Skadden

Privacy & Cybersecurity Update

1 Dismissal in P.F. Chang's Data Breach Case Shows Challenge Plaintiffs Face in Such Actions

2 Eleventh Circuit Court of Appeals Decision Underscores the Need to Evaluate Insurance Programs for Cyber Coverage

3 FCC Advisory Committee Releases Cybersecurity Recommendations Based on NIST Framework

5 FTC Authority Questioned During Oral Argument in *FTC v. Wyndham* Case

7 Ten Million Dollar Settlement in Target Consumer Data Breach Lawsuit Provides Insight Into Scope of Damages

7 FTC and Dutch Data Protection Authority Agree to Cooperate on Privacy Enforcement

8 State Action: Connecticut Attorney General Establishes Dedicated Privacy and Data Security Department

8 NIST Releases Draft Framework for 'Internet of Things' Devices

Dismissal in P.F. Chang's Data Breach Case Shows Challenge Plaintiffs Face in Such Actions

A Washington district court dismissed a plaintiff's complaint in the P.F. Chang's data breach case, highlighting the difficulty that plaintiffs have in establishing negligence and other causes of action in these matters.

A recent decision by a district court in Washington state dismissing the plaintiff's action in *Lovell v. P.F. Chang's China Bistro, Inc*. highlights the difficulty plaintiffs have had in sustaining an action in many data breach cases. The decision also highlights that the number of data breaches that have occurred is starting to make courts increasingly circumspect of specific damages claimed by customers.

The Lovell case stemmed out of a data breach that P.F. Chang's suffered between September 2013 and June 2014 in which credit card information, including that of the plaintiff, was stolen. Lovell alleged that he was harmed in three ways: (1) he paid too much for P.F. Chang's food because he would have paid less for the food or not purchased it at all had he known about the restaurant's security shortcomings, (2) he must take "long, costly, and frustrating" steps to protect himself from unauthorized charges, including replacing his existing credit cards and joining credit fraud watch lists, and (3) he may be subjected to harassment or stalking as a result of the security breach.

The court dismissed each of Lovell's causes of action as set forth below:

Negligence. The court found that Lovell could not recover on his overpayment theory since he had failed to explain how P.F. Chang's alleged negligence diminished the value of the food he ate or caused him to frequent the restaurant. The court also held that the mere danger of future harm (*i.e.*, the fear of stalking) was insufficient to sustain a claim of negligence. As the court noted, Lovell had not explicitly alleged that he was anxious from the possibility of stalking. Interestingly, the court also held that it would not presume such anxiety in a data breach. It remains to be seen if future defendants pick up on this logic. Similarly, the court found that plaintiff's concerns over costs he might incur in the future did not support a negligence claim.

Breach of Implied Contract. Lovell argued that he had an implied contract with P.F. Chang's to protect his data when he paid by credit card. The court dismissed this claim, finding that any implied contract was to provide food to Lovell, not to protect his data. "Plaintiff provides no evidence from which one could plausibly infer that defendant intended to contractually bind itself to a general standard of reasonable care or any particular cybersecurity standard or protocol by accepting payment via a credit or debit card."

Breach of Fiduciary Duty. Lovell alleged that P.F. Chang's owed him a fiduciary duty when it requested and accepted his confidential financial information as payment. The court noted that Lovell elected on his own to pay by credit card and that there is no fiduciary duty between a restaurant and its patrons. As the court explained in dismissing this allegation, Lovell and P.F. Chang's had "only the most fleeting contact with each other," and there was no evidence that P.F. Chang's made any representations regarding its security protocols to Lovell or otherwise induced him to disclose his credit card information.

Strict Liability. Lovell's strict liability claim was based on a theory that "modern consumers are forced to rely on credit cards for many purchases, that they have no control over how the confidential information is safeguarded, and that vendors 'are best able to distribute the costs of maintaining the security of the data and the consequences of the breach of such security.'" The court found that this allegation did not satisfy the standards of strict liability since: (1) accepting credit cards or storing financial information is not an abnormally dangerous activity, and (2) there were no dangerous products at issue.

Negligent Misrepresentation. Lovell also alleged that P.F. Chang's was aware that its security protocols did not satisfy industry standards but hid this fact from Lovell, and that this information would have been material to his decision to dine at P.F. Chang's. In a decision that once again relied on the prevalence of data breaches, the court held that "recent disclosures of cybersecurity problems (such as those involving Target, Sony, and/or Home Depot) suggest that, while the breaches make headlines, they do not have much effect on consumer activities." Lovell had therefore failed to create a plausible inference that disclosures regarding cybersecurity measures would be material to his decision on whether to dine at P.F. Chang's. The court also noted that Lovell had not "overpaid" for security measures since customers pay the same price regardless of whether they pay by cash or credit card.

Eleventh Circuit Court of Appeals Decision Underscores the Need to Evaluate Insurance Programs for Cyber Coverage

A recent decision by the Eleventh Circuit highlights that traditional insurance policies may not cover a cyberattack. This decision is an important reminder for companies to review their insurance policies to assess the scope of their coverage for cyberattacks.

Insurance coverage for cyber losses continues to garner well-deserved attention from insurers and policyholders alike as companies of all types and sizes determine how best to manage cyber risks. While the specialty cyber insurance market remains in its nascent stages, a recent decision from the U.S. Court of Appeals for the Eleventh Circuit, *Metro Brokers, Inc. v. Transportation Ins. Co.*,[1] illustrates that it is increasingly clear that traditional insurance policies may not provide cyber coverage.

In that case, Metro Brokers, Inc. (Metro), a real estate brokerage firm in Georgia, used its bank's online Automated Clearing House (ACH) system to make payments from Metro accounts. A Metro employee would log into the online banking system with a username and password and then receive an email or text with a randomly generated single-transaction security code needed to further verify the identity of the person creating or authorizing the ACH transfer. On December 10, 2011, hackers logged into the bank's online system using a Metro employee's username and password. Then, using the security codes, the thieves "authorized" over $188,000 in payments from a Metro client escrow account to several other accounts throughout the country. Although the details of the hack were unclear, the thieves likely obtained Metro login credentials through a key logger virus known as "Zeus" that was found on several Metro computers.

Metro filed an insurance claim under its property policy for the more than $154,000 in stolen funds that remained unrecovered. Metro's insurer, Transportation Insurance Company (TIC), denied coverage based on the policy's malicious-code and system-penetration exclusions. Metro responded by filing a two-count complaint against TIC for breach of contract and bad faith. According to

[1] No. 14-12969, 2015 WL 925301 (11th Cir. Mar. 5, 2015).

Metro, the loss was covered by the policy's Fraud and Alteration (F&A) endorsement, which provided that TIC "will pay for loss resulting directly from 'forgery' or alteration of, on, or in any check, draft, promissory note, bill of exchange, or similar written promise, order or direction to pay a sum certain." The policy defined "forgery" as "the signing of the name of another person or organization with intent to deceive."

The court rejected Metro's coverage argument for multiple reasons. The court initially observed that the ACH transfers "did not involve 'a check, draft, promissory note, [or] bill of exchange.'" Nor could the transfers "be characterized as involving a 'written promise, order or direction to pay' that was 'similar' to the three enumerated instruments." In this regard, the court reasoned that both federal and Georgia law treated electronic fund transfers differently from transfers made by check, draft or bill of exchange. Indeed, the court emphasized that "the Electronic Fund Transfer Act defines an 'electronic fund transfer' as 'any transfer of funds, *other than a transaction originated by check, draft, or similar paper instrument*.'"[2] Because the ACH transfers did not fall among and were unlike the instruments listed in the F&A endorsement, the court found that this coverage extension did not encompass the present loss.

Moreover, the court added that the theft did not involve the "'signing of [a] name,' as required by the policy's 'forgery' definition." While the F&A endorsement expressly included forged electronic signatures, the court refused to equate a username, password or the randomly generated security codes with a "'signature' (electronic or otherwise)" within the meaning of the policy. Because Metro failed to establish that its loss was covered under the policy's F&A endorsement, the court affirmed summary judgment in favor of TIC. The court nonetheless also noted that Metro's claim was barred by the policy's malicious-code exclusion, which defined "malicious code" to include, among other things, "computer viruses," such as Zeus, the key logger virus employed by the thieves.

Practice Points

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. As shown by the Eleventh Circuit's decision in *Metro Brokers*, however, policyholders who rely on traditional insurance policies to respond to cyber losses may find themselves trying to fit a square peg into a round hole. This is all the more true given the industrywide uptick in the imposition of broad cyber exclusions on many traditional insurance policies. As one component of any risk management program, companies are best served by proactively evaluating and thoroughly understanding their insurance programs with respect to cyber risks before any such losses materialize.

[2] Quoting 15 U.S.C. § 1693a(7). The court also noted that Georgia's Uniform Commercial Code on fund transfers expressly does not apply to electronic fund transfers governed by the federal Electronic Fund Transfer Act.

FCC Advisory Committee Releases Cybersecurity Recommendations Based on NIST Framework

The FCC continues to take a more proactive role in cybersecurity, in this case by releasing a report on Cybersecurity Risk Management and Best Practices. The report provides important guidance on how companies regulated by the FCC should view cybersecurity preparedness.

On March 18, 2015, the Communications Security, Reliability and Interoperability Council (CSRIC), a federal advisory committee chartered by the Federal Communications Commission (FCC), released its report on Cybersecurity Risk Management and Best Practices (Cybersecurity Report). CSRIC includes representatives from large and small communications providers, academia, government and nonprofit organizations, and is chartered for two-year periods to provide advice to the FCC on security-related practices. The FCC renewed the CSRIC charter for the fourth time in March 2013, and CSRIC IV was tasked, in part, with developing voluntary mechanisms to provide assurance to the FCC and the public that communications providers are appropriately managing cybersecurity risks across their enterprises. The Cybersecurity Report was the culmination of a nearly two-year review process by Working Group 4 of CSRIC IV aimed at addressing the FCC's cybersecurity concerns.

In the wake of President Barack Obama's executive order requesting development of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (see our December 2014 *Privacy & Cybersecurity Update*), the FCC directed CSRIC to develop recommendations for communications providers based on the NIST framework. The FCC asked that

those recommendations: (1) be specifically tailored to individual companies' needs and risks, (2) be based on meaningful indicators that cybersecurity risk was appropriately managed, and (3) permit meaningful assessments, both by companies and by outside parties such as the FCC.

The Cybersecurity Report

The Cybersecurity Report divides the U.S. communications sector into five segments: broadcast, cable, satellite, wireless and wireline. After considering a number of factors, including sector dependencies and risks, the NIST framework and its guidance, and the availability of measurements, CSRIC arrived at three general recommendations for all segments:

- *Hold FCC-initiated voluntary confidential meetings with specific companies to allow them to inform the FCC about their risk management practices*. These meetings would provide a forum for companies to present information about cyber threats and the measures they take to counteract them in a protected setting. Confidentiality of information would be assured under the Protected Critical Infrastructure Information program administered by the Department of Homeland Security (DHS).
- *Add components in the Communications Sector Annual Report (SAR) discussing cybersecurity risk management for each of the segments described above*. The SAR, developed by the communications sector in response to DHS critical infrastructure security concerns, would now specifically address cybersecurity risks.
- *Encourage industry participation in the DHS Critical Infrastructure Cyber Community program*. The goal of the DHS program is to develop additional reference materials and expertise on sector-specific cybersecurity threats and to ensure that they are disseminated to companies more broadly to increase their cybersecurity awareness.

In addition, the Cybersecurity Report offers guidance on implementing the NIST framework to members of the communications industry on a segment-by-segment basis. Each segment's recommendations were separately drafted by a different Working Group 4 subgroup, and each provides its recommendations in a separate section of the report targeted at the relevant companies. Broadly speaking, a number of the segment-specific sections recapitulate NIST's recommended sub-categories of activity and divide them into high, medium and low priorities, as appropriate to those segments. For example, across several segments, inventorying physical devices and systems is recognized as a high-priority activity, whereas properly categorizing incidents is generally considered to be a lower priority. The segment-specific sections also provide use cases for industry segment personnel interested in leveraging the NIST framework.

Finally, the Cybersecurity Report also includes a number of additional reports from Working Group 4 subgroups aimed at addressing nonsegment-specific cybersecurity concerns, including developing measurable cybersecurity indicators and understanding sector-specific threats. The metrics section is of particular interest here, as it is intended to advance a framework for the government and industry to work together to develop quantifiable measurements that companies may then use to report to the government on the industry's progress in improving its cybersecurity.

Takeaways

While certain federal agencies have issued suggestions, publicly or privately, on how critical infrastructure enterprises should use the NIST framework, the Cybersecurity Report instead provides an industry perspective on NIST framework implementation. Working Group 4 reiterates that the application of the NIST framework must remain flexible and that companies' ability to self-tailor the framework to fit their individual security needs is one of the key benefits it provides. In particular, it pre-emptively pushes back on any codification of the NIST Framework: The very first "macro-level" conclusion is that "[n]o new regulations are needed or warranted to address conformity to the NIST Framework."

Whether the industry and private-sector representatives that authored the Cybersecurity Report will be successful in maintaining the open, collaboration-driven cybersecurity regulatory regime the report contemplates remains to be seen. In a speech last June, FCC Chairman Tom Wheeler suggested that the FCC would use the NIST Cybersecurity Framework as a springboard to develop a cybersecurity risk management tool specific to the communications sector. Chairman Wheeler implied that once metrics were developed, the tool would serve as a means to assess companies based on the NIST framework. Based on the Cybersecurity Report, FCC efforts to develop quantifiable measurements still appear to be in the early stages, and their effectiveness remains undetermined. Any perceived FCC assessment successes may serve as a template for other independent regulatory agencies interested in applying the NIST framework to other sectors.

Next Steps

In a relatively unusual step in responding to a CSRIC report, the FCC Public Safety and Homeland Security Bureau (Bureau)

has issued a public notice seeking comment from communications providers and the public on the Cybersecurity Report, with comments and replies to be posted in a public docket. Once the FCC develops a record on appropriate cybersecurity practices, industry representatives will want to carefully follow its next steps.

Comments on the Cybersecurity Report will be due on May 29, and replies to comments on June 26. The Bureau has asked for general comment and also for commenters' responses to a number of specific questions, including the following:

1. In what ways are the CSRIC IV recommendations sufficient to meet the FCC's goal of reducing cybersecurity risk to critical infrastructure, enterprises, and consumers? In what ways, if any, might these recommendations be improved, augmented, or made more specific?
2. These recommendations include the following voluntary mechanisms to provide assurances to provide evidence of the communications sector's commitment to enhance cybersecurity risk management capabilities. [The FCC] seek[s] comment on each as indicated:
   - FCC-convened confidential company-specific meetings or other communications formats. How should the Commission prepare for and conduct these meetings to ensure that they result in information that is useful for assessing the state of cybersecurity risk management among communications providers?
   - A new component of the Communications Sector Annual Report that focuses on segment-specific cybersecurity risk management. What measures should this Annual Report include to provide appropriate levels of visibility about the state of cybersecurity risk management over time?
   - Active and dedicated participation in DHS' Critical Infrastructure Cyber Community C3 Voluntary Program. How should the Commission coordinate with DHS in the context of the C3 Voluntary Program to help small and mid-sized communications providers make use of the CSRIC recommendations?
3. What barriers, if any, would inhibit industry's effective application of the voluntary mechanisms discussed throughout the report? What differences exist based on factors such as size? How might these barriers be mitigated?

Parties interested in commenting on the suggestions made in the Cybersecurity Report, or on the responses of others, once filed, should reach out to their Skadden points of contact listed at the end of this Update.

FTC Authority Questioned During Oral Argument in *FTC v. Wyndham* Case

In the latest round of the ongoing battle between Wyndham and the FTC regarding the FTC's jurisdiction over cybersecurity claims, a Third Circuit panel asked a series of tough questions regarding the FTC's position.

On March 3, 2015, a three-judge panel for the U.S. Court of Appeals for the Third Circuit heard arguments in *Federal Trade Commission v. Wyndham Worldwide Corp*., the key case focused on whether the FTC has the authority to pursue actions against businesses for unfair trade practices based on their allegedly insufficient data security practices. Although the FTC has prevailed in each stage of this litigation, questions posed by the Third Circuit judges suggest that they may be less willing to read such broad authority into Section 5 of the FTC Act as previous courts have done.

Background

The FTC/Wyndham action began in 2012 when the FTC issued a complaint against Wyndham related to three separate data breach incidents that occurred between 2008 and 2009. Rather than settle with the FTC, as 50 companies had previously done when faced with a similar complaint, Wyndham moved to dismiss the claim. Wyndham based its motion on three main arguments: (1) the unfairness standard under the FTC Act did not encompass unreasonable data security measures, (2) the FTC had not given businesses like Wyndham notice that unreasonable data security measures were unfair, and (3) the FTC's complaint did not sufficiently allege consumer injury as required by the FTC Act. The New Jersey District Court rejected all of these arguments and denied Wyndham's motion to dismiss the complaint. Wyndham filed an interlocutory appeal, and in August 2014, the Third Circuit agreed to hear the case.

Although both Wyndham's and the FTC's primary legal arguments are now quite familiar to observers (between the motion to dismiss briefing in the district court and the appellate briefing to the Third Circuit), the oral arguments provided important insight into what factors each side finds most important in determining this issue. Further, the comments and questions from the panel throughout the argument give an interesting glimpse into how the court may ultimately decide the case.

Key Moments From Wyndham's Argument

In its argument, Wyndham highlighted the FTC's failure to identify the actual cause of the breaches in 2008 and 2009, or how Wyndham's cybersecurity deficiencies were a likely cause of the breach. According to Wyndham, this failure supported two of its primary legal arguments: (1) the FTC had not adequately pled that Wyndham's cybersecurity practices caused consumer harm, and (2) the FTC could only allege that Wyndham acted negligently, and no federal court had interpreted negligence as sufficient for establishing an unfair trade practice (at least according to Wyndham). Wyndham argued that if the court sided in the FTC's favor, the regime would ultimately become one of strict liability where any data security breach would be a per se unfair trade practice.

Wyndham also highlighted that the FTC could only make general allegations against Wyndham and did not move for an injunction because it could not satisfy Third Circuit case law requiring a detailed order for injunctions. Wyndham also argued that this lack of specificity meant the FTC failed to prove "substantial consumer harm," as required under the FTC Act. This point was also underscored by Wyndham's argument that the FTC still has failed to find a single consumer who experienced any out-of-pocket expenses as a result of the breach.

While Wyndham focused on these factual deficiencies, arguing that the FTC failed to meet its pleading burden, the court noted that such issues may be more properly resolved at a later stage in the case. Nonetheless, if the court does decide that the FTC has met its pleading burden at this stage, it is likely that Wyndham's oral argument here is a preview into arguments we can expect to see being made on a motion for summary judgment or potentially at trial.

Key Moments From the FTC's Argument

Although the FTC's presentation remained close to its previous arguments on the relevant issues, it made certain important admissions that revealed the FTC's position on key aspects of the case. First, the FTC argued that in its view, the term "unfair" is limited only by the three factors Congress introduced into the FTC Act in Section 5(n); namely, the action is: (1) likely to cause substantial consumer harm that (2) the consumer cannot reasonably avoid, and (3) is not outweighed by the benefits to the consumers or the businesses competition. This position reveals the amount of discretion the FTC believes it has in defining what an "unfair" cybersecurity practice is under its enabling act. In essence, the FTC argued that the term "unfair" is itself an "unbounded concept" that could be extended to fit any conduct, subject to the foregoing three requirements.

The FTC also maintained that its decisions and consent decrees were formal agency determinations with precedential value. This position highlights the FTC's view of its own authority to determine and make policy in this area. In response to questioning from the court, the FTC stated that it expected "careful general counsels" to read and be aware of these FTC decisions and consent decrees, and that those alone were enough to provide businesses with notice of what practices the FTC deemed to be unfair.

Questions From the Court

To most observers, the most interesting aspect of the oral argument was the questioning directed toward the FTC. Early on into the FTC's argument, the judges began pressing whether the FTC was asking federal courts to declare, for the first time, that unreasonable cybersecurity practices were "unfair." The FTC ultimately conceded that if the court determined that the FTC had not yet declared those practices unfair, it was indeed asking the court to do so.

The panel also asked the FTC several questions about the legislative history of the FTC Act, particularly the provision that allows the FTC to seek injunctions in federal court. The court suggested that such authority was only intended to apply in ordinary fraud cases where the agency determines that there is no need for a detailed administrative consideration, and that this was clearly not such a case. In other words, the panel's questions indicated that it could interpret the FTC Act as preventing the agency from bringing cases of first impression, like this one, into federal court without first going through the cumbersome administrative procedure of notice and rulemaking.

Finally, the court seemed skeptical regarding the FTC's position that previous consent decrees or decisions by the FTC effectively put companies on notice of what was "unfair," and it even directly asked the FTC whether a company could violate a statute by engaging in conduct the FTC had yet to declare unfair. At another point, one judge stated that if he were a company's general counsel, he would not think to look to FTC consent decrees when advising his clients.

In general, the questioning throughout the argument suggested that the panel was much more interested in pinning down the FTC on its exact position than it was for Wyndham. The FTC was faced with more "tough" questions and received much more push-back on its arguments. While this could be interpreted as skepticism from the Third Circuit, it remains to be seen whether the judges were leaning in favor of the FTC and were merely interested in understanding the boundaries of the FTC's position.

Conclusion

Regardless of the ultimate outcome of the case, the Third Circuit's decision here will likely change how businesses and the FTC interact moving forward. In addition to the direct implications for cybersecurity practices, a determination in this case is likely to define the FTC's authority and discretion in bringing unfair trade practices cases in undefined areas for the near future. We will continue to watch this case and provide updates as information becomes available.

Ten Million Dollar Settlement in Target Consumer Data Breach Lawsuit Provides Insight Into Scope of Damages

The Target class action lawsuits by consumers ended with a settlement agreement that highlights how difficult it is for consumers to establish damages in data breach attacks.

Background

As most know, in December 2013, Target announced that over a period of more than three weeks during the holiday shopping season, computer hackers had stolen credit and debit card information for approximately 110 million Target customers by installing malware on the store's computer servers. Lawsuits were filed on the heels of the announcement and consolidated into a multidistrict litigation in Minnesota. In December 2014, the U.S. District Court for the District of Minnesota granted in part and denied in part Target's motion to dismiss. (See our December 2014 *Privacy & Cybersecurity Update*.) On March 18, 2015, the parties unveiled the terms of a settlement that the court preliminarily approved the next day. The scope of the settlement provides important insight into the scope of damages in many large-scale and well-publicized data breaches.

Terms of the Settlement

Under the terms of the settlement, Target will pay $10 million into an interest-bearing, nonreversionary compensation fund. Consumers who can document their losses (such as unauthorized, unreimbursed charges on their accounts, card replacement fees and late fees that were the result of the fraudulent charges) will be eligible for recovery up to $10,000 each, including time spent addressing unauthorized charges on their accounts for $10 an hour up to two hours. Class members who cannot document their losses will be entitled to an equal amount of the remainder of the settlement fund, after service payments to the lead plaintiffs.

Target also agreed to appoint a high-level executive as chief information security officer, to maintain a written information security program, and create a process to monitor information security events and respond to any events determined to present a threat.

Practice Points

The $10 million figure is surely modest relative to the magnitude and scope of the data breach, as well as the publicity it received. However, the number is in line with other data security breach settlements given plaintiffs' difficulty proving damages in these types of cases. For example, Sony Corporation agreed to pay $15 million to resolve claims over a breach that led to the theft of names, addresses and possibly credit card data belonging to 60 million user accounts, while LinkedIn Corp. paid $1.25 million to settle a suit over the exposure of 6.5 million passwords and AvMed Inc. agreed to $3 million to settle claims involving 1.2 million customers whose personal information was compromised in a laptop theft. Similarly, TD Ameritrade agreed to settle a class action data breach suit over claims that third parties improperly accessed their customers' email addresses, for $2.5 million to $6.5 million, depending on the number of submitted claims.

In most of these cases, plaintiffs are hard-pressed to identify fraudulent charges for which they were not reimbursed or actual cases of identity theft.

Despite these settlement figures, companies should expect the plaintiffs' bar to continue its current trend of filing consumer class actions following the data breaches because such cases are driven largely by attorneys' fees. The Target settlement agreement permits plaintiffs' attorneys to recover as much as $6.75 million. Thus, companies should continue to conduct cybersecurity audits of their processes and governance, and formulate rapid response plans to swiftly address any signs of a data breach.

FTC and Dutch Data Protection Authority Agree to Cooperate on Privacy Enforcement

An information-sharing agreement between the FTC and Dutch regulators provides another example of the increasing international cooperation between privacy enforcement bodies.

The FTC and the Dutch Data Protection Authority signed a memorandum of understanding (MOU) on March 9, 2015, that provides for information sharing between the United States and the Netherlands in order to protect consumer privacy in both countries.

Pursuant to the MOU, the enforcement agencies agree to share information in order to investigate and enforce cross-border privacy violations. In addition, the parties will work together on training and research related to privacy.

The MOU, which is not legally binding, sets forth circumstances under which data may be shared, along with procedures that the nations will follow in order to ensure that the information shared remains secure and confidential (*e.g.*, transferring the information in a secure format). Either party may decline requests for assistance or limit its cooperation at its own discretion, whether because motivated by law or other "important interests."

The MOU, which is similar to agreements currently in place with authorities in Ireland and the United Kingdom, demonstrates the increased willingness of the FTC to cooperate with regulators from other countries on privacy-related matters. In a press release announcing the agreement, the FTC emphasized the importance of increased international cooperation on privacy issues, particularly in light of the ease with which personal information can travel across borders.

State Action: Connecticut Attorney General Establishes Dedicated Privacy and Data Security Department

Connecticut has created a dedicated Privacy and Data Security Department, highlighting the expanding role of states in the area of privacy and cybersecurity.

Connecticut has joined the ranks of states stepping in to fill gaps in federal law in the area of data privacy and security. On March 11, 2015, Connecticut Attorney General George Jepsen announced his office is establishing a Privacy and Data Security Department (Department). The newly established department will expand upon the responsibilities of the Privacy Task Force formed by AG Jepsen in 2011 and will continue as a standalone department within the Connecticut Office of the Attorney General. AG Jepsen appointed Assistant Attorney General Matthew Fitzsimmons as head of the department, which will be staffed by dedicated attorneys, a contract technical consultant and other experts in fields such as health care and finance. The department will oversee investigations involving consumer privacy and data security as well as educate the public on the issue.

Connecticut is not the only state looking to assert itself as a leader in the area of data privacy and security. New York Attorney General Eric T. Schneiderman proposed the Data Security Act (see our January 2015 *Privacy & Cybersecurity Update*) earlier this year in an effort to set data security standards for entities that own, maintain or possess private information. Florida, Illinois, Massachusetts, Connecticut and New York, along with attorney general offices from many other states, investigated Target Corp., Neiman Marcus Group LTD and Michaels Stores Inc. after these companies experienced data breaches. California joined with Iowa, Connecticut, Illinois, Massachusetts and New York to investigate the breach at Home Depot Inc.

With states becoming more active in investigating data breaches as well as passing and enforcing data security legislation, the area may become covered by a patchwork of potentially conflicting laws. As with data breach notification laws, such a patchwork arrangement could create compliance difficulties for businesses that operate in multiple states.

NIST Releases Draft Framework for 'Internet of Things' Devices

A few weeks ago, the FTC weighed in on the 'Internet of Things' by issuing a report. NIST has now issued its own report, focusing primarily on technical aspects but with some important views on privacy as well.

On March 3, 2015, the National Institute for Standards and Technology (NIST), through its Cyber-Physical Systems Public Working Group, released a draft framework for "cyber-physical systems," or CPS. Simply put, cyber-physical systems are physical systems that combine real-time sensing and some type of response driven by that real-time sensing. Though CPS comprises a broader universe of systems, "Internet of Things" devices such as activity tracking wristbands and smart, Internet-connected thermostats are examples of CPS. The goal of the framework is to establish a common, integrated set of standards that developers will use when creating CPS devices, so that devices from different developers and addressing different needs will be able to interoperate in a global CPS network.

Cybersecurity and Privacy Themes

Though largely focused on technical matters, a pervasive theme throughout the framework is the need to address cybersecurity and

privacy issues presented by CPS. Each of the various workstreams that contributed to the draft framework recognized the need to address cybersecurity and privacy matters in their technical and other recommendations. In studying these issues, the working group has recognized that, while the work done to date on cybersecurity and privacy matters in the traditional information technology space can be helpful for some of these issues, CPS presents different challenges that require further study. The working group established a special subgroup devoted to these issues, and that subgroup has been tasked with creating a set of tailored cybersecurity requirements and a privacy framework for CPS.

The framework describes some of the specific cybersecurity threats and considerations that CPS must take into account, including:

- The physical nature of the device and the opportunities it provides for an attack.
- The potential for compromised devices to be used to trigger real-world consequences, such as deactivating equipment that should be active or vice versa.
- The fact that many CPS devices are "always on" makes issuing security patches over time impractical.
- CPS devices will often be faced with physical constraints, including the amount of memory available for software not devoted to its core functionality.
- The complex interactions between different CPS devices may provide opportunities for an attack that individual developers did not consider when designing their specific devices.
- Some CPS devices will have extraordinarily long lifespans, which may continue beyond when the manufacturer stops supporting the device.
- Devices may collect data that, in isolation, does not present privacy issues, but when collected and examined in the aggregate, or when aggregated with other data collected by other devices, poses significant privacy concerns of which neither the user nor the developer is aware.

The draft framework does not propose specific solutions to all of these issues, but rather, focuses on the fact that developers need to take these risks into account and suggests various approaches to addressing them. For example, on the issue of data collection and use, the framework suggests that CPS devices collect only the minimum data that they need and take care to ensure data is purged securely.

Security and Privacy a Key Issue Across Policy and Technical Organizations

The draft framework's focus on cybersecurity and privacy matters highlights the importance of these issues and the attention being given to them by policy and technical organizations. As we have discussed in prior editions of this newsletter, the Federal Trade Commission has made privacy and cybersecurity policy and enforcement — especially with respect to the "Internet of Things" — a key priority. The FTC has taken action against a number of companies over these types of issues and has issued various reports and other guidance on cybersecurity and privacy practices, including its January 2015 detailed report and set of recommendations relating to the "Internet of Things."

Next Steps

The draft framework is incomplete, and some sections do not even reflect consensus among working group participants, so plenty of work remains. Among the next steps in the short term is a set of in-person meetings on April 7 and 8 in Gaithersburg, Maryland. Ultimately, the working group aims to release a final framework sometime in 2016.

Additional 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