Skadden

Privacy & Cybersecurity Update

House and Senate Vote to Disallow FCC Privacy Rule

As we reported in our February 2017 *Privacy & Cybersecurity Update*, the Federal Communications Commission's (FCC) privacy rule for internet service providers was likely to have been struck down, on partisan grounds, before it ever was implemented. This month, Congress voted to repeal the rule, as expected. While there are clear privacy implications, the result has less to do with partisan views on personal privacy and more to do with partisan views on the scope of authority of the FCC.

Background

In October 2016, the FCC announced new internet service provider (ISP) privacy rules that required ISPs to obtain explicit "opt-in" consent before collecting a wide range of what was deemed "sensitive information," inform consumers as to what data the ISP would collect and allow consumers to opt out of most ISP information collection. While "sensitive" data included categories that traditionally are considered sensitive, such as health and financial information and information concerning children, it also included a number of categories that are the lynchpin of targeted advertising and a key revenue source for ISPs, including web browsing and app usage history. On March 1, 2017, Acting Federal Trade Commission (FTC) Chairwoman Maureen K. Ohlhausen and FCC Chairman Ajit Pai stated their disagreement with "the FCC's unilateral decision in 2015 to strip the FTC of its authority over broadband providers' privacy and data security practices, removing an effective cop from the beat," and that privacy jurisdiction should be returned to the FTC. The FCC then announced it was staying implementation of the rules.

The Senate and the House, voting on partisan grounds, have now each approved a resolution under the Congressional Review Act to repeal the FCC's privacy rule. While many have painted the decision as a vote against personal privacy, the reality is that it was more a repudiation of the FCC's decision to bring ISPs under the FCC's purview during the Obama administration by reclassifying them as common carriers under the Communications Act.

Impact

The impact of the decision remains unclear since ISPs have, historically, not been limited in their data collection practices. Additionally, as many have pointed out, the FCC rules would not have regulated search engines or social network sites that liberally use personal data to target ads and generate revenue. Nonetheless, many counter that consumers can more easily opt out of using search engines and social networks with privacy policies they oppose than they can drop an ISP. In addition, it has been easier to opt out of data collection when using a social network compared to an ISP.

Privacy focus under the Trump administration now shifts to the FTC, where it remains to be seen whether the agency will remain an active enforcer of personal privacy.

Return to Table of Contents

New York State Reports Significant Increase in Data Breach Incidents

The New York state attorney general has released findings that the number of data breach reports in the state increased more than 60 percent from the previous year.

New York State Attorney General Eric T. Schneiderman released a report in early March 2017 detailing the number of data breach notices his office received in 2016. Approximately 1,300 reports were disclosed, which was a record high and a 60 percent increase over 2015. The New York Attorney General's Office has collected such data since 2005. According to the report, personal records — primarily social security numbers and financial account information — of 1.6 million New Yorkers were exposed, triple the number from 2015. Although, not surprisingly, hacking was suspected as the primary cause of these compromises and accounted for 40 percent of the reports, and "inadvertent disclosure" was a close second with 37 percent. This category includes employee negligence, inadvertent exposure of records, insider wrongdoing and the loss of a device or media. While hacking and inadvertent disclosure were almost equal in terms of the number of incidents, hacking represented the vast majority of individual records that were compromised (70 percent as compared to 19 percent for inadvertent disclosure), suggesting that most inadvertent disclosure incidents involve small data sets.

While the number of overall hacking incidents increased sharply, it was noteworthy that only two of the reported incidents constituted very large-scale compromises of records: the breaches of Newkirk Products, Inc. in October 2016 and an HSBC bank in 2016. Prior years had seen fewer overall incidents, but more large-scale attacks.

Practice Points

New York is one of a number of states that require disclosure of a data breach not only to individual residents, but also, without unreasonable delay, to a state agency; in this case the Office of the Attorney General. The report did not provide more guidance on what constituted "unreasonable delay" but noted that it had received notices ranging from a few days to a few months after an incident, and that the timing for notices seemed to be increasing. While the New York attorney general's report did not critique any notice as unreasonably delayed, companies should be mindful that New York is focused on the timeliness in which the state is receiving notices, and could, in the future, find a company has waited too long.

Although not stated explicitly, the report also puts all companies doing business in New York on further notice regarding the prevalence of external attacks and the need to implement industry-standard cybersecurity measures and have a cybersecurity response plan in place. The report also highlights the prevalence of negligence in losing records, an area that companies have far more power to control.

Return to Table of Contents

Annual FISMA Report Shows Major Information Security Incidents

The Office of Management and Budget (OMB) released its annual report detailing how federal agencies are progressing toward cybersecurity performance goal and where they need improvement.

The annual report by the OMB pursuant to the Federal Information Security Modernization Act of 2014 (FISMA) details federal agencies' progress toward cybersecurity performance goals. The report also includes assessments by independent inspectors general regarding areas in need of improvement. This year's report, for the 2016 fiscal year, discusses information security incidents suffered by the federal government, progress in cyberattack prevention efforts and the implementation of cybersecurity programs designed to protect federal systems.

Section II.C of the FISMA report for fiscal year 2016 discusses major information security incidents endured by federal agencies. There were 30,899 incidents reported during this time period, with 16 of those incidents qualifying for the designation of "major incident." These major incidents result in mandatory reporting requirements to Congress.

The OMB defined what constitutes a major incident in its "Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements," but the agency changed the definition in new guidance, titled "OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements." The new definition states that a "major incident" is any incident that is likely to result in demonstrable harm to the national security interests, foreign relations and/or economy of the United States, or to the public confidence, civil liberties and/or public health and safety of the American people. The OMB indicates that agencies should consult other related government publications to help determine the severity of an incident.

Analogously, the new guidance stated that a breach involving personally identifiable information (PII) is a major incident if such PII — if exfiltrated, modified, deleted or otherwise compromised — is likely to result in demonstrable harm to the national security interests, foreign relations and/or economy of the United States, or to the public confidence, civil liberties or public health and safety of the American people. A major incident related to PII is also triggered if there is modification of, unauthorized deletion of, unauthorized exfiltration of or unauthorized access to 100,000 or more individuals' PII.

Return to Table of Contents

Trump Administration Cybersecurity Developments

The Trump administration took several cybersecurity steps in March, including appointing a "cyber czar" to oversee the administration's cybersecurity efforts and addressing cyberattack protection in its proposed budget.

In March 2017, the Trump administration selected Rob Joyce of the National Security Agency (NSA) as its new "cyber czar." In this role, Joyce will be responsible for the administration's cybersecurity efforts, as part of the National Security Council. Joyce previously led the NSA's Information Assurance Directorate, which was responsible, in part, for securing federal national security systems against cyberattacks.

President Donald Trump's views on cybersecurity also were reflected in his proposed budget for the 2018 fiscal year. However, as with many areas of the proposed budget, how one interprets these views depends on which numbers are being examined. For example, President Trump proposed to allocate $1.5 billion for the Department of Homeland Security (DHS) to protect federal networks and critical infrastructure from cyberattacks. This allocation exceeds the $900 million that the Obama administration had proposed for a similar DHS program, but pales in comparison to the $19 billion proposed by the Obama administration that was spread across various government cybersecurity initiatives. The Trump administration did not provide further guidance on how it expected the $1.5 billion to be allocated.

President Trump's proposed budget also highlights the goal of increased sharing of cybersecurity incident information with other federal agencies and the private sector, something the Obama administration had similarly stressed the importance of to enhance the nation's cybersecurity.

Return to Table of Contents

FTC Issues Guidance to Companies Facing Phishing Scams

The FTC distributed advice outlining how companies should respond to phishing scams, which have increased in practice significantly over the past year.

On March 6, 2017, the Federal Trade Commission issued advice for businesses attacked through phishing scams, a type of cyberattack that uses company names to deceive consumers into disclosing personal information or money.[1] According to the Anti-Phishing Working Group, a public-private international partnership that advises on cyberattacks, there were more than 1 million phishing attacks in 2016, a 65 percent increase over 2015. This data is based on phishing attacks reported to the group by its member companies, global research partners, the group's website and email submissions.[2]

The FTC emphasized that consumers tricked by phishing scams may lose trust in the targeted company, harming both the company's reputation and financial prosperity. Thus, the FTC suggests that the first step for a company affected by a phishing scam is to notify consumers through social media, email or written communication about the attack. Companies should advise consumers to

[1] For the FTC guidelines, including a video, see here.

[2] For more information on phishing trends in 2016, see here.

disregard suspicious emails or texts alleging to be the company and should explain that a legitimate company would not typically solicit personal information via text or email.

Companies should report the scam to the FBI's Internet Crime Complaint Center and file a complaint with the FTC. Businesses also should consider urging consumers to forward any phishing emails to the Anti-Phishing Working Group.

An affected company can protect consumers by directing them to the FTC's identify theft site at IdentityTheft.gov, where consumers can report identity theft they may have incurred from disclosing personal information.

Whether or not a company is a victim of a phishing scam, the FTC encourages all businesses to treat the threat of a phishing scam as a reminder to update security practices. One way to do so is through the FTC's extensive online resources, including its data security portal, which provides guidance to avoid and address data breaches.

Return to Table of Contents

Federal District Court Denies Employer's Motion to Compel Discovery of GPS Data

A federal district court in Indiana ruled against a company that was seeking to obtain GPS data from employees' cell phones. The case had put into question whether employees' personal device data was open to examination even during nonwork hours.

In *Crabtree v. Angie's List Inc.*, a federal district court in Indiana denied an employer's motion to compel discovery of its former employees' cell phone GPS data. Angie's List, Inc. sought the GPS data to defend against allegations that it did not pay employees for all hours worked. The employees were senior sales representatives who spent a significant amount of their workday on the phone and often used their personal devices for work purposes.

In its motion to compel discovery, the employer argued that access to the employees' cell phone GPS and location data would help it construct a detailed timeline of when the employees were working. The employer stated such data was necessary because the company tracked hours based on whether or not the employees were logged in to their computers, however, the employees could remain logged in, but be inactive for several hours. Using the GPS data, the employer explained, would identify whether the employee had left the office or was otherwise not working during that time.

Emphasizing the employees' privacy interests, the court distinguished the case at issue from a similar case where a plaintiff was permitted to obtain GPS data from trucks used in the defendant's business to test the accuracy of the data previously provided by the defendant. Here, the court reasoned, providing GPS data covering 24 hours per day would result in tracking the employees' movements well outside of the workday. Further, the GPS data would not accurately portray whether the employees were working at any given time because employees were often expected to work remotely. Stating the employer had "not demonstrated that the GPS and location data from the employees' cell phones would be more probative" than the data already in its possession, the court held that the examination of the GPS data on the employees' personal cell phones was "not proportional to the needs of the case."

Return to Table of Contents

Personal Device Communications Regarding Public Matters May Constitute Public Records in California

In *City of San Jose v. Superior Court*,[3] the California Supreme Court unanimously held that communications of a public officer or employee made via a personal account or device that concern the "conduct of public business" may be construed as public records subject to disclosure in response to a California Public Records Act (CPRA) request. Such devices and accounts include, but are not limited to, personal cell phones, computers and email accounts.

Basic Facts and Issue

In 2009, Ted Smith requested the disclosure of public records from the city of San Jose concerning certain redevelopment efforts in downtown San Jose. The city released communications made using city telephone and email accounts, but did not disclose communications made using the individuals' personal accounts. Smith sued for declaratory relief, arguing that the CPRA's definition of "public records" more broadly encompassed all communications of official public business, regardless of how such records are created, communicated or stored. The city contested this theory, contending that messages communicated through personal accounts are not public records "because they are not within the public entity's custody or control." The trial court initially granted summary judgment for Smith, but an appeals court issued a writ

[3] 389 P.3d 848 (2017),

of mandate, conversely holding that communications from private devices were exempt from CPRA disclosure. The Supreme Court was subsequently left to determine the narrow issue of whether "writings concerning the conduct of public business" are beyond the CPRA's reach merely because they were sent or received using a nongovernmental account or device.

Discussion

In carefully weighing the salient policy interests of the CPRA, the court ultimately concluded that writings cannot escape the scope of the CPRA's disclosure obligations simply by being created, stored or transmitted via a nongovernmental account or device. The court concluded that "an employees' communications about official agency business may be subject to CPRA regardless of the type of account used in their preparation or transmission," so long as the communications relate in some substantive way to the public's business.

In so concluding, the court began its analysis by examining the statutory predicates that constitute a public record under the disclosure obligations of the CPRA; namely, whether it is (1) a writing, (2) with content relating to the conduct of the public's business, which is (3) prepared by, or (4) owned, used or retained by any state or local agency.

With respect to the first element, the court confirmed the well-established conclusion that emails, text messages and other forms of digital communications across various electronic platforms constitute "writings" under the CPRA. The court, however, noted that the immediate and fleeting nature of electronic communications has blurred the lines between official work-related communications and those that are purely private communications produced by an officer or employee. To address this issue, the court employed the second element as a framework to distinguish between work-related and purely private communications. The court clarified that to qualify as a public record under the CPRA, "a writing must relate in some substantive way to the conduct of the public's business." Though this standard is broad, the court noted that "it is not so elastic as to include every piece of information the public may find interesting. Communications that are primarily no more than incidental mentions of agency business, generally will not constitute public records."

The city's primary statutorily-based contentions to the extension of the CPRA to communications on private devices and accounts stem from the third and fourth elements of a public record, which require that the writing be "prepared, owned, used or retained by any state or local agency. The city essentially argued that the definition of local agency does not specifically include individual government officials or staff members, and thus their communications in their individual and personal capacity do not constitute public records subject to the CPRA. The court rejected the city's argument, noting that the city incorrectly focuses on the "owned, used, or retained by" aspect of the public records definition and ignores the "prepared by" aspect. The court further stated that "a writing is commonly understood to have been prepared by the person who wrote it. If an agency employee prepares a writing that substantively relates to the conduct of public business, that writing would appear to satisfy the [CPRA]'s definition of a public record."

In addition, the city also argued that because public records include only materials in an agency's possession or are directly accessible to the agency, communications on personal devices and accounts are thus beyond an agency's reach and fall outside the CPRA. The court also rejected this argument, observing that records related to public business are subject to disclosure if they are in an agency's actual or constructive possession, and that constructive possession of records is established when the agency has the right to control the records through another person, namely the employee or official. The court concluded that the city had constructive possession through the "preparation" of the communications through its officials and employees. In rejecting the city's arguments, the court refused to adopt a categorical exclusion of documents from the CPRA's definition of public records simply because they exist on personal accounts or devices. Consequently, so long as the communications are (1) "prepared" by employees and officials of a public entity and (2) relate in some substantive way to the conduct of the public's business, such communications likely will be subject to the disclosure obligations under the CPRA.

Public Policy and Privacy Considerations

This case clearly implicates the privacy rights of public employees and officials. To address such concerns, the court noted that individual privacy concerns "can and should be addressed on a case-by-case basis." As a final matter, the court provided non-binding guidance regarding how public entities can strike the balance between privacy and disclosure in responding to CPRA requests. A public agency's "first step should be to communicate the request to the employees in questions. The agency may then reasonably rely on these employees to search their own personal files, accounts and devices for responsive materials." The court further suggests that public agencies may adopt policies that will reduce the likelihood of public records

being held in employees' private accounts, such as "requiring employees to use or copy their government accounts for all communications touching on public business."

Ultimately, the court emphasized that it "does not hold that any particular search method is required or necessarily adequate." From this decision, however, one thing is clear: the use of private devices or accounts for the conduct of public business now carries an increased burden with respect to proper disclosure of public agency information. As the lines between private and public communications are blurred by virtue of digital and electronic communication, public agencies ought to re-evaluate their policies regarding the use of private devices or accounts for the conduct of public business.

Return to Table of Contents

EU Court Draws Limits on the 'Right to be Forgotten'

The European Court of Justice (ECJ) recently drew new limits on the "right to be forgotten," ruling that an Italian citizen is not owed damages from an Italian business group that accurately linked him to a bankrupt company in a public database.

Background

In May 2014, in *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, the ECJ issued a landmark decision holding that search engine operators could be compelled to take down search results containing personal data of a data subject if the data subject asked them to do so.[4] This so-called "right to be forgotten" will become a formal part of European data privacy law when the General Data Protection Regulation (GDPR) goes into effect in May 2018.

That ruling was challenged in *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*.[5] Manni, the sole director of a building company that had been awarded a contract for the construction of a tourist complex, brought an action against the Lecce Chamber of Commerce claiming that his properties were not selling because it was apparent from the register maintained by the Chamber of Commerce that he had been the sole director and liquidator of another company that had been declared insolvent. The insolvent company had since been struck from the register. Manni alleged that personal data concerning him had been processed by a company that specialized in risk assessment and the collection and processing of market information, and that notwithstanding a request to remove the data from the register, the Chamber of Commerce had not done so. Manni thus sought an order requiring the Chamber of Commerce to erase, anonymize or block the data linking him to the liquidated company, as well as seeking compensation for reputational damages suffered as a result of the connection.

The lower court upheld Manni's claim, ordering the Chamber of Commerce to anonymize the data linking Manni to the liquidated company and to pay compensation for the damage suffered by him. The court held that "it is not permissible for entries in the register which link the name of an individual to a critical phase in the life of the company (such as its liquidation) to be permanent, unless there is a specific general interest in their retention and disclosure." The court also noted that after an appropriate period from the conclusion of liquidation and after the company has been removed from the register, assuming there is no statute declaring otherwise, the name of the person who was the sole director of that company is not necessary or useful. The Chamber of Commerce then appealed that judgment.

The ECJ Ruling

The ECJ considered the effects of Council Directive 68/151 of March 9, 1968, which protects information of organizations from third parties, and the European Data Directive 95/46/EC on the case at hand. The court noted that under these directives, EU member states must allow individuals to request the authority responsible for maintaining the register to limit access to their personal data after a certain period of time has elapsed from the dissolution of the applicable company.

Specifically, under Article 2(1)(j) of the Data Directive, the appointment of liquidators, particulars concerning them and, in principle, their respective powers, also must be disclosed. Pursuant to Article 3 of Directive 68/151, those particulars must be transcribed by each member state either in a central register, commercial register or companies register, with a copy of the register obtainable by application. The court further explained that the purpose of that Article is to enable interested third parties to inform themselves of relevant matters, without such a third party having to establish a right of interest in the relevant

[4] See our May 2014 *Privacy & Cybersecurity Update* for our previous coverage of this case here.

[5] *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Manni*, Judgment of the Court (Second Chamber), Case C-398/15 (March 9, 2017). The full opinion can be found online here.

information. In that regard, the court decided that it may be, "in principle[,] necessary for the personal data of natural persons … to remain on the register and/or accessible to any third party upon request also after the activity has ceased and the company concerned has been dissolved."

The court concluded that, as EU law currently stands, it is for each member state to determine whether individuals may apply to the authority responsible for keeping the register for a limitation on access to their personal data by third parties who can demonstrate a specific interest in consulting that data. Such a decision should be made on a case-by-case assessment, if it is exceptionally justified, on "compelling legitimate grounds relating to their particular situation," and "on the expiry of a sufficiently long period after the dissolution of the company concerned."

In Manni's case, the court noted that his inability to sell tourist units because potential buyers have access to the database linking him to a failed company does not warrant his right to be forgotten, as potential buyers have a legitimate interest in his past business dealings. This ruling is binding on the Italian Appeals Court, which must now decide the case accordingly.

Return to Table of Contents

European Parliament Civil Liberties Committee Critiques Privacy Shield

A European Parliament committee monitoring civil liberties passed a non binding resolution declaring the EU-U.S. Privacy Shield inadequate, highlighting concerns relating to U.S.-based mass surveillance and protections for EU citizens.

Since the EU-U.S. Privacy Shield went into effect in July 2016, the agreement has come under scrutiny and a fair amount of criticism, particularly from EU-based privacy advocates. The agreement provides a privacy self-certification framework that enables companies to transfer personal data from the European Union and the three European Economic Area member states (Norway, Liechtenstein and Iceland) to the United States. It replaced the Safe Harbor, which was struck down by the European Court of Justice in October 2015. Over 1,800 companies have self-certified and rely on the agreement for EU-U.S. transborder data flow.

Now, the agreement has faced its latest and perhaps most significant challenge. European Parliament's Civil Liberties, Justice, and Home Affairs Committee (LIBE Committee) has passed a resolution declaring the Privacy Shield inadequate. The LIBE Committee has pressed for a complete review of the agreement by the European Commission, which already was scheduled to take place this summer as part of the first annual review.

The LIBE Committee highlighted a number of concerns, including the fact that the U.S. engages in mass surveillance for national security purposes. While the Privacy Shield includes a number of protections for EU citizens against such surveillance, it apparently was not enough to persuade the LIBE Committee. The committee felt that the "ombudsperson" who is designated to address complaints about U.S. surveillance practices lacks the independence to make neutral decisions.

The resolution passed by the LIBE Committee does not have binding effect, and it must still be voted on by the full European Parliament. However, the resolution signals that the Privacy Shield may come under harsh criticism during the annual review, and the EU may demand certain additional concessions from the U.S. for the agreement to continue.

Return to Table of Contents

Contacts in the Cybersecurity and Privacy Group

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

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

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

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

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

Jen Spaziano
Partner / Washington D.C.
202.371.7872
jen.spaziano@skadden.com

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

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

William Ridgway
Counsel / Chicago
312.407.0449
william.ridgway@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

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000