noted above, the EU Court of Justice made this decision after referrals from the Irish and Austrian courts; the Data Retention Directive has likewise been the subject of Supreme Court litigation in Germany, where it was not fully implemented due to constitutionality concerns. Several states that struggled to transpose the directive into domestic law while ensuring respect of fundamental rights will now feel free to change their legislation.

---

[10] Directive 2006/24/EC of the European Parliament and the Council of March 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[11] *Digital Rights Ireland Ltd. et al. v. Ireland*, Joined Cases C—293/12 and C—594/12, European Court of Justice (Grand Chamber), April 8, 2014, §§ 37 and 65, http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=173571.
[12] Charter of Fundamental Rights of the European Union, 2000/C 364/01, articles 7 and 8, www.europarl.europa.eu/charter/pdf/text_en.pdf.
[13] *Digital Rights Ireland Ltd. et al. v. Ireland*, §§ 56-59.
[14] *Ibid.*, §§ 60-62.
[15] *Ibid.*, §§ 63-64.
[16] *Ibid.*, § 66.
[17] *Ibid.*, § 32, §§ 67-68.

Secondly, it is conceivable that past or current criminal cases resting on data collected on the basis of the directive could now be called into question. The court has not specifically limited the temporal effect of its judgment, and as a result, "the declaration of invalidity takes effect from the data on which the Directive entered into force" – that is, 2006.[18]

Thirdly, domestic law enforcement schemes resting on aggressive data collection and retention could be effected. For example, the U.K. government has been contemplating a data retention scheme allowing it to order Internet service providers and phone companies to collect and store customer data for up to 12 months. The plan has caused controversy within the coalition in government over recent months. It could now be much more difficult to implement.

Lastly, this decision will weigh on EU institutions as they work to overhaul Europe's privacy protection mechanisms. Advocacy groups such as Privacy International have hailed the ruling as a victory for privacy rights. The decision also comes on the back of the EU Parliament's vote for stronger data protection rules in a draft Data Protection Regulation last month, signaling a possible move towards stronger privacy protections. However, it remains up to EU legislators to draft a new, more narrowly defined directive that allows the retention and use of data to investigate serious crimes, while taking into account the proportionality imperative emphasized by the European Court of Justice.

EU INTRODUCES PROCESSOR TO SUB-PROCESSOR MODEL CONTRACT

One of the primary means that companies use to satisfy the transborder data flow restrictions imposed by the European Union Data Protection Directive are the so-called "model contracts." These contracts, which are literally form agreements provided by the EU, "adduce adequate safeguards" for protecting personal information. Signatories to these model contracts may therefore transfer personal information regarding EU citizens from any of the 27 EU member states and three European Economic Area member countries (Norway, Liechtenstein and Iceland) to countries that do not otherwise provide "adequate" data privacy protection.

The model contracts came in a variety of permutations, including "controller to controller" and "controller to processor." A "data controller" is the entity that is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data … ."[19] For all practical purposes, this is the entity that owns or controls the data and can determine how it is used and processed. A "data processor," in contrast, is the entity that "processes personal data on behalf of the controller,"[20] and is only authorized to perform data processing to the extent permitted given by the controller.

On March 21, 2014, the Article 29 Working Party, which is the key advisory body to the European Commission on privacy matters, proposed the addition of a new model contract from "processors" to "sub-processors." This new model contract is meant to address the growing reality that many EU-based data processors send personal information from the EU to sub-processors located outside the EU, often through the cloud. These draft model clauses must now be formally adopted by the European Commission before companies can take advantage of them.

---

[18] Court of Justice of the European Union, "The Court of Justice declares the Data Retention Directive to be invalid", Press Release No 54/14, April 8, 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.
[19] Article 2(d) of the EU Data Directive.
[20] Article 2(e) of the EU Data Directive.

In general, the structure and content of the processor to sub-processor clauses are similar to those included in the controller-to-processor model clauses, with certain key exceptions. Of course, the processor would need to first obtain the written consent of the data controller before it passed personal information onto a sub-processor under the new proposed model contract.

EU ARTICLE 29 EXPANDS DATA BREACH NOTIFICATION REQUIREMENTS

In an opinion adopted on March 25, 2014, the EU's Article 29 Data Protection Working Party (WP29) clarified the obligation for data controllers to notify data subjects of personal data breaches.[21] The WP29 is 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. Its opinions are not binding, although, given the make-up of its membership, they are typically seen as very persuasive.

Under current legislation, the notification obligation is limited to providers of electronic communications services. Such providers are required to notify data subjects in the event of a personal data breach that is likely to adversely affect such data subjects' personal data or privacy. This obligation will soon be expanded to all data controllers with the upcoming adoption of the EU General Data Protection Regulation. Anticipating the adoption of that regulation, the WP29 issued an opinion to provide general guidance for all data controllers "in order to help them to decide whether to notify data subjects in case of a personal data breach."

As the law currently stands, data controllers are obligated to take security measures to prevent personal data breaches. When breaches do happen, they have an obligation to notify the competent national Data Protection Authority, and when a breach is likely to affect the personal data or privacy of a data subject, they have an obligation to notify that subject. There is, however, an important exemption to the latter rule: data subjects do not need to be notified if the compromised information was encrypted previously or otherwise rendered unintelligible, so that the breach entails only negligible privacy risks. The new WP29 opinion helps controllers decide whether or not to notify data subjects in case of a breach.

WHEN SHOULD NOTIFICATION TAKE PLACE?

The WP29 provides a non-exhaustive list of examples where data subjects should be notified. The opinion categorizes breaches as "availability breaches" (accidental destruction or loss of data), "integrity breaches" (alteration of data) and "confidentiality breaches" (unauthorized disclosure of data). For example:

the employee of an Internet service provider gives a third party the login and password to access a company's client database. The data is encrypted, but login details give the third party access to a user interface with decrypted data. This is a "confidentiality breach," and clients must be notified; or

the encrypted laptop of a financial advisor is stolen. The data is encrypted, and the encryption key has not been compromised. However, the data was not backed up and has been lost, and subjects will need to give their information again. Some clients might also miss deadlines or suffer other adverse consequences. This is deemed an "availability breach," and since clients will be affected by the breach they must be notified.

---

[21] Opinion 03/2014 on Personal Data Breach Notification. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

WHEN NOTIFICATION IS NOT REQUIRED

The WP29 provides general guidance on cases that do not require notification. While this assessment must be made on a case-by-case basis, the WP29 outlines broad case scenarios that may give rise to an exemption. These are confidentiality breach scenarios where the data was obtained by unauthorized persons, but was previously encrypted using state-of-the-art technology, and the security key was not compromised. The data will be unintelligible to any person not authorized to access it.

KEY ISSUES

Finally, the WP29 discusses the main issues controllers might encounter in considering whether to notify data subjects. In particular:

- the definition of a personal data breach: a data breach is personal when the compromised data qualifies as personal data under the EU Data Protection Directive (Directive 95/46/EC), that is when a natural person is identified or identifiable, directly or indirectly, from the data; and
- in deciding whether to notify data subjects, all potential consequences and adverse effects on them, even of secondary order, should be taken into consideration.

The data subject must be notified even if he/she is the only person concerned by the breach.

STEPS TAKEN TOWARD 'DO-NOT-TRACK' SYSTEM

At the end of April the World Wide Web Consortium group (W3C) , working to develop a "do-not-track" protocol for Internet browsing, released a proposed standard signal to enable consumers to indicate that they do not want their data to be collected across different web-sites. Though much remains to be resolved, this development is a significant step towards a standardized do-not-track system.

BACKGROUND

In theory, a do-not-track system would enable consumers easily to request that online advertising networks not track their activities across different websites. When do-not-track was initially proposed to the FTC as a standard in 2007, consumers had to contact dozens of network companies individually, and each company had a different process for submitting such requests and different policies as to how, and if, those requests would be honored.

Since that initial proposal, do-not-track has followed a troubled path. The FTC endorsed the concept in a 2010 privacy report, one year after researchers developed a prototype. In 2010 and 2011, the major browsers began incorporating do-not-track technology into their prod-ucts, but the standards and protocols surrounding this technology were not uniform. Further, different browser developers took different approaches to the default setting for do-not-track (with Microsoft setting a default do-not-track request in its Internet Explorer product). Some advertiser networks said they would not honor do-not-track settings in browsers that enable them by default — on the theory that they wanted the do-not-track signal to reflect a specific choice by each consumer.

In 2011, the W3C — the technical standards setting organization for the world wide web — created a Tracking Protection Working Group to develop a do-not-track standard by 2012. Members of the group reflected an array of interests, including browser developers, adver-tising networks and consumer advocacy groups. Despite an initial sense of optimism, the

group's efforts were hampered by infighting and disagreements between members, resulting in some prominent defections and leadership changes. Key issues disputed included what was meant by "tracking" and "third party," and the situation became so dire that in the fall of 2013 the working group voted on whether to continue its work or disband without agreeing on a protocol.

Eventually, the group decided to tackle the do-not-track issue in two stages: first, develop a standard for the do-not-track signal itself; second, develop a standard for how advertisers and browsers should comply with do-not-track requests. The group's release of a proposed standard signals reflects near-completion of the first stage (the group is calling for any final comments on the technical standard by June 18), and transition to work on the second.

THE PROPOSED STANDARD

The group's proposed signal standard describes how users can communicate to ad servers that they do not want advertisers to be permitted to collect data across different websites, and how these advertisers can communicate their responses to such requests. Significantly, the standard does not apply to site operators collecting data on how consumers use their sites, nor does it mandate compliance with do-not-track requests. Indeed, it includes specific protocols for advertisers to respond to consumer requests by signaling that they will not honor these requests, or to qualify how they will honor the requests by providing a link to a description of how the advertiser will collect and use data. It would then be up to the browser companies and consumers to decide what actions to take based on the advertiser's responses.

Assuming the signal standard is adopted, the working group faces daunting problems in the second phase of trying to develop a common approach to do-not-track compliance. While there appears to be general agreement on allowing site operators to collect data for fraud prevention, billing and other operational purposes, for example, there remain open questions on whether they can collect data for cross-site analytics and ad targeting. One of the group's chairs, Justin Brookman, has explained that the group hopes to develop a set of standardized compliance policies that advertisers can adopt for their businesses, each with variations on policies for data collection and use. A standardized set of policies and variations is necessary, Brookman points out, to prevent users and browser developers from being overwhelmed with dozens or hundreds of different policies.

The working group hopes to develop its compliance framework by the end of 2014 and to have a final do-not-track standard by 2015.

COMPTROLLER OF THE CURRENCY STRESSES IMPORTANCE OF CYBERSECURITY

Speaking at an April 16, 2014, meeting of the CES Government, the group that oversees the Consumer Electronics Show, Comptroller of the Currency Thomas J. Curry, stressed the importance of cybersecurity to his agency and to financial service regulators.[22]

Curry indicated that he had worked with the other members of the Federal Financial Institutions Examination Council to set up a Cybersecurity and Critical Infrastructure Working Group. This group has already begun meeting with intelligence, law enforcement and homeland security officials to determine how to best implement President Obama's Executive Order on Cybersecurity, as well as recommendations of the Financial Stability Oversight Council. Curry noted that the impact of a cyberattack on a financial services system could be even more disruptive than a data breach at a retail store.

[22] Text of speech is available at http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-59.pdf.

Curry outlined some of the key threats to financial institutions face today:

- The hacker community includes not only individuals acting alone, but also countries that serve as criminal havens for hackers by "turning a blind eye" toward illicit activities, or even sponsor attacks.
- The financial services industry is particularly vulnerable because of the industry's reliance on interconnections between various parties and systems. All of these third-party relationships and connections provide potential access points to all of the connected networks and introduce new and different weaknesses into the system. Curry stressed the need for rigorous diligence and supervision of third-party vendors and partners, especially since hackers will exploit smaller players who may not have extensive cybersecurity defenses.[23]
- The nature of the Internet also means that a large part of the systems used by financial institutions is outside of their direct control.
- Third parties have access to large amounts of sensitive bank or customer data. Since this is an industry that is built on reputation, "a single data breach involving confidential customer information can be extremely costly."

Finally, Curry urged financial institutions to communicate with each other, as well as with relevant government agencies, to share information about cyberattacks and to establish best practices. Curry cited as an example of private-public cooperation the Financial Services Information Sharing and Analysis Center (an information-sharing nonprofit organization run by financial institutions, that includes the OCC and other public sector agencies as members) and the Financial Services Sector Coordinating Council (formed by the private sector after September 11, 2001, and which brings together private sector firms and trade associations across banking, financial markets and insurance).

---

[23] Curry referenced the OCC's October 2013 guidance on third-party risk that deals with the management of third party vendors. OCC, *Risk Management Guidance*, October 20, 2013, available at http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

SKADDEN CONTACTS

STUART D. LEVI
Partner / New York
212.735.2750
stuart.levi@skadden.com

ANASTASIA T. ROCKAS
Partner / New York
212.735.2987
anastasia.rockas@skadden.com

JAMES S. TALBOT
Counsel / New York
212.735.4133
james.talbot@skadden.com

GREGOIRE BERTROU
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@skadden.com

OLIVIER BOULON
Associate / Paris
33.1.55.27.11.32
olivier.boulon@skadden.com