Skadden

Privacy & Cybersecurity Update

New York and Massachusetts Officials Ask Congress Not to Override State Data Security and Breach Notification Laws

Representatives of the attorneys general of New York and Massachusetts are asking Congress to allow states to continue to develop their own data security and breach notification laws, which may mean that companies will continue to face a range of different data requirements across the states.

On October 25, 2017, officials from the New York and Massachusetts attorneys general offices asked members of the House of Representatives considering omnibus federal data security and breach notification laws not to prevent states from enacting their own laws on the subject. Urging the federal government to set a "floor and not a ceiling," they argued that state lawmakers should be allowed to impose their own data security and breach notice requirements in addition to any that might be imposed at the federal level. Such an approach, however, would of course vitiate any benefits from an omnibus federal data protection law and leave companies with the same burden they currently have of tracking and complying with different state laws across the country.

Calls for Federal Regulation and Federal Moderation

Ever since states began passing their own data security and breach notification laws, U.S. companies have expressed their frustration with having to track and comply with a multitude of different requirements from state to state. Industry groups repeatedly have implored Congress to enact an omnibus federal law to alleviate this burden. In recent years, a number of data security and breach notification bills have been introduced on Capitol Hill, but few have gained any real traction. Recent high publicity and massive data breaches have increased pressure to enact such a law.

With this background — and with some momentum building behind an effort to pass federal legislation — representatives from the New York and Massachusetts attorneys general offices testified in a committee hearing that, while federal law would be welcome, there is concern about pre-emption of state laws. "I would submit that any

law that is proposed that is weaker than the law we currently have today is worse than doing nothing," noted Sara Cable, an assistant attorney general from Massachusetts.

Key Takeaway: Potential for Continued Disharmony

If Congress adopts the approach urged by the attorneys general representatives, companies likely will continue to face a myriad of different — sometimes inconsistent — requirements across states. Companies that use personal information in their businesses should watch closely how this congressional debate evolves.

Return to Table of Contents

NAIC Adopts Insurance Data Security Model Law

On October 24, 2017, the National Association of Insurance Commissioners (NAIC) adopted the Insurance Data Security Model Law, which establishes minimum data security standards and obligations applicable to a broad range of insurance industry players, including insurers, brokers and producers. If widely adopted by state legislatures, the Model Law will promote the establishment of uniform nationwide standards for data security and breach notification in the insurance industry.

On October 24, 2017, following a lengthy comment period, input from various interested constituents and six iterations of the Model Law, the NAIC adopted the Insurance Data Security Model Law during a joint meeting of its executive committee, which had initially introduced the Model Law, and Plenary.[1] The law is now available for consideration and adoption by states. The Model Law, which is based on New York's cybersecurity regulations that went into effect in March,[2] establishes "standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees." Licensees are defined to include insurers, agents, brokers and other persons and entities required to be licensed under state law. If widely adopted, the Model Law will help promote uniformity of data security and breach notification standards applicable to the insurance industry.

Model Law Requirements

The Model Law protects against cybersecurity events that adversely affect policyholders as well as insurers. In order to do so, all licensees are required to perform comprehensive risk assessments to identify "reasonably foreseeable threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information" and assess those threats based on their likelihood, potential damage and the adequacy of any safeguards in place.

Based on their risk assessment, licensees are required by the Model Law to (1) develop, implement and maintain comprehensive written information security programs commensurate with the licensee's size and complexity, the nature and scope of its activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by or in the possession, custody or control of the licensee; (2) include cybersecurity risks in its enterprise risk management process; (3) stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information; and (4) provide its personnel with cybersecurity awareness training that accounts for risks identified in the licensee's risk assessment. Licensees must certify compliance with the Model Law's data security requirements on an annual basis.

In recognition of the increasing use of cloud-based services to store data, the Model Law also mandates that licensees exercise diligence in selecting third-party service providers. Additionally, it mandates that licensees require their third-party service providers to implement appropriate security measures to protect all information systems and nonpublic information accessible to, or held by, the service provider.

If a licensee learns that a cybersecurity event has or may have occurred, the Model Law requires that the licensee promptly conduct an investigation to assess the nature and scope of the event. Further, the licensee must notify the insurance commissioner of the state in which the licensee is domiciled within 72 hours of learning of the event and provide details (to the extent available), including the date of the event; how the information was exposed, lost, stolen or the like; how the event was discovered; the period during which the licensee's system was compromised; and efforts made to remediate the situation. The licensee also must notify the insurance commissioners of other impacted states if the licensee reasonably believes that the breach impacted 250 or more consumers residing in the state. In addition, the Model Law requires licensees to comply with any applicable state data breach notification law.

[1] The Model Law is available here.

[2] See our December 2016 *Privacy & Cybersecurity Update* for a discussion of these regulations.

The Model Law grants the insurance commissioner certain enforcement powers, including the power to investigate the affairs of any licensee to determine whether it has engaged in any conduct in violation of the Model Law and to "take action that is necessary or appropriate" to enforce the Model Law when the insurance commissioner has reason to believe that a licensee has been, or is engaged in, conduct in the state that violates the Model Law. The Model Law is intended to supersede state and federal laws of general applicability addressing data security and data breach notifications.

Key Takeaway: Future Impact

While it remains to be seen whether and to what extent state legislatures will adopt the Model Law, the establishment of uniform minimum data security measures and mandatory protocols for responding to a data breach may help offer some level of certainty and predictability in the aftermath of a data breach. This, in turn, may lead to increased consumer confidence and demand for insurance products. Widespread adoption of the Model Law also would promote uniformity across jurisdictions with respect to cybersecurity and data breach notification requirements applicable to insurers, which may help ease the burden on an already highly regulated industry.

Return to Table of Contents

European Commission Upholds EU-US Privacy Shield

Following an annual review of the EU-U.S. Privacy Shield arrangement, EU officials have determined that the Privacy Shield continues to ensure adequate protection for transatlantic data protection.

On October 18, 2017, the European Commission (commission or EU commission) announced its conclusion that that EU-U.S. Privacy Shield arrangement does provide a valid mechanism for enabling organizations to transfer personal information from the EU to the United States.[3] As a variety of organizations had expressed concern that the commission would invalidate, seek to amend or simply sharply criticize the Privacy Shield regime, the commission's conclusion should provide some stability to an uncertain privacy environment.

Background on the Current Privacy Framework

In 2016, the United States and the European Commission adopted the EU-U.S. Privacy Shield, a self-certification framework designed to enable companies to transfer personal data from the EU and the three European Economic Area member states — Norway, Liechtenstein and Iceland — to the U.S. Under the EU Data Protection Directive, personal data about EU citizens can only be transferred to countries with "adequate" data protection laws in place. Notably, only a few countries satisfy this standard, and the U.S. is not one of them. However, under the Privacy Shield Framework, companies that self-certify their adherence to seven broad data privacy principles may transfer personal data outside of the EU to the U.S.

The Privacy Shield replaced the previous framework between the EU and U.S. known as the Safe Harbor Privacy Principles, which the Court of Justice of the European Union invalidated in October 2015 in the *Schrems v. Data Protection Commissioner* case. In the *Schrems* decision, the court found that the Safe Harbor failed to adequately protect the privacy of EU citizens, mainly due to the U.S. government's ability to access personal data for national security purposes. The Privacy Shield aimed to remedy the inadequacies of the Safe Harbor, however, after the Privacy Shield's adoption, many privacy advocates criticized the replacement framework for failing to address the government's surveillance concerns raised in *Schrems*.[4]

The recent review of the Privacy Shield followed on the heels of a resolution adopted by the European Parliament on April 6, 2017, which formally raised concerns about the Privacy Shield and called for a closer review of the adequacy of the protections it affords EU citizens. As a general theme, the resolution expressed, among other issues, a deep concern that bulk surveillance by the U.S. government is not prohibited outright under the current framework.

The commission reached its conclusion after conducting the first annual official review of the EU-U.S. Privacy Shield on September 18 and 19, 2017, in Washington, D.C. The Privacy Shield agreement requires such a review each year, so organizations that seek to export data from the EU to the U.S. should be mindful of these reviews and any proposed revisions to the arrangement that may result.

[3] For the full report issued by the European Commission, see here.

[4] For more information regarding criticism of the Privacy Shield, see our April 2017 *Privacy and Cybersecurity Update*.

Privacy Shield Review: Key Findings and Recommendations

Despite the concerns raised by the European Parliament, the commission found that "the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organizations in the United States." In support of its conclusion, the commission made the following key findings:

- **Increased Governmental Oversight:** The commission found that the current Privacy Shield framework addresses several concerning elements raised in the *Schrems* case, particularly, that the Privacy Shield "provides for more regular and rigorous monitoring by the Department of Commerce."
- **Availability of Redress Mechanisms:** In response to an additional concern from the *Schrems* case, the commission found that the Privacy Shield "significantly strengthens the possibilities for EU individuals to obtain redress," and pointed to the American Arbitration Association's Privacy Shield Arbitration Panel and the ombudsperson mechanism.[5]
- **Limiting Access by Government Agencies:** The commission further found that safeguards have been implemented to limit access to personal data by national security agencies and specifically have called attention to the Presidential Policy Directive 28, which applies to the personal data of individuals regardless of nationality.
- **Satisfactory Certification Process:** With buy-in from 2,400 companies, the commission found that the certification process has been "handled in an overall satisfactory manner."
- **Increased Cooperation:** Finally, the commission pointed to the increased "cooperation [between U.S. and] European data protection authorities," citing as examples the Staff Working Document on the Privacy Shield Annual Review and the formation of an informal panel of data protection authorities (DPAs).

In addition to its key findings, the commission also used its first annual review to outline several recommendations for how the Privacy Shield could be improved. Generally, the commission recommended that U.S. authorities give "more timely and comprehensive information about developments relevant to the Privacy Shield, or anything that might jeopardize the protections it provides," as well as bolster awareness of how EU citizens can exercise their rights under the Privacy Shield. In addition, the commission made the following specific recommendations:

- **Preventing False Privacy Shield Claims:** The commission has recommended that the U.S. Department of Commerce (DoC) take the following actions: (1) prohibit companies awaiting designation under the Privacy Shield from publicly referring to their certification until it has been finalized by the DoC and included on the Privacy Shield list; and (2) regularly and proactively "conduct [Internet] searches for false claims," which undermine the credibility of the system as a whole.
- **Researching Automated Decision-Making:** The commission has recommended further research on the use of personal data for automated decision-making, a concern that was raised under the April 2017 resolution.
- **Preserving Protections Under PPD-28:** In response to Section 702 of the U.S. Foreign Intelligence Surveillance Act's pending expiration in December 2017, the commission has recommended preserving the protections of PPD-28 in future reforms.
- **Filling Posts in Executive Branch:** Several concerns in the April 2017 resolution stemmed from the substantial number of unfilled roles in President Trump's executive branch tasked with enforcing the Privacy Shield. With this in mind, the commission has called for the "swift appointment" of a permanent Privacy Shield Ombudsperson and any missing members of the Privacy and Civil Liberties Oversight Board.
- **Increasing Cooperation:** The commission also has recommended an increase in cooperation between the DoC and European DPAs in an effort to develop "convergence in the interpretation" of the Privacy Shield, which will provide stakeholders and companies with "greater legal certainty."

Application to GDPR Unclear

The commission conducted its review of the Privacy Shield based on the current EU privacy law, Data Protection Directive 95/46/EC. Despite encouragement from members of the European Parliament, the commission did not evaluate the adequacy of the Privacy Shield under the EU's new General Data Protection Regulation (GDPR), which replaces the current law and will go into effect in May 2018. It is possible, therefore, that the commission will at a later date determine that the Privacy Shield provides inadequate protection under the more stringent GDPR.

Key Takeaways

While concerns that the Privacy Shield might be invalidated have subsided for the time being, the recommendations issued by the European Commission identify significant areas for improvement that, if left unaddressed, may revive anxieties surrounding the framework's future. Moreover, the commission has not expressed a view of the Privacy Shield's adequacy under the

[5] Concerns over the adequacy of the redress mechanism form part of the basis for a pending challenge to the EU's "standard contractual clauses" for transferring data, which has been submitted to the Court of Justice of the European Union for review. A further discussion of this case is included in this edition of the *Privacy and Cybersecurity Update*.

GDPR. As a result, while it appears the Privacy Shield is a reliable basis for transferring personal data from the EU to the U.S. for the time being, it is possible that will change in the future.

Return to Table of Contents

EU Advisory Body Issues Draft Guidance on GDPR

The European Union's Article 29 Data Protection Working Party has issued its guidance for interpreting the EU's GDPR requirements for data breach notification requirements and for data profiling (including automated decision-making).

On October 17, 2017, the Article 29 Data Protection Working Party (WP29) released two proposed guidelines relating to obligations under the EU GDPR. The first guideline relates to data breach notifications required under the GDPR, and the second relates to profiling and automated decision-making. Both of these guidelines are open to public comment until November 28, 2017.

Role of WP29

WP29 is an EU advisory body made up of representatives from the data protection authorities of EU members. It is charged with providing expert guidance on data protection issues and promoting uniform application of data protection laws across the EU. Though not technically binding on EU member states' individual data protection commissioners,[6] WP29's guidance carries a good deal of weight when the individual commissioners evaluate data privacy issues.

Draft Breach Notification Guidelines

The GDPR imposes strict obligations on data controllers and processors to ensure the security of personal data, including a mechanism for data breach notifications that requires notification to the competent supervisory authority and, in some cases, the individuals affected by the breach. This month, WP29 released its proposed guidelines to provide more detailed explanations about the data breach notification mechanism and to clarify certain key concepts.[7]

Notification Requirements Generally

Under the GDPR, in the event of a personal data breach, data controllers are required to (1) notify the competent supervisory authority within 72 hours of becoming aware of such breach unless "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons," and (2) if there is a "high risk to the rights and freedoms of natural persons," notify the individuals whose data is subject to the breach without undue delay. Data controllers who fail to comply with these GDPR requirements could be subject to sanctions or an administrative fine of up to €10 million or 2 percent of the data controller's worldwide annual turnover.

WP29 recommends that the controllers look to the following criteria when assessing risk following a data breach:

- type of breach;
- nature, sensitivity and volume of personal data;
- ease of identification of individuals;
- severity of consequences for individuals;
- special characteristics of individuals (*e.g.*, children);
- number of affected individuals; and
- special characteristics of the data controller.

Notification to Supervising Authority

WP29's guidance clarifies that, for purposes of notifying the supervising authority, a controller becomes "aware" of a data breach when it has a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised." Conducting an initial investigation of the incident (which "should begin as soon as possible") does not mean a controller is aware of a breach. Data processors also should notify data controllers of breaches "without undue delay," which should be "immediate" to help data controllers adhere to the timeframe requirements.

When a data breach affects individuals in more than one EU member state and notification is required, the controller must notify the lead supervisory authority. If a data controller fails to identify the lead supervisory authority, it should at least notify the local authority where the breach occurred. WP29 recommends that controllers indicate whether individuals in other member states are likely to be affected.

[6] See the WP29 opinions and recommendations here.

[7] Available here.

Information in Notification to Supervising Authority

Under the GDPR, the notification to the supervisory authority should describe:

- the nature of the breach (including the categories and approximate number of data subjects and personal data records concerned);
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach; and
- the measures the controller has taken or proposes to take to address the breach (including measures to mitigate its possible adverse effects).

WP29's guidance states that "if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (*e.g.*, identity theft, fraud, financial loss, threat to professional secrecy)," controllers should note these categories. It is acceptable to notify the supervising authority in phases, as more information becomes available, and the guidance notes that "there is no penalty for reporting an incident that ultimately transpires not to be a breach."

The controller also should maintain documentation to enable the supervisory authority to verify compliance with the above, including documenting any such personal data breaches, noting the facts relating thereto, its effects and the remedial action taken. WP29's guidance suggests data controllers include in such documentation the "effects and consequences of the breach, along with the remedial action taken by the controller," and an explanation of data controllers' reasoning for their decisions in response to the breach, including justifications for not notifying the supervisory authority.

Notification to Data Subjects

Communication to data subjects of breaches should be clear and transparent and, for example, should not be sent as an attachment to a newsletter or other standard message. WP29's guidance provides the following examples of transparent communication methods: SMS, direct message and prominent website banners. The guidance also emphasized that the best method to choose will "maximize the changes of properly communicating information to all affected individuals," which may mean employing several methods of communication.

The notification to individuals whose personal data are subject to the breach is not required where:

- the controller has implemented appropriate technical and organizational protection measures (*e.g.*, encryption), which were applied to the personal data affected by the breach;
- the controller has taken subsequent corrective measures to ensure that the risk to such data subjects is no longer likely to materialize; and
- doing so would involve disproportionate effort (in which case, the controller can inform such data subjects with a public communication).

WP29's guidance also notes that controllers should be aware of breach notification requirements in other legislation that may be applicable to them, *e.g.*, the eIDAS Regulation; the NIS Directive; the Citizens' Rights Directive; the Breach Notification Regulation; and professional, medical or legal notification duties.

Guidelines on Profiling Under the GDPR

WP29 has adopted new draft guidelines covering profiling and automated decision-making under the GDPR to provide safeguards against the risk that a potentially damaging decision is made without human intervention.[8]

The GDPR identifies profiling as automated processing of data to analyze or make predictions about individuals' personal preferences, behaviors and attitudes, such that any simple assessment or classification of individuals based on characteristics could be considered profiling under the GDPR, even without predictive purpose.[9] The GDPR identifies three ways of using profiling: (1) general profiling; (2) decision-making-based profiling; and (3) solely automated decision-making.

Prohibition on Automated Decision-Making

Fully automated individual decision-making, which WP29 defines as "the ability to make decisions by technological means without human involvement," is generally prohibited under Article 22 of the GDPR, however the article also provides exceptions to this prohibition. Article 22 also includes a requirement that there be measures in place to safeguard the data subject's rights, freedoms and legitimate interests.

[8] Available here.

[9] In particular, the GDPR focuses on profiling used to analyze or predict a subject's performance at work, economic situation, health, personal preferences, reliability, behavior, location or movements. An overview of decision-making rights can be found here.

According to WP29's draft guidelines, the prohibition on fully automated decision-making only applies when the decision based on such technology "has a legal effect on or similarly significantly affects someone." WP29 provides the following examples of "legal effects":

- impingements on the freedom to associate with others;
- impingements on the freedom to vote in an election or take legal action; or
- an effect on legal contractual status or rights.

With regard to "similarly significant" effects, the guidance clarifies that these effects do not necessarily need to be legal, and that the threshold is whether or not the decision may have "the potential to significantly influence the circumstances, behavior or choices of the individuals concerned." As examples of decisions with these similarly significant effects, WP29 cites:

- automatic refusal of an online credit application; and
- e-recruiting practices without any human intervention.

Exceptions to the Prohibition

Article 22(2) of the GDPR sets forth the following three exceptions to the prohibition on fully automated decision-making:

- the processing is necessary for the performance of or entering into a contract;
- the processing is authorized by EU or member state law to which the controller is subject and that also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; and
- the processing is based on the data subject's explicit consent.

According to WP29, whether or not the processing should be considered "necessary" should be interpreted narrowly. The guidance states that the consent exception is limited and makes clear that the exception for entering into a contract is not satisfied by including profiling in the small print of an otherwise unrelated contract.

Data subjects of automated decision-making have the right to be informed of the controller's obligations, and as a result controllers using automated decision-making must tell the subject they are engaging in such activity, provide meaningful information about the logic involved, and explain the significance and envisaged consequences of the processing. WP29 suggests controllers provide this information regardless of whether the processing falls within the definition of automated decision-processing.

To satisfy obligations under the GDPR to protect the rights, freedoms and legitimate interests of data subjects, and to include suitable protections for data subjects, WP29's guidance suggests that minimum safeguards should include an explanation to the data subject of the decision reached, a way for the data subject to obtain human intervention and to express his or her point of view. The GDPR requires controllers to have the following safeguards in place:

- ensure processing is fair and transparent by providing meaningful information about the logic involved, the significance and the foreseeable consequences;
- use appropriate mathematical or statistical procedures;
- implement appropriate technical and organizational measures to minimize and correct inaccuracies; and
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Although the GDPR does not apply a blanket prohibition on using profiling and automated decision-making in relation to children, WP29 suggests that controllers "refrain, in general, from profiling [children] for marketing purposes," but also states that children's data may be processed on the basis of the exceptions above "as appropriate" (such as to protect the children's welfare).

Return to Table of Contents

FTC Signals 'Rule of Reason' on Privacy and Cybersecurity; New Chairman and Commissioners Nominated

Acting Federal Trade Commission (FTC) Chairman Maureen Ohlhausen has outlined the FTC's approach to privacy and cybersecurity matters, explaining that the commission will adopt a "rule of reason" approach to enforcement and a lighter touch on establishing standards of behavior.

On October 10, 2017, acting FTC Chairman Maureen Ohlhausen outlined a change to the commission's approach to policing privacy and cybersecurity matters. In describing the agency's new "rule of reason" approach, she explained that the commission would not seek to impose unnecessary and undue costs and burdens on businesses.

On October 18, 2017, President Donald Trump nominated Joseph Simons to be the next chairman of the FTC, and he nominated Noah Phillips and Rohit Chopra to fill the two remaining vacancies on the commission.

If President Trump's three nominees are confirmed by Congress — which most believe likely — Republican appointees will occupy three of the five commission seats, at least until September 2018 when Ohlhausen's term will expire.[10] Although Ohlhausen was passed over for the permanent chairman role, most believe that the commission will adopt the type of pro-business approach towards privacy and cybersecurity matters that she described.

Perfect Security Is Not Required

In her statements, Ohlhausen indicated the FTC does not require companies to have "perfect security." Speaking at a National Cybersecurity Awareness Month event hosted by the National Rural Electric Cooperative Association, she said that companies that take cybersecurity and privacy matters seriously, and take reasonable steps to protect their networks and their customers' information, may not need to fear an FTC action against them, even if they are successfully attacked. "We only require reasonable security, not perfect security," she explained.

Ohlhausen also described some of the types of reasonable security measures the FTC would look for in assessing whether a company acted reasonably, including addressing known security vulnerabilities and being honest in statements to consumers about cybersecurity.

Shift From Prior Approach

Ohlhausen, whom President Trump appointed as acting chair this year but who also had a seat on the commission during the Obama administration, has historically been critical of the commission's approach to privacy and cybersecurity measures. She had been against the commission's efforts to create cybersecurity and privacy standards, believing its approach led to trivial information being subject to the same types of protections as more sensitive information.

In the past, the commission had taken an active role in trying to establish privacy and cybersecurity standards, publishing a number of reports and issuing industry-wide guidance on these issues. Under Ohlhausen's leadership, it seems likely the commission will be less active in this area.

With respect to enforcement, however, Ohlhausen does not seem to be proposing a dramatic change. She noted there will likely be cases in which the FTC investigates a security breach and ultimately takes no action based on its assessment that the company in question took a reasonable approach to security issues. If the investigation finds otherwise (as she noted it did in August with respect to Uber) the commission will act. These practices would be consistent with the commission's general historical approach, in which, as Ohlhausen has noted, the commission primarily focused on the "low hanging fruit" with respect to these matters.

Key Takeaway

Ohlhausen's comments suggest that the FTC will take a light touch with respect to privacy and cybersecurity matters in the future, refraining from imposing general standards on practices and taking action in only the most egregious cases. Nevertheless, companies should take cybersecurity matters seriously and ensure they are honest with consumers about their practices.

Return to Table of Contents

Justice Department Pushes for 'Responsible Encryption'

The Justice Department is continuing the debate over the use of encryption in consumer products and whether technology companies should build into their systems a method to enable authorized third parties to decrypt consumer information.

On October 10, 2017, Justice Department Deputy Attorney General Rod Rosenstein called for technology companies to stop providing consumers with encryption tools that make their information unavailable to law enforcement. Instead, he proposed that companies adopt "responsible encryption" approaches that would include an ability for law enforcement to decrypt the information. In a speech at the U.S. Naval Academy in Annapolis, Maryland, Rosenstein explained that warrant-proof encryption poses serious obstacles to the prevention and investigation of crimes.

Background

The tension between concern for public safety and protection of consumer privacy has come into focus in recent years as American technology providers have declined to decrypt customer information, even if faced with a court order to do so. In February 2016, the FBI sought Apple's cooperation in decrypting

[10] By law, no more than three commissioners can be from the same political party. Chopra will fill the open Democratic seat.

the contents of the iPhones used by terrorists in a deadly attack in San Bernardino, California. Apple's refusal — the company claimed it was unable to break the encryption on its customers' devices — brought significant media attention to the issue and prompted a number of major tech companies to articulate positions in favor of privacy (among them Google, Facebook and Twitter). Ultimately, the FBI engaged third-party professional hackers to unlock the devices.

This conflict between privacy and security is not new, but one that has grown more complex as technology has evolved, especially because of technology companies' view that the impenetrability of their encryption systems is a competitive advantage. As consumer demand for secure products is increasing, tech manufacturers and providers remain competitive by offering the most advanced protection for personal data and devices.

On the other hand, the government views such impenetrable encryption as a major obstacle to law enforcement and intelligence gathering. In a speech called "Going Dark" in 2014, then-FBI Director James Comey explained that the failure of law enforcement to keep up with technology advances has created a serious public safety issue. "We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so," said Comey, who further called for assistance and cooperation from technology companies.

'Responsible Encryption'

In his speech, Rosenstein called for technology companies to engage in "responsible encryption" — encryption technology that would enable law enforcement or the technology companies themselves to decrypt information with appropriate authorization. Although he avoided using the term in his speech, Rosenstein's proposal is, in effect, to leave a "back door" in commercially available encryption technologies.

Privacy advocates and technology companies have for many years expressed concerns over the types of encryption technology that Rosenstein advocates. Leaving a mechanism for a third party (such as law enforcement or a technology company) to decrypt information without the user's consent increases the risk that unscrupulous third parties will gain access to the same decryption technology.

Key Takeaway: The Debate Will Go On

The tension between consumers' interest in secure communications and law enforcement's interest in preventing and investigating crime will undoubtedly continue for some time. The Justice Department's call for "responsible encryption" harkens back to the days of the "Clipper Chip" in the 1990s (the technology developed by the National Security Agency to encrypt voice communications, which included a back door for the NSA that was eventually cracked) and other calls for methods to decrypt communications. Companies that enable consumers to encrypt their information should expect continued pressure to develop technologies and/or procedures that seek to resolve this tension.

Return to Table of Contents

Irish High Court Questions Use of Standard Contractual Clauses for Data Transfer

An Irish court has raised serious questions as to the adequacy of the EU's "standard contractual clauses" as a mechanism for allowing transfers of personal data from the EU to the United States.

An October 3, 2017, ruling of the Irish High Court has placed in doubt the continued validity of the European Union's standard contractual clauses as a tool for transferring data outside of the EU. The court expressed concerns regarding protection of EU citizens' data in light of the scope of U.S. surveillance powers and the lack of any effective remedy under U.S. law that is compatible with the EU Charter of Fundamental Rights, neither of which are remediable through contractual clauses. Nevertheless, the court determined that the Court of Justice of the European Union (CJEU) is the proper body to decide whether these contractual clauses should continue to serve as adequate means to demonstrate protection of data, and thus will refer the question to the CJEU for consideration.

Background

Under EU data protection law, data collectors may not export personal data outside the EU to countries that do not, in the EU's view, have adequate data protection laws in place, including the U.S. EU laws do provide a small number of specific ways to enable such a transfer, including through the use of certain standard contractual clauses developed and endorsed by the European Commission. These clauses, which are widely in use today, are incorporated into agreements between EU and U.S. organizations and provide certain contractual data protection rights that are not otherwise available under U.S. law. Other mechanisms include the Privacy Shield negotiated between U.S. and EU regulators, and the use of "binding corporate rules" within multinational organizations.

Max Schrems, an EU privacy activist who filed a complaint with the Irish data protection commissioner against Facebook Ireland Ltd. that ultimately led to the invalidation of the EU/U.S. Safe Harbor regime, also filed a complaint calling into question the validity of the standard contractual clauses. Following the CJEU's ruling on the Safe Harbor, and seeing that much of the CJEU's reasoning seemed to apply equally to other data transfer mechanisms, Schrems argued that the standard contractual clauses do not provide the adequate legal protection necessary to otherwise permit data transfers to the U.S.

The Irish data protection commissioner found that U.S. law does not provide adequate legal remedies to EU citizens, and that this is a shortcoming that cannot be remedied by the standard contractual clauses. However, it also determined that a judicial decision would be required to find the clauses invalid, and thus raised the question to the Irish High Court.

The Court's Ruling

The Irish High Court ruled that valid concerns exist as to whether the standard contractual clauses can provide adequate protection in light of what it perceives as deficient protections under U.S. law. In particular, the court noted the lack of any effective remedy under U.S. law that is commensurate with the requirements of the EU Charter of Fundamental Rights, as well as the risk that the U.S. surveillance regime would lead U.S. authorities to access and process data of EU citizens, in contravention of fundamental rights guaranteed under the charter.

The court noted that the EU/U.S. Privacy Shield regime — which was negotiated as a replacement for the now-defunct Safe Harbor — includes a requirement that the U.S. maintain an ombudsperson to respond to EU citizen complaints. However, it rejected that argument that this mechanism provides effective redress to EU data subjects (who are not parties to the standard contractual clauses) because the ombudsperson is not a judge and is not independent of the executive.

Nevertheless, the Irish High Court concluded that the CJEU is the proper body to review the matter, given a desire for uniformity in the application of data laws across the EU. Accordingly, the court will formulate and refer several questions to the CJEU for a preliminary determination regarding the continued validity of the standard contractual clauses.

The exact framing of the questions that the Irish High Court will offer to the CJEU has not yet been determined. The court is currently accepting submissions regarding the questions to be referred to the CJEU from the parties involved in the matter.

Key Takeaways

The Irish High Court's ruling itself does not have any immediate implications for the use of standard contractual clauses. Having such contracts in place remains a valid means of demonstrating sufficient protections to permit transfers of data outside the EU, including to the U.S. Although it is possible that the CJEU will consider the Irish High Court's questions on an expedited basis given the significance of these issues, it may take some time for a final decision to be rendered. However, if the CJEU ultimately shares the Irish High Court's concerns regarding effective redress, it is unclear that any form of modified model clauses will remedy the concerns. Such a ruling also could impact the Privacy Shield and the binding corporate rules mechanisms for data transfer because the concerns about the effectiveness of the ombudsperson would, presumably, apply to them as well.

While it is far too early for entities to consider contingency plans if the model clauses are invalidated, entities relying on data transfers outside the EU on these bases should keep a close eye on this court case.

Return to Table of Contents

Canadian Privacy Commissioner Intends to Expand Privacy Law Enforcement

The Office of the Privacy Commissioner of Canada released its annual privacy report, announcing an expansion of its approach to privacy compliance and enforcement. The report also included proposals to reform the country's privacy laws.

On September 21, 2017, in its annual report to parliament, the Office of the Privacy Commissioner of Canada (OPC) announced an expanded approach to enforcement of federal privacy laws and made proposals to expand its authority in this area.[11] This is the first time in more than 15 years that Canada is changing the way it enforces its privacy regulation. The report also repeated requests for a reform of federal privacy regulations.

Background

The OPC is the body appointed by Canadian Parliament to oversee compliance with the country's privacy laws, including the Personal Information Protection and Electronic Documents

[11] The OPC's "2016-2017 Annual Report to Parliament on *Personal Information Protection and Electronic Documents Act and the Privacy Act*" is available here.

Act (PIPEDA). Since its founding in 2001, the OPC has acted primarily as an ombudsperson, launching investigations based on complaints received from consumers, rather than taking action on its own initiative. The office has relatively little enforcement power, as it has no authority to issue binding orders to companies. Instead, it acts primarily as an advisory body, tasked with educating the public and parliament on privacy matters. As such, it can only make non-binding recommendations on how companies can revise their practices to comply with law, which companies typically adopt.

Privacy Commissioner Daniel Therrien repeatedly has raised concerns that Canada's current privacy enforcement model is not strict enough, especially in light of the European Union's new GDPR set to come into force in May 2018, which is stricter than its predecessors. The EU has noted in the past that Canada's "adequacy" status is partial in that it only covers PIPEDA, and all future adequacy decisions will involve a comprehensive assessment of the country's privacy regime. The report recognizes that Canada risks losing its adequacy status with the EU if it does not continue to modernize its approach to privacy.

New Approach

Under the OPC's new enforcement model, the office will be able to proactively launch its own investigations in addition to responding to consumer complaints. According to the report, the OPC may be better placed than individuals to identify privacy problems. The office noted that technologies and privacy issues are becoming more complex, making it "increasingly difficult for individuals to fully comprehend" them. The OPC believes that it will be better able to analyze and understand these complexities, and then take action when appropriate.

The report proposed additional reforms to the federal privacy law that would grant the OPC the power to issue orders and levy monetary penalties against companies that violate Canadian privacy laws. It also proposes allowing the OPC to perform voluntary or involuntary audits of the privacy measures taken by companies. These reforms would enable the OPC to assume a key enforcement role with respect to Canadian privacy laws, potentially creating a greater incentive for companies to revise their practices.

Key Takeaways

The OPC's announced changes to its enforcement approach, as well as its requests for greater enforcement authority, are consistent with a general international trend towards greater privacy enforcement. Companies that conduct business in Canada can expect greater scrutiny in the future and should ensure their current practices comply with Canadian privacy laws.

Return to Table of Contents

California District Court Limits FTC's 'Unfairness' Doctrine in Cybersecurity Cases

A California district court has limited the FTC's ability to pursue companies for engaging in "unfair" practices by requiring it to allege more than general risk to consumer information.

On September 19, 2017, a California district court dismissed claims brought by the FTC alleging that D-Link, a networking equipment company, engaged in "unfair" cybersecurity practices under the FTC Act.[12] However, the court refused to dismiss the FTC's claims that the company made "deceptive" representations about the security of its products to consumers. In making its ruling, the court held that the FTC needed to allege more than a mere general risk to consumer information when pursuing claims based on unfair business practices.

Background

On January 5, 2017, the FTC filed a complaint against D-Link under the FTC's authority to regulate unfair and deceptive privacy and cybersecurity practices.[13] The FTC alleged that D-Link engaged in unfair practices by marketing routers and security cameras with widely known and reasonably foreseeable risks of unauthorized access, including the use of hard-coded user credentials and other potential exploits. It also alleged that D-Link engaged in deceptive business practices by marketing the products as supporting the latest wireless security features to help prevent unauthorized access and the best possible encryption, among other safeguards. Although the FTC did not allege that these vulnerabilities resulted in the unauthorized access or misuse of anyone's personal information, the agency asserted they put consumer information at risk of being exposed.

[12] See *FTC v. D-Link Sys., Inc.*, No. 3:17-cv-00039 (N.D. Cal. Sept. 19, 2017). The full text of the district court's order can be found here.

[13] The full text of the complaint can be found here.

There is little debate that the FTC Act provides the agency with the authority to regulate unfair or deceptive acts or practices regarding the privacy and cybersecurity of a company's products. However, the question of what actually constitutes an unfair business practice under the FTC Act has been the subject of heated legal disputes.

For example, in *FTC v. Wyndham Worldwide Corporation*,[14] the FTC alleged that the hotel chain Wyndham had engaged in unfair cybersecurity practices and misrepresented the security of its computer systems in its privacy policy. The hotel chain had failed to protect its computer systems against three hacks in two years, resulting in the theft of customers' personal and financial information and more than $10 million in fraudulent charges. In response to the FTC's allegations, Wyndham challenged the FTC's authority to regulate unfair cybersecurity practices. The Third Circuit disagreed with Wyndham's position and held that the FTC Act granted the agency the authority to regulate in this area.

In *Wyndham*, the hotel chain's inadequate cybersecurity practices were claimed to have resulted in millions of dollars of damage to consumers. However, the FTC's complaint against D-Link posed a different question: Could the FTC's claim of unfair cybersecurity practices survive a motion to dismiss where the agency failed to allege any unauthorized access or misuse of consumers' personal information?

The Court's Decision

Pleadings for Deceptive Acts

The district court first addressed what pleading standard the FTC must meet when it alleges that a company has engaged in deceptive acts related to its privacy and cybersecurity practices. In general, a complaint must contain only a short and plain statement of the jurisdiction of the court, a short and plain statement of the claim showing that the plaintiff is entitled to relief, and a demand for the relief sought. However, the court held that when the FTC alleges that a company has engaged in deceptive privacy and cybersecurity practices, the agency must meet the more stringent pleading requirements under Rule 9(b) to avoid dismissal. That rule requires plaintiffs to state "with particularity" the circumstances that make up the alleged deception or fraud. Thus, to survive a motion to dismiss, the FTC must identify particular deceptive statements or misrepresentations that caused injury to consumers.

In this case, the district court did not dismiss the FTC's claims that D-Link deceived its consumers because the FTC identified specific alleged misrepresentations made by D-Link regarding the company's privacy and cybersecurity practices. However, the court raised the bar for future claims of deceptive privacy and cybersecurity practices brought by the FTC.[15]

Unfair Acts

As for the FTC's claim of unfair cybersecurity practices, the court first identified the elements of an unfairness claim under the FTC Act. To avoid dismissal of a claim that a company engaged in unfair cybersecurity practices, the FTC must allege that the practice (1) causes or is likely to cause substantial injury to consumers, (2) is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.[16]

The court held that the FTC failed to allege that D-Link's cybersecurity practices had caused or were likely to cause substantial injury. The commission did not allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed. Instead, it relied solely on the likelihood that D-Link put consumers at risk because, according to the commission, "remote attackers could take simple steps, using widely available tools, to locate and exploit Defendants' devices, which were widely known to be vulnerable." The court held that more concrete allegations were needed to support a claim, notwithstanding that the statute addresses practices that cause actual injury or are likely to cause injury.

However, the court provided some guidance as to how the FTC might amend its complaint — and style future complaints — to survive a motion to dismiss:

> "[H]ad [the FTC] tied the unfairness claim to the representations underlying the deception claims, it might have had a more colorable injury element. A consumer's purchase of a device that fails to be reasonably secure — let alone as secured as advertised — would likely be in the ballpark of a 'substantial injury,' particularly when aggregated across a large group of consumers."

[14] 799 F.3d 236 (3d Cir. 2015). The full text of the opinion can be found here.

[15] The court did not decide whether Rule 9(b)'s more stringent pleading standard applies to claims of unfair cybersecurity practices.

[16] See 15 U.S.C. § 45(n).

The court appears to be reasoning that the purchase of a product that offers less protection than advertised is, in and of itself, an injury sufficient to support a claim of unfair business practices in violation of the FTC Act.

It remains to be seen whether the FTC will follow the court's suggestion to connect the claims of deceptive and unfair cybersecurity practices in its amended complaint, which must be filed by January 12, 2018.

Key Takeaways

The district court's decision limits the likelihood that the FTC will succeed in actions against companies for unfair cybersecurity practices where the company made no deceptive statements and its practices did not result in any actual harm to consumers. In doing so, the court seems to be limiting the FTC's ability to claim unfair business practices that are likely to cause harm, as described in the statute, unless the practices are coupled with deceptive practices or actual consumer harm. The decision will be a welcome one for companies that were concerned about the uncertainties surrounding the FTC's efforts to prevent unfair cybersecurity practices.

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

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

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

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

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

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

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

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

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

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

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