SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

Skadden PRIVACY UPDATE

An Overview of Legislative, Regulatory and Technology Developments in the Privacy Sector

2.9.12

INSIDE

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact **Stuart D. Levi**, 212.735.2750, stuart.levi@skadden.com or your regular Skadden contact.

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

EU to Revamp Its Data Privacy Rules

Ever since the adoption of the EU Data Protection Directive in 1995, the European Union (EU) has been viewed as a leader in the regulation of data privacy. Now, some 12 years later, the EU is once again in the spotlight, with the European Commission proposing a significant reworking of the EU's approach to data protection. The commission's proposal, coming after a two-year study of online activity and the use of personal information, is designed both to enhance individual privacy protection and to simplify the administrative process for companies that must today deal with multiple data protection authorities, and a myriad of similar, but different, country-specific laws. The proposed regulation also would impact U.S. companies that collect or process personal data of EU citizens, and likely will need to adopt how they handle such data.

The premise underlying the commission's proposal is that global commerce will be enhanced if users feel comfortable with how their data may be used and processed. Moreover, EU companies would have a competitive advantage if the EU offered this level of protection when other countries do not.

The European Commission's proposal (the Regulation) — comprised of draft regulations and explanatory texts — was published on January 25, 2012.[1] The proposal will now be discussed, and potentially modified, by the EU's Council of Ministers and the European Parliament, a process that could take approximately one year. Once a final draft is adopted by the European Parliament, it would likely go into effect within two years.

Set forth below is a summary of some of the key provisions included within the proposed Regulation.

Simplifying Compliance

CREATING A SINGLE, UNIFIED REGULATION

Under the Data Protection Directive of 1995 (Directive),[2] while each EU Member State was required to enact and implement data privacy laws that met the minimum requirements of the Directive, they were free to design their own laws and regulations. The result was a myriad of national data privacy laws, each taking a slightly different approach. Companies transacting business in multiple European jurisdictions therefore needed to track, and comply with, multiple laws, often at high administrative costs. Thus, the Directive's attempt of creating a unified data protection regime to enhance EU economic activity fell far short of its intended goal.

1 Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012).

2 Council Directive 95/46/EC, 1995 O.J. (L 281).

In order to alleviate this problem, the European Commission's current proposal is couched as a Regulation, as opposed to a Directive. The Regulation would create a single uniform data privacy law across all EU members, thus eliminating the current country-specific structure.[3]

DEALING WITH A SINGLE DATA PROTECTION AUTHORITY

As part of simplifying the administrative burden on data controllers and processors, under the proposed Regulation entities with offices in multiple Member States would no longer be required to deal with the data protection authority (DPA) in each country. Rather, the DPA in the country where the data controller or data processor has its "main establishment" would be responsible for supervising the activities of that entity in all Member States. In addition, individuals will have the right to refer all cases to their home DPA, even when their personal data is processed outside of their home country.

DOCUMENTING DATA PROCESSING OPERATIONS

The EU Directive currently requires "notification" of an entity's data processing activities to each applicable DPA. This sometimes cumbersome requirement would be replaced by a new paradigm in which data controllers and processors instead would be required to create and maintain documentation of their data processing activities. Such documentation only would need to be provided when requested by a DPA. While the administrative burden would be reduced, companies would nonetheless be required tdo monitor and document their own processing activities. Much of the documentation that companies will be required to maintain is similar to what is mandated under the current Directive with certain additions, such as the obligation to record transborder data transfers.

OUTSOURCING AND CLOUD COMPUTING

The proposed Regulation recognizes that, in today's environment, there can be more than one data controller. This can have an important impact on outsourcing and cloud computing relationships where the vendor could be deemed a data controller along with its customer that collected the data. Joint data controllers are required to determine the extent to which they are required to comply with the Regulation and are jointly responsible for failing to do so. The European Commission also has highlighted the expanded use of binding corporate rules (discussed below) to make it easier for companies to engage in cloud computing within their own organizations

Enhancing Individual Protections

REVAMPING THE CONSENT REQUIREMENT

When the EU Directive was being debated in the mid 1990's, one of the key issues was the form of individual consent that would be required when collecting data. The Directive arrived at the concept of "opt-out" consent, with certain exceptions for sensitive data. The proposed Regulation would revamp the consent requirement, by imposing a "specific, informed, and explicit" consent standard. Companies can therefore no longer assume that individuals have consented because they did not check a box opting-out. Rather, they will need to develop a means for demonstrating explicit consent.

A NEW "RIGHT TO BE FORGOTTEN" AND "RIGHT TO PORTABILITY"

The current EU Directive provides individuals with certain basic privacy rights, such as the right to access and correct their information. The proposed Regulation adds a new "right to be forgotten." As its name implies, this right would allow an individual to demand that his or her personal data be erased fully so that it can no longer be accessed by any means.

---

3 The European Commission's proposal also includes a separate Directive that would address criminal investigations.

The Regulation also would add a "right of portability" that would prohibit a data controller from preventing an individual from migrating his or her data from that controller to another. The controller also would be obligated to provide the data to the individual in a commonly used format. In practical terms, this would allow users of a social networking site to require the provider to give them their data in a format that would allow them to port that data to another social network.

NOTICE OF DATA SECURITY BREACHES (30-32)

The Regulation would add a requirement that data controller's provide notification of security breaches involving personal data; a concept with which U.S. companies are already familiar under the various state laws that exist today. Under the Regulation, the data controller would be required to provide notice to the DPA within 24 hours and to the affected data subjects if the breach "is likely to adversely affect the protection of the personal data or the privacy of the data subject." In this respect, the European Commission has adopted the less-onerous approach of only requiring notice where an adverse affect is likely, as opposed to requiring notice whenever there has been unauthorized access to data, a more rigorous standard that some U.S. states have imposed. Notice to individuals must be provided without undue delay after the DPA has been notified.

PRIVACY BY DESIGN

Companies will be required to adopt so-called "privacy by design" concepts into their business operations. Under this approach, often discussed in U.S. privacy proposals, data protection safeguards are to be included in products and services at their earliest stages of development. The idea is that companies will be more mindful of privacy concerns if they are included at the product development stage. The Regulations also suggest that the default settings for sites should be privacy-friendly.

IMPACT ON NON-EU COMPANIES (40-45)

The proposed regulation would impose a number of new obligations on non-EU entities. For example, data controllers outside the EU, but who process data of EU residents, would be required to have a designated data representative in the EU. However, the proposed Regulation does not make it more difficult to send personal data from Member States to the U.S. The Regulation leaves in place the options of using model contracts or contractual clauses that have been approved by a DPA. In addition, the proposed Regulation expands the availability of binding corporate rules as an option for sending data outside the EU, particularly within a corporation. While under the current Directive, such rules must be approved by three different DPAs, the proposed Regulation only would require approval from one DPA. Transfers made under binding corporate rules also would no longer require prior authorization.

The proposed Regulations also propose to streamline the process for determining whether a country offers an "adequate" level of data protection that would allow transborder data flows from the EU without the need for other protections such as model contracts.

Sanctions for Non-Compliance

Entities that violate the proposed Regulation face the potential of significant penalties and sanctions. Under the regulations, violators are subject to fines of up to 1 million euros or 2 percent of the entity's annual global turnover, figures that are much higher than current penalties.

Impact on U.S. Companies

It will be at least two years before the proposed Regulation goes into effect, and many provisions may be modified or even eliminated during the review process that is about to unfold. Nonetheless, companies that collect or process any data of EU citizens, including if it is data

concerning their own employees, should closely track how the Regulation evolves. In addition, the structure proposed by the EU, and the position it has taken on certain issues could have an influence on data privacy legislation that is being considered in the U.S.

Class Action Lawsuits for Data Breaches

When companies evaluate the ever-growing risk of data security breaches, they focus, in part, on the potential for third party class actions brought by the individuals whose data has been breached. A recent Third Circuit decision, *Reilly v. Ceridian Corporation*,[4] has helped bring some clarity to assessing this risk. In that case, the court dismissed a data security breach class action complaint holding that, without evidence of any actual harm caused by a breach, claims of "an increased risk of identity theft" are insufficient to confer standing.

BACKGROUND

Ceridian Corporation — a Human Resources, payroll and benefits processing firm — collects and processes personal and financial information about its clients' employees. This information includes the employees' names, addresses, social security numbers, dates of birth and bank account information.

In December 2009, Ceridian experienced a data security breach when an anonymous hacker infiltrated Ceridian's Powerpay system. While 27,000 employees at 1,900 companies potentially were exposed as a result of the breach, there was no evidence that the hacker actually read, copied or understood the data. Following the breach, Ceridian worked with law enforcement and professional investigators to determine which information the hacker may have accessed. Ceridian also issued a letter to those individuals whose information was accessed, notifying them of the breach, and arranged to provide the potentially affected individuals with free credit monitoring and identity theft protection for a year.

A class action of those whose data was breached was filed in October 2010. The complaint alleged three harms: a) exposure to an increased risk of identity theft, b) costs incurred to monitor credit activity and c) emotional distress. Ceridian filed a motion to dismiss the case for lack of standing and failure to state a claim. The district court granted Ceridian's motion, finding that the plaintiffs lacked standing, and that even if they had standing, they had failed to state a proper claim. The plaintiffs appealed.

THIRD CIRCUIT DECISION

In order to establish standing, a plaintiff must establish "injury-in-fact," under which the plaintiff must have suffered the invasion of a legally protected interest that is a) concrete and particularized, and b) actual or imminent, and not conjectural or hypothetical. Vague allegations of possible future injury historically have not been sufficient to satisfy this requirement.

The Third Circuit found that the plaintiffs' argument relied on speculation regarding a hypothetical future injury, and therefore was insufficient to confer standing. The court noted that the plaintiffs' argument depended upon a string of assumptions: that the unknown hacker (a) actually read, copied and understood the personal information contained in the database, (b) intends to commit criminal acts in the future by misusing this information and (c) is able to use this information to commit identity theft in such a way that would harm the plaintiffs. The plaintiffs had failed to provide any evidence that their personal data has been, or ever will be, misused. The court found the plaintiffs' position to be too tenuous to be assumed without any proof, and that unless and until these conjectures come true, the plaintiffs have not suffered any injury. Without misuse of the information, according to the court, there is no harm.

---

4 *Reilly v. Ceridian Corp.*, No. 11-1738, 2011 WL 6144191 (Dec. 12, 2011).

CONTRAST WITH OTHER CIRCUITS

The Third Circuit's decision in *Reilly* seemingly stands in contrast to rulings of other Circuits in similar identity theft class actions. In *Pisciotta, v. Old National Bancorp,*[5] a case involving the hacking of a bank website, the Seventh Circuit found that an increase in the risk of future identity theft was sufficient alone to satisfy the injury-in-fact requirement. Similarly, in *Krottner v. Starbucks*[6], the Ninth Circuit found that the theft of a laptop containing personal information from a Starbucks was sufficient to create a "credible threat of real and immediate harm," and confer standing.

The Third Circuit distinguished these cases, finding that they presented more evidence of harm or future harm than present in the case before it. In *Pisciotta*, there was evidence that the hacker's intrusion was sophisticated, intentional and malicious, while in *Krottner*, an unauthorized person actually attempted to open a bank account using the information held on the laptop. In contrast, the Ceridian hacker merely penetrated a firewall, and there was no identifiable "taking" of information or evidence of the intention to do so.

The Third Circuit also criticized the *Pisciotta* and *Krottner* courts for their cursory analyses of the standing requirement. Those cases analogized data theft situations to defective medical device or toxic substance exposure cases, but the court found that these rationales fell short for two reasons. First, in those cases, an injury undoubtedly has occurred; for example, a person was exposed to a toxic substance, damaging cells and introducing a disease mechanism. In such situations, in contrast to data breach cases, the only problem is quantification, not whether damage has in fact been done. Second, the nature of the human health concerns inherent in toxic tort and medical device cases loosens the test for standing. According to the *Reilly* court, any future damages that might arise as a result of a data security breach adequately can be redressed with money damages, with little concern that the plaintiffs will become sick or die as a result of the harm. The court also rejected an analogy to environmental injury cases, where standing requirements are similarly loosened due to the potential inability for future compensation to adequately return plaintiffs to their original position.

The *Reilly* decision also should be considered in light of the First Circuit's recent court decision in *Anderson v. Hannaford*.[7] In that case, hackers broke into a grocery store's electronic payment processing system, stealing up to 4.2 million credit and debit card numbers, expiration dates, and security codes. At the district court, the claims of plaintiffs who had not actually experienced unauthorized charges were dismissed, and the claims of those whose unauthorized charges had been reversed were deemed "too remote" to allow recovery. However, the First Circuit reversed in part and ruled that all plaintiffs were entitled to compensation for mitigation damages, to recover amounts spent purchasing identity theft insurance and accessing replacement cards. This indicates that in the case of a security breach, preventative actions taken to avoid future damage may be considered reasonable, and therefore compensable, even for individuals who have not personally experienced identity theft. It was highly relevant to *Anderson* that the hackers in that case were sophisticated thieves acting intentionally to use the stolen data to their financial advantage and actually did so in thousands of cases. Unlike in *Reilly*, in *Anderson* "the card owners were not merely exposed to a hypothetical risk, but to a real risk of misuse."

PRACTICE POINTS

The different approaches of the Third, Seventh and Ninth Circuits to the question of standing in data security breach cases, albeit under different fact patterns, indicates that this issue is by no means resolved. Nonetheless, the *Reilly* decision provides important precedent for companies to argue that plaintiffs must come forward with evidence of actual harm (*e.g.*, actual identity theft) to establish standing. This information should go into any risk and liability assessment of a data security breach.

---

5 *Pisciotta v. Old National Bancorp*, 499 F. 3d 629 (7th Cir. 2007).

6 *Krottner v. Starbucks Corp.*, 628 F. 3d 1139 (9th Cir. 2010).

7 *Anderson v. Hannaford Brothers Co.*, Nos. 10-2384, 10-2450 (1st Cir. C.A., Oct. 20, 2011).