June 2015

Skadden

Privacy & Cybersecurity Update

USA Freedom Act Brings Changes to Surveillance Program

The new Freedom Act changes the way the government collects information in bulk.

On June 2, 2015, following expiration of three controversial provisions of the USA Patriot Act, President Barack Obama signed into law the USA Freedom Act, setting into motion a change to the National Security Agency's (NSA) controversial surveillance program. The reception of the Freedom Act's passage has been mixed; some believe it to be a meaningful post-9/11 surveillance improvement, while others maintain it does little to ameliorate privacy concerns.

As reported in the May 2015 edition of *Privacy & Cybersecurity Update*, the NSA's mass data collection program first came under public scrutiny in 2013 following former government contractor Edward Snowden's information leak. Under the authority of Section 215 of the Patriot Act, the program involved telecommunications operators delivering telephone record metadata directly to the NSA. The NSA would then comb through this data to gather information on anticipated terrorist threats. In May 2015, in *ACLU v. Clapper*,[1] the U.S. Court of Appeals for the Second Circuit rejected the interpretation of Section 215 that granted the government this sweeping power. The court found that allowing the collection of business records that are "relevant to an authorized investigation" under Section 215 could not be read to include the dragnet collection of telephone records for a broad counterterrorism effort. *Clapper* thus foreshadowed the imminent dismantling of the existing surveillance apparatus.

The Freedom Act, approved by the Senate in a 67-32 vote in early June 2015, is the first piece of legislation to reform post-9/11 surveillance measures. Under this law, Congress removed the government's role in record storage by shifting the collection burden to telecom companies like AT&T and Verizon. This tactical transfer does not eliminate government access to the collected records altogether. The government can still require telecom companies to turn records over to the government in response to a targeted government warrant approved by the Foreign Intelligence Surveillance Court. To further place a check on mass data collection, the bill requires the NSA to submit targeted search criteria in its surveillance requests as opposed to broad categories like entire geographical regions or networks.

[1] *American Civil Liberties Union v. Clapper,* 785 F.3d 787 (2d Cir. 2015).

The rolling back of the NSA's surveillance powers does not fully alleviate privacy concerns that some have raised. The Freedom Act temporarily reinstitutes the telephone record collection program for six months as the NSA and telecom companies transition to the new program. Furthermore, the Freedom Act does nothing to address the agency's surveillance of the Internet under programs like PRISM, the existence of which was also made public by Snowden.

Return to Table of Contents

Connecticut Enacts Bill Imposing Tighter Data Security Obligations

A new law would make Connecticut the first state to mandate the provision of identity theft protection for data breach victims.

If signed into law, Connecticut will be the first state to require that companies provide identity theft protection services to Connecticut residents who are the victims of a data breach involving their Social Security number and first and last name or first initial and last name. The bill, "An Act Improving Data Security and Agency Effectiveness,"[2] requires companies to, starting October 1, 2015, provide these services for at least 12 months in the event of a data breach. The law also would require companies to notify residents of the breach "without unreasonable delay but not later than ninety days after the discovery of such breach," and also to notify the state attorney general.

While 47 states have data breach notification laws, Connecticut would be the first to explicitly mandate that companies provide identity theft services and information on how affected residents can place a credit freeze on their file. As we reported in our October 2014 *Privacy & Cybersecurity Update*, in 2014, California became the first state to address the provision of identity theft protection. However, the bill's wording was highly ambiguous, stating that "an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months."[3] Given the use of the words "if any," it remains unclear whether California requires businesses to provide these services for 12 months or whether the law imposes a 12-month minimum requirement only if a company chooses to provide these services. In contrast, Connecticut's bill makes clear that companies must provide identity theft protection services for one year.

Under the law, an entity would not need to notify Connecticut residents and provide identity theft prevention services if, after an investigation with relevant federal, state and local agencies, the entity reasonably determined that the breach was unlikely to harm the affected individuals.

State Contractor Requirements

The bill also imposes new obligations, effective July 1, 2015, for contractors that receive confidential information from state agencies. All entities with confidential information from state agencies must implement and maintain a comprehensive data security program at its own expense. The program must include the use of security policies relating to the storage, access and transportation of confidential data, restrictions on access, annual review of security measures and ongoing security awareness training for employees. In addition, contractors must store confidential data in a secure server, on secure drives, behind firewall protections monitored by intrusion detection software. Lastly, in the event of an actual or suspected breach, the contractor must notify the state contracting agency and the state attorney general "as soon as practical" after becoming aware and stop all use of the data.

The law provides flexibility for the Office of Policy and Management secretary to require additional or alternate protections under certain circumstances. Factors to consider in fashioning alternative protocols include the type and amount of confidential information being shared, the purpose for which the information is being shared and the types of goods or services involved in the contract.

Insurance Industry Requirements

The law also tightens data protection protocols for health insurance providers, pharmacy benefit managers, third-party administrators and utilization review companies. Starting October 1, 2015, each entity must implement and maintain a comprehensive information security program to protect the personal information of insureds and enrollees. The program must include, among other measures, access control rules, unique user identifications and passwords that must be reset at least every six months, encryption of information under specific circumstances, security breach monitoring, employee training on security systems and oversight of third parties with which the health care company shares personal information. On or after October 1, 2015, each company must annually certify, under penalty of perjury, to the Connecticut Insurance Department that it maintains a comprehensive information security program meeting the legal requirements.

[2] S.B. 949, 2015 Leg. (Conn. 2015).

[3] Cal. Civ. Code § 1798.84(d)(2)(G).

Takeaway

The bill signifies a move toward stricter data breach prevention requirements and stronger consumer protection mandates in the event of a breach. Any company conducting business in Connecticut should be prepared for passage of the law by ensuring its data breach prevention and response protocols comply with the act's requirements. The act also is yet another example of how states are filling the void created by a lack of federal data breach notification or cybersecurity laws.

Return to Table of Contents

Pennsylvania Court Dismisses Data Breach Negligence Claim

A Pennsylvania decision will make it more difficult for plaintiffs to sustain negligence claims for data breaches in that state.

On May 28, 2015, in *Dittman v. UPMC*,[4] an Allegheny County judge dismissed a class action lawsuit seeking damages stemming from a massive data breach at the University of Pittsburgh Medical Center (UPMC). The court's reasoning highlights the obstacles that class action plaintiffs are facing in data breach cases. Specifically, the court's foreclosure of a negligence theory for data breaches absent physical injury or property loss joins a growing number of state courts that have found that these plaintiffs cannot sustain a class action in data breach cases. However, due to the unique aspects of Pennsylvania state law, the broader impact of *Dittman* remains to be seen.

Background

UPMC is an integrated global nonprofit health services enterprise with more than 60,000 employees. In 2014, UPMC first discovered that it had suffered a massive data breach when various employees' tax returns were filed fraudulently. It later found that names, birthdates, addresses, Social Security numbers, tax information, salaries and bank account information of all 62,000 employees had been stolen from UPMC's computer system. In response, UPMC offered free fraud detection services to all employees and also established a payroll hot line and retained a tax firm to help workers complete IRS identity theft forms. Employees alternatively were offered a $400 reimbursement if they used their own accountants to check for fraud.

Following the discovery of the data breach, a class representing all 62,000 current UPMC employees brought suit. The class asserted two claims against UPMC. First, it asserted a negligence claim, alleging that UPMC breached its duty of care to safeguard and secure its employees' personal information. Second, the class brought a claim for breach of an implied contract, arguing that UPMC breached its implied contractual obligation to protect the security of employee information. UPMC filed preliminary objections arguing that (i) the class representatives did not have standing to maintain an action premised on a hypothetical future injury, (ii) the negligence claim was barred by the economic loss doctrine, and (iii) the breach of contract claim failed for lack of mutual intent and consideration.

The Court's Ruling

The court sustained UPMC's preliminary objections to both claims, concluding that under the state's economic loss doctrine, no cause of action can exist for negligence that resulted solely in economic losses unaccompanied by physical injury or property damage.[5] This dismissal is significant because it largely forecloses negligence liability in Pennsylvania data breach cases, since these cases rarely, if ever, involve physical injury or property damage. The court also dismissed the claim for breach of implied contract because there was no "meeting of the minds." UPMC made no promises and signed no agreement securing employee protection against data breaches.

In rendering its decision, the court analyzed the public policy implications of creating an affirmative duty of care for companies to protect information from data breaches by third parties. The court offered three rationales for not creating such a duty:

- **Proliferation of Data Breaches.** The court observed that the frequency and sophistication of data breaches made it almost impossible for entities like UPMC to prevent. The creation of a private cause of action in negligence would therefore result in a flood of litigation that Pennsylvania courts are not equipped to handle.
- **Heavy Burden on Business Entities and Employers.** The court also highlighted the strain data breach lawsuits would have on businesses that would be required to expend substantial resources for suits grounded in negligence and breach of contract. According to the court, "these entities are victims of the same criminal activity as the plaintiffs." Moreover, the court, citing the Pennsylvania Supreme Court's decision in *Seebold v. Prison Health Services, Inc.*,[6] noted that imposing

[4] *Dittman v. UPMC*, No. GD-14-003285 (Pa. Ct. Com. Pl., Allegheny Cnty., May 28, 2015).

[5] This principle was established in *Excavation Technologies, Inc. v. Columbia Gas Co.*, 936 A.2d. 111 (Pa. Super. 2007).

[6] *Seebold v. Prison Health Services, Inc.*, 57 A.3d 1232 (Pa. 2012).

this duty of care on businesses could put them out of business entirely. Judge R. Stanton Wettick Jr. emphasized that requiring additional safeguards and improved protection systems would be costly and still would not guarantee protection for employees (and thus be a liability for the employers).

- **Legislature's Role.** The court also highlighted the state legislature's role in shaping the law on data breaches. The legislature previously passed the Pennsylvania Data Breach Act, which addresses the obligations of entities that suffer a breach of their computer system. Given the legislature's proven awareness of these issues, the court suggested that any future developments of the law should be of a legislative, not judicial, nature.

Practice Point

As we have previously reported, including in our March 2015 *Privacy & Cybersecurity Update*, victims of data breaches face a difficult road when pursuing their claims. They must show a demonstrable injury or an imminent threat of future injury, which in and of itself is difficult given the nature of data breaches. Now, in Pennsylvania and states with similar legal doctrines, *Dittman* adds another requirement — the injury cannot solely be economic loss, but rather must be accompanied by physical injury or property damage.

The court's discussion of the policy considerations of imposing negligence liability in data breach cases lends another concerned voice to the debate. Courts in Pennsylvania and other states have noted that while companies might have a duty to protect against data breaches, that duty must be balanced against the practical reality that protecting against such breaches is almost impossible, especially since companies are themselves victims. In Pennsylvania, at least, that balance has fallen in favor of companies and employers, with *Dittman* potentially serving as valuable protection from data breach liability.

Return to Table of Contents

Nevada Federal Court Dismisses Claims Against Zappos over Customer Data Breach

A Nevada court holds that plaintiffs in a data breach case could not establish standing.

In yet another setback for plaintiffs seeking to bring cases against companies arising from data breaches, a Nevada court found in *In re Zappos.com, Inc., Customer Data Security Beach Litigation*,[7] that the plaintiffs, whose personal data had been breached when Zappos was hacked in 2012, lacked Article III standing to sue for damages, and granted Zappos' motion to dismiss.

Background

Zappos, an online apparel retailer owned by Amazon.com, Inc., suffered a data breach in January 2012, when hackers gained access to Zappos' servers containing the personal identifying information of approximately 24 million customers. The next day, Zappos notified customers of the data breach, which involved customer names, account numbers, addresses and the last four digits of their credit card numbers. Several customers sued Zappos for damages, alleging various causes of action, including negligence, public disclosure of private facts and breach of contract.[8] The plaintiffs subsequently consolidated their pleadings into two separate class action complaints. Zappos filed a motion to dismiss for lack of standing and failure to state a claim, which the court granted in part and denied in part. After about two and a half years of procedural jockeying and a failed attempt at mediation, Zappos renewed its motion to dismiss.

Zappos argued that the plaintiffs failed to allege actual damages arising from the data breach. The plaintiffs, however, contended that they had Article III standing based on (i) the increased threat of future harm as a result of the breach, (ii) the decreased value to their personal information, and (iii) the cost they incurred to mitigate the risk of harm. The court rejected all three of the plaintiffs' theories and granted Zappos' motion to dismiss.

Increased Risk of Harm Under *Clapper* and *Krottner*

In order to determine whether the plaintiffs had standing based on increased threat of future identity theft and fraud, the court looked to precedent set by the U.S. Court of Appeals for the Ninth Circuit in 2010 in *Krottner v. Starbucks Corp.*,[9] and in 2014 by the U.S. Supreme Court in *Clapper v. Amnesty International*.[10] In *Krottner*, the Ninth Circuit set forth a two-prong test for victims of data breaches to establish standing: The plaintiff must have suffered (i) "a credible threat of harm," which must be (ii) "both real and immediate, not conjectural or hypothetical." Four years later, in *Clapper*, the Supreme Court established an arguably more rigorous standard for standing, holding that the injury must be "certainly impending." Relying on *Clapper*, a number of courts have held that the mere increased risk of identity theft or fraud, without allegations of actual harm, is insufficient to establish standing. While some have asserted that *Krottner* and *Clapper* are incompatible, the *Zappos* court did not see any issue with reconciling them, noting that *Krottner*'s

[7] No. 12 CV 00325, 2015 WL 3466943 (D. Nev. Jun. 1, 2015).

[8] *In re Zappos.com, Inc., Customer Data Security Breach Litigation*, No. 3:12–cv–00325–RCJ–VPC, 2013 WL 4830497 (D. Nev. Sept. 9, 2013).

[9] 628 F.3d 1139 (9th Cir. 2010).

[10] 133 S.Ct. 1138 (2014).

two-part test requires the "same immediacy of harm that the Supreme Court emphasized in *Clapper*."

The *Zappos* court determined, based on this precedent, that the immediacy of the potential harm is what is critical: "It is not enough that the credible threat may occur at some point in the future … even if a plaintiff faces a real threat, she has no standing until that threat is immediate." The court then noted that three and a half years had gone by since the Zappos breach occurred, and none of the plaintiffs had alleged they actually suffered the feared harm. Although the court resisted speculating about the significance of the passage of time for evaluating the credibility of a threat, time was indeed relevant to determine the imminence of the harm. The court concluded, "There must be a point at which a future threat can no longer be considered certainly impending or immediate, despite its still being credible." It held that, in this case, the plaintiffs' potential harm was not sufficiently imminent to confer standing under *Clapper* and *Krottner*.[11]

Other Arguments: Decreased Value of Personal Information and Cost to Mitigate Harm

The court quickly dispensed with the plaintiffs' argument that they were entitled to recover because the breach had deprived them of the "substantial value" of their personal information. The court pointed out that the plaintiffs did not indicate how their information became less valuable as a result of the breach, nor did they attempt to sell their information unsuccessfully.

Finally the court rejected the suggestion that the purchase of credit monitoring services warranted standing. Even though the purchase may have been reasonable and based on rational fears, plaintiffs cannot "manufacture standing by inflicting harm on themselves," the court ruled.

Conclusion

In re Zappos.com highlights that immediacy of the threatened harm is key to establishing standing under Article III in the context of a data security breach. A lengthy passage of time without incident suggests that the threat is no longer imminent and impending, even if it is still credible. But although the court here held that the plaintiffs did not have standing, *Zappos* left open the possibility that increased risk of injury is not necessarily insufficient. Plaintiffs may have standing so long as their risk of harm meets the *Clapper* or *Krottner* requirements: The threat must be real, credible, certain and imminent.

Return to Table of Contents

Recent Decision Keeps Spotlight on Cyber Insurance

A Utah district court decision highlights some of the difficulties with relying on traditional insurance for data breach claims.

Insurance coverage for cyber losses and data breaches has become an increasingly important consideration for companies of all types and sizes. A recent decision illustrates the need to thoroughly understand what types of risks may and may not be covered by certain policies in order to best use insurance as a risk management tool.

In *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc.*,[12] the U.S. District Court for the District of Utah addressed coverage under a cyberinsurance policy. In that case, Travelers issued a CyberFirst policy to Federal Recovery Services, Inc. (FRS) and Federal Recovery Acceptance, Inc. (FRA), which were in the business of providing electronic data processing services to their customers, including fitness center operator Global Fitness Holdings, LLC (Global). Global's members provided credit card or bank account information (Member Accounts Data) that enabled Global to automatically collect monthly membership dues. Pursuant to a servicing agreement, FRA electronically withdrew the requisite funds from the member accounts and transferred those funds, less FRA's fee, to Global. For security purposes, FRA retained the only copy of the Member Accounts Data.

In connection with an asset purchase agreement (APA), Global subsequently agreed to transfer all of its Member Accounts Data to L.A. Fitness. After initially agreeing to cooperate in that data transfer, FRA allegedly withheld "several critical pieces of the information," including credit card, checking account and savings account information. Instead, and despite repeated requests for its return, FRA allegedly "withheld the Member Accounts Data until Global Fitness satisfied several vague demands for significant compensation." Global thus filed suit against FRA, asserting claims for conversion, tortious interference with the APA and breach of contract. Global later amended the complaint by adding similar allegations against FRS, namely that it, too, with-

[11] The court distinguished prior Ninth Circuit cases in which plaintiff targets of a data security breach were deemed to have standing, *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-cv-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014) and *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014). In those cases, the plaintiffs noted that their stolen information surfaced on the Internet shortly after the breach, and they were temporarily unable to use certain paid services. More importantly, the courts in both those cases ruled on the motion to dismiss much sooner after the breach than in this case.

[12] No. 2:14-CV-170 TS, 2015 WL 2201797, at *1 (D. Utah May 11, 2015).

held the Member Accounts Data "unless and until Global Fitness satisfied several demands for significant compensation above and beyond what were provided in the [servicing] Agreement."

FRS and FRA tendered defense of the action to Travelers under the CyberFirst® policy's Technology Errors and Omissions Liability Form, which provided coverage if the loss is caused by an "errors and omissions wrongful act," defined by the policy as "any error, omission or negligent act." Travelers responded by filing a coverage action, seeking a declaration that it owed no duty to defend FRA and FRS against Global's claims in the underlying litigation because they did not constitute an "errors and omissions wrongful act." FRA and FRS moved for summary judgment on the issue, countering that Global's claim that they "'withheld' the data is broad enough to encompass [a] possible error, omission or negligent act."

But after comparing the allegations of the underlying complaint to the insurance policy (employing the so-called "eight corners" rule in which a liability insurer›s duty to defend its insured is assessed by reviewing the claims asserted in the plaintiff›s complaint, without reference to matters outside the four corners of the complaint plus the four corners of the policy), the court agreed with Travelers, opining that FRS and FRA's "argument does not withstand scrutiny." Specifically, the court found that "Global does not allege that Defendants knowingly withheld the data because of an error, omission, or negligence." Rather, "Global alleges that Defendants knowingly withheld this information and refused to turn it over until Global met certain demands … despite repeated requests from Global to provide the data." Thus, "[i]nstead of alleging errors, omissions, or negligence, Global alleges *knowledge, willfulness, and malice*." Because "none of Global's allegations involve errors, omissions, or negligence," the court ruled that Travelers had no duty to defend FRA and FRS in this instance.

* * *

The outcome of any particular insurance claim will turn on the specific facts and policy language, and all potentially available coverage should be carefully considered in the wake of a loss of any nature. The court's decision in *Travelers* illustrates that even specialty cybersecurity policies have their boundaries, and that courts will apply long-established rules of construction in their interpretation. As one component of any risk management program, companies continue to be best served by proactively evaluating and thoroughly understanding their insurance programs with respect to cyber/data risks before any such losses materialize.

Return to Table of Contents

EU Moves One Step Closer to New General Data Protection Regulation

EU moves to the next stage in its efforts to enact a new General Data Protection Regulation.

For the last three years, there has been much discussion and political wrangling regarding a new a new General Data Protection Regulation for the European Union. The proposed regulation would create a single data protection law for all of the EU that would apply to all businesses processing personal data of EU citizens, regardless of where they are located in the world. On June 15, 2015, a significant hurdle was overcome that increases the likelihood of the regulation being enacted. On that date, ministers representing the member states at the EU Justice and Home Affairs Council reached an agreement on a so-called General Approach to the Proposed Regulation. The next step, which commenced on June 24, 2015, will be for "trilogue" discussions among the European Parliament, Council of Ministers and European Commission to arrive at a single consensus regulation. The objective is to reach such a consensus by the end of 2015.

Among the many critical issues that these different bodies must now resolve are:

- The standard of individual consent that would be required before personal data could be processed. While the European Parliament has backed rules requiring "explicit" consent, the council's draft specifies the need for "unambiguous" consent to personal data processing.
- The level of sanctions that can be imposed for a violation of the new law. Parliament has advocated sanctions for violating the regulation of up to 5 percent of a company's annual global turnover, while the council has advocated a 2 percent turnover.
- Whether, and to what extent, an individual EU member could maintain or introduce more specific provisions or further conditions in their own national laws.
- The so-called "right to be forgotten," under which individuals would be allowed to require search engines, and perhaps even websites, to erase data about them.
- The creation of a "one-stop-shop" system in which companies would only have to deal with a single data protection authority, even if they do business in multiple countries.

Given the number of issues to address, resolution by the end of 2015 may be unrealistic. However, the commencement of trilogue discussions is an important next step in this process.

Return to Table of Contents

Contacts in the Privacy and Cybersecurity Group

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

Cyrus Amir-Mokri
Partner / New York
212.735.3279
cyrus.amir-mokri@skadden.com

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

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

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

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

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

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