Skadden

Privacy & Cybersecurity Update

FCC Approves New Rules for Broadband Privacy

The FCC has approved new rules addressing how internet service providers must protect broadband users' privacy.

The Federal Communications Commission (FCC) voted on October 27, 2016 to approve a proposal for rules to safeguard the privacy of broadband users. These rules require internet service providers (ISPs) to obtain explicit "opt-in" consent before collecting a wide range of what is deemed "sensitive information," provide information to consumers about the data the ISP collects and allow consumers to opt out of most ISP collection of information.

Rules Requirements

The FCC has not yet published the final order describing the rules, but considering the commission's initial notice of proposed rulemaking, FCC Chairman Tom Wheeler's fact sheet outlining the ultimate proposed order in advance of the October meeting, and other FCC blog posts and related reporting, the broad outlines of the new rules are reasonably clear. Based on what has been made available to date, the new rules will require ISPs to:

- notify consumers about the types of information they are collecting. ISPs must provide this information when a customer signs up for service, and then update their customers if the privacy policy changes in significant ways. This information also must always be available on an ISP's website or mobile app. The commission also has directed its Consumer Advisory Committee (CAC) to develop a standardized privacy notice format that, although voluntary, would provide a "safe harbor" for ISPs that choose to adopt it;
- specify how and for what purposes that information can be used and shared;
- identify the types of entities with which the ISP shares the information;
- most significantly, ISPs must offer affirmative opt-in consent for the collection and use of sensitive data. Opt-in consent refers to a paradigm where the default is that a consumer's data may not be used unless the consumer checks a box, or otherwise

manifests his or her explicit consent that his or her data may be used. While "sensitive" data includes categories that are traditionally considered sensitive, such as health and financial information and information concerning children, it also includes a number of categories that are the lynchpin of targeted advertising and a key revenue source for ISPs, including web browsing and app usage history. Many ISPs have expressed concern that obtaining opt-in consent for such data will hamper their ability to sell targeted advertising, resulting in higher prices for consumers. However, ISPs are prohibited from refusing to serve customers who do not consent to the use and sharing of their information for commercial purposes;

- take reasonable measures to protect consumer data from breaches and other vulnerabilities;
- notify consumers as soon as possible, but no later than 30 days, after reasonable determination of a breach, and notify the FCC, the FBI and the Secret Service of breaches affecting 5,000 or more customers no later than seven business days after reasonable determination of the breach. The FCC must be notified at the same time as customers if the breach affects fewer than 5,000 customers;
- disclose any plans that relate service price to privacy protections;
- allow consumers to "opt out" of using other personal data except as necessary for the provision of service, billing and certain other purposes; and
- adequately "de-identify" consumer data before sharing it as non-personal data.

Timing

The final effective dates of the rules will be announced with publication of the final order in the Federal Register. Based on information available to date, the various aspects of the order are to go into effect according to the following timeline:

- Data security requirements: 90 days after the order is published;
- Data breach notification requirements: six months after the order is published; and
- Notice and consent requirements: 12 months after the order is published, though small providers are expected to have an additional 12 months to come into compliance.

Rationale

Chairman Wheeler published a blog post on October 6, 2016, on the FCC's website[1] outlining his reasoning for proposing the new regulations. He emphasized that, prior to the passage of the new rules, there had been no regulations in place outlining how ISPs could use and share customers' personal information even though parallel rules had been in place for decades requiring telephone companies to protect the information associated with phone calls and text messages.

"Our goal throughout the process has been straightforward: to give consumers the tools they need to make informed decisions about how ISPs use and share their data, and the confidence that ISPs are taking steps to keep that data secure, all while providing ISPs the flexibility they need to continue to innovate," Wheeler wrote in the post.

Wheeler also wrote that the new rules are based on extensive feedback the FCC has received from consumer and public interest groups, fixed and mobile ISPs, advertisers, app and software developers, academics, other government actors including the FTC, and individual consumers.

FCC Jurisdiction and Scope of Rules

Broadband service providers have only recently become subject to FCC jurisdiction. Their status changed when the FCC reclassified broadband as a utility last year as part of new net neutrality regulations, a decision recently upheld by the U.S. Court of Appeals for the District of Columbia Circuit.[2]

The new rules apply to information collected from consumers using broadband services, such as residential or mobile connections. The rules do not, however, apply to the privacy practices of websites or apps, over which the FTC has authority (even if the website or app is owned by a broadband provider).

Retreat From Initial Proposal

The new scaled-back rules were proposed after the FCC received strong negative feedback on an initial proposal by Chairman Wheeler. ISPs such as Verizon, AT&T and Comcast criticized the initial proposal for subjecting them to more stringent requirements than those imposed by the FTC, which apply to major web services such as Facebook, Twitter and Google. In particular, the ISPs objected to broad requirements under the initial proposal that required them to obtain affirmative consent for using nearly all consumer data. The more limited consent and opt-out obligations in the new rules reflect a concession to these industry concerns.

Next Steps

The final order from the FCC describing the rules are expected to be released by the FCC in the coming days. Once the rules have passed through internal executive branch review, they will

[1] Available here.

[2] Available here.

be published in the Federal Register, and unless challenged in court and subject to a stay, the rules can be expected to take effect soon thereafter based on the timeline above. We will be monitoring for publication by the FCC, and will provide updates as they develop.

Return to Table of Contents

FTC Releases Playbook for Data Breach Response and Notification

The Federal Trade Commission has issued guidance for how companies should respond to data breaches. Companies should expect that the FTC and plaintiffs' attorneys will use this guidance as a benchmark to determine if companies have responded appropriately to a data breach.

On October 25, 2016, the Federal Trade Commission (FTC) released a guidebook, together with a blog post and accompanying video, on how companies should respond to data breaches, including how they should notify affected consumers. The FTC also attached a model letter to be sent to individuals informing them of the data breach, which we expect will become the form that most companies under the jurisdiction of the FTC adopt.

Although the guidelines are nonbinding, companies should expect that the FTC will use them as a benchmark when determining if a company's response to a data breach was so inadequate that it constituted unfair business practices under the FTC Act. Further, other agencies may use this guidance as a foundation for crafting their own data breach response guidelines. Finally, companies can expect that plaintiffs' attorneys will highlight any disconnect between the guidelines and the company's actions in responding to a data breach while trying to establish that the company acted negligently.

Response to Data Breach

In its guidance, the FTC addresses the key steps companies should take in response to a data breach, with specific recommendations for action at each step, beginning with the steps taken to secure operations and ending with providing required notices of the breach.

Secure Operations

Companies that suffer a data breach should move quickly to secure their operations. In order to achieve this, the FTC suggests companies should:

- secure systems and fix vulnerabilities that caused the breach;
- assemble a team of experts to conduct the breach response, including a forensics team and external legal counsel;
- secure physical areas potentially related to the breach, including by locking them and changing access codes;
- stop additional data loss by taking affected equipment offline immediately and updating credentials and passwords;
- remove improperly posted information from the web, both on sites the company controls and by making requests of the applicable third parties from third-party sites; and
- interview people who discovered the breach to gather information on the breach.

In taking these steps, the FTC advises not to turn off affected machines or otherwise destroy forensic evidence.

Fix Vulnerabilities

After securing systems against additional losses, companies should fix vulnerabilities that caused the breach. As part of this process, the FTC suggests companies should:

- if a service provider was involved, review its access privileges to company information and ensure it is taking steps to prevent further breaches;
- examine whether existing efforts to segment internal networks to contain damage have been effective;
- work with forensics experts to determine how the breach occurred and whether defensive measures such as encryption were enabled; and
- have a comprehensive communication plan for providing information to employees, customers, business partners and investors of the incident, but do not publicly share information that could put consumers at risk.

Notify Appropriate Parties

Companies will need to notify law enforcement as well as other affected businesses and consumers. In order to provide proper notifications, companies should:

- determine their legal requirements involving notice, including state data breach notification requirements;
- notify law enforcement, starting with the local police and then the FBI or Secret Service if local police are not familiar with these types of investigations;
- check whether health information was involved and Health Insurance Portability and Accountability Act (HIPAA) notification requirements are implicated;

- if account information was affected, notify affected businesses such as credit card companies and banks so that they can monitor for fraudulent activity;
- if information stored on behalf of other companies was affected, notify the other companies;
- if names and Social Security numbers were affected, contact the major credit bureaus; and
- notify consumers so they can take steps to reduce the chance their information will be misused.

Recommendations and Form of Letter for Notice to Individuals

The FTC's guidance includes a number of specific suggestions for how to manage and what to say in notifications to individuals affected by a data breach. In particular, the FTC suggests providing at least one year of free credit monitoring or other support if financial information or Social Security numbers were affected.

The FTC also attached a model letter to be sent to individuals, which calls on companies to provide information on:

- how the breach occurred;
- what information was taken;
- how thieves used the information (if known);
- what steps the company has taken to remedy the situation;
- what actions the company is taking to protect the individual, such as free credit monitoring; and
- how to reach relevant contacts in the company's organization for more information.

The FTC also recommends telling consumers how to contact the FTC and local law enforcement about the misuse of their information.

Role in FTC Enforcement and Potential Litigation

The FTC guidance goes beyond existing state and federal requirements relating to data breach notification by describing the full process for responding to a breach. The FTC has been very active in policing cybersecurity matters on the basis of its general authority to police unfair business practices. Given the absence of specific standards, the FTC has looked to industry practices and its own guidance to determine whether companies have violated the law. It is likely that the commission will look to its data breach response guidance in evaluating companies in the future. In addition, plaintiffs' attorneys are likely to look to the FTC's guidance as a benchmark for evaluating whether companies have responded appropriately.

Return to Table of Contents

Grocer Not Entitled to Coverage Under Traditional Insurance Policy for Liabilities Stemming from Computer Hacking Incident

An Alabama federal court recently ruled in favor of an insurer in a coverage battle with its insured, a grocery store operator, holding that the insured was not entitled to coverage under its business insurance policy for litigation commenced against it stemming from a cyberattack on its computer systems that compromised its customers' confidential data.

On October 25, 2016, the U.S. District Court for the Northern District of Alabama ruled in *Camp's Grocery, Inc. v. State Farm Fire & Cas. Co.* that a grocery store operator could not look to its business insurance policy for third-party claims arising out of an alleged computer hacking incident that compromised its customers' confidential data.[3] That ruling adds to the growing number of decisions throughout the country finding that policyholders may not be covered for cyber losses under "traditional," noncyber insurance policies due to electronic data-related exclusions and serves as a reminder to policyholders to evaluate the adequacy of their coverage for cyber losses.

Background and Language of Policy

In the case, three credit unions sued Camp's Grocery, Inc., an Alabama-based Piggly Wiggly, LLC franchisee, alleging that the grocer's failure to adequately safeguard its computer systems led to a computer hacking incident. The credit unions allege that the computer hack compromised confidential credit, debit and check card information of its customers, which in turn caused the credit unions to suffer losses on their cardholder accounts. These losses included the reissuance of cards, reimbursement of customers for fraud losses and administrative expenses associated with investigating, correcting and preventing fraud.

At the time of the hacking incident, Camp's Grocery was insured by State Farm Fire & Casualty Company pursuant to a business insurance package policy. The coverage provided by the policy included first-party property coverage, third-party liability coverage and inland marine computer property coverage which insured, among other things, "accidental direct loss" to "electronic data" including certain data of Camp's Grocery's customers used in connection with its business operations. Notably, some of the coverages contained limitations on electronic data-related losses: The first-party property coverage expressly excluded "electronic data" from the definition of "covered

[3] No. 4:16-CV-0204-JEO, 2016 WL 6217161 (N.D. Ala. Oct. 25, 2016).

property," while the third-party liability coverage was subject to an electronic data exclusion. Camp's Grocery sought coverage under the policy's third-party liability and inland marine computer property coverages, and insurance litigation ensued.

Court's Decision

In granting summary judgment in favor of State Farm, the court concluded that the policy did not afford coverage to Camp's Grocery for the underlying action. The court rebuffed Camp's Grocery's argument that it was entitled to coverage based on the inland marine computer property coverage for the credit unions' claims against it. The court instead found that those provisions "unambiguously afforded first-party coverage only," citing the fact that "there [was] no language ... whereby State Farm promise[d] to 'defend' or 'indemnify' the insured, whether in regard to claims involving computer equipment, electronic data, or anything else, for that matter."

The court was equally unpersuaded by Camp's Grocery's argument that it was covered under the policy's business liability coverage because the credit union's alleged losses for replacement of customer debit and credit cards constituted covered "property damage." While acknowledging that the business liability coverage insured Camp's Grocery for third-party property damage claims, the court nevertheless found Camp's Grocery's argument to be flawed because the credit unions did not allege that the grocer's actions resulted in physical damage to their customers' credit and debit cards. Rather, the court found, the underlying action alleged the compromise of "intangible electronic data contained on the cards," which did not constitute "property damage" under the policy and, in any event, fell within the policy's electronic data exclusion.

Key Takeaway

As the court's decision in *Camp's Grocery* illustrates, traditional insurance policies, including seemingly comprehensive package policies, may not respond to cyber losses. With an increasing number of insurers expressly limiting coverage for cyber incidents under traditional policies through the inclusion of electronic data exclusions and the like, businesses of all types would be well advised to consider purchasing coverage specifically geared to cyber losses, to the extent not already in place, to avoid being left without coverage in the event of a cyber incident.

Return to Table of Contents

National Highway Traffic Safety Administration Issues Voluntary Guidance for Automotive Cybersecurity

The NHTSA has released nonbinding guidance on cybersecurity practices for the automotive industry.

On October 24, 2016, the National Highway Traffic Safety Administration (NHTSA) issued "Cybersecurity Best Practices for Modern Vehicles" (NHTSA Guidance), a 21-page document offering voluntary guidance for improving motor vehicle cybersecurity. The document arrives at a time of increased concerns about automotive cybersecurity for the industry and consumers, and may provide a future benchmark against which auto companies and their suppliers are measured.[4]

Background

In July 2015, two researchers successfully hacked and took over control of a Jeep Cherokee using a laptop located miles away. As a result of the hack, the NHTSA recalled nearly 1.5 million vehicles, marking the first time the agency used its enforcement authority due to a cybersecurity vulnerability. Since July 2015, private-sector and governmental stakeholders have created a range of security initiatives for the automotive industry. In the private sector, three key initiatives were introduced in 2016 alone. These include the SAE Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, the Automotive Sharing and Analysis Center (Auto ISAC), and a cybersecurity best practices framework developed by two automotive trade associations.

Purpose of NHTSA Guidance

The NHTSA's focus on cybersecurity reflects a priority of the U.S. Department of Transportation to protect consumers from malicious cyberattacks and unauthorized access. The NHTSA Guidance is based on public feedback received by the NHTSA, as well as the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework). According to the NHTSA, the guidance was conceived as a "resource to supplement existing voluntary cybersecurity standards," and has a dual purpose: First,

[4] The NHTSA's guidance is available here.

to provide best practices to help protect against breaches and other security failures that can put motor vehicle safety at risk, and second, to provide a solid foundation for developing a risk-based approach to prevent cybersecurity issues in the automotive industry.

General Cybersecurity Guidance

The NHTSA Guidance offers two general cybersecurity principles:

Layered Approach

According to the NHTSA Guidance, and in accordance with the NIST Framework, the automotive industry should develop a layered approach to vehicle cybersecurity. This approach should:

- be built upon risk-based prioritized identification and protection of safety-critical vehicle control systems and personally identifiable information;
- provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
- design methods and measures to facilitate rapid recovery from incidents when they occur; and
- institutionalize methods for accelerated adoption of lessons learned across the industry through effective information sharing, such as through participation in Auto ISAC.

Information Technology Security Controls

The NHTSA Guidance suggests that the automotive industry review and adapt the standards and controls designed for information technology networks utilized by other industry sectors. These include ISO 27000 series standards and other best practices, such as the Center for Internet Security's "Critical Security Controls for Effective Cyber Defense" (CIS CSC). Moreover, industry leaders should follow the CIS CSC recommendations, which include: performing cybersecurity gap assessment, developing implementation road maps, executing cybersecurity plans, integrating controls into vehicle systems and business operations, and reporting and monitoring progress. through iterative cycles.

Automotive Industry Cybersecurity Guidance

Outside of the two general cybersecurity principles, the NHTSA Guidance describes seven recommendations on subjects ranging from product development to best practices on researching and validating cybersecurity measures. These principles include:

1. Vehicle Development Process With Explicit Cybersecurity Considerations

The safety of vehicle occupants and other road users should be a primary consideration when assessing risk. Companies can mitigate such risks by making cybersecurity a priority through:

- **Designing systems free of unreasonable safety risks:** Companies should develop an ongoing process to evaluate risks and should systematically conduct safety risk assessment steps for the full life cycle of the vehicle. Companies also should develop rapid detection and remediation capabilities.
- **Considering privacy and cybersecurity risks throughout the entire life cycle of the vehicle:** The life cycle of the vehicle includes conception, design, manufacture, sale, use, maintenance, resale and decommissioning.
- **Collecting and documenting information:** The automotive industry should collect information on any potential attack and share such information with the Auto ISAC. Companies should fully document any subsequent actions, changes, design choices and analyses.

2. Leadership Priority on Product Cybersecurity

The automotive industry should foster a culture that is prepared to handle cybersecurity challenges. Companies should facilitate a top-down emphasis on cybersecurity to demonstrate seriousness throughout their organizations. The NHTSA suggests that such corporate priorities can be created by:

- **Allocating resources:** Companies should allocate dedicated resources for research, investigations and testing of cybersecurity measures
- **Establishing communication channels:** Companies should facilitate seamless communication through organizational ranks related to product cybersecurity and should enable independent voices within the safety design process.

3. Information Sharing

The NHTSA was instrumental in the formation of Auto ISAC and encourages all members of the vehicle manufacturing industry to participate. The guidance document also encourages Auto ISAC to expand its membership to suppliers and other vehicle segments.

4. Vulnerability Reporting/Disclosure Policy

Companies should develop additional mechanisms for information sharing, such as a vulnerability reporting and disclosure program. Automotive industry members should consider creating their own vulnerability reporting and disclosure policies or adopting a version used in a different sector. These policies should provide external cybersecurity researchers with guidance on how to disclose issues to automotive industry companies and

should describe the relationship between the company and any cybersecurity researchers.

5. Vulnerability/Exploit/Incident Response Process

The automotive industry should have a process for responding to incidents, vulnerabilities and exploits. This process should:

- cover impact assessment, containment, recovery and remediation actions;
- outline roles for each responsible group and specify requirements for internal and external coordination;
- ensure rapid response without sole dependence on any single individual;
- define metrics used to assess effectiveness of response process;
- document details of each identified and reported vulnerability, exploit or incident, and report them to the Auto ISAC, US-Cert and to the industrial control systems CERT, at the discretion of the company; and
- run periodic response capabilities exercises to test effectiveness of disclosure policy operations and internal response processes.

6. Self-Auditing

The NHTSA recommends that the automotive industry participate in self-auditing by:

- documenting details related to the cybersecurity process, which may include risk assessments, penetration results and organizational decisions;
- retaining documents through the expected life span of the associated product; and
- regularly revising documents such as cybersecurity requirements as new information, data and research become available.

7. Fundamental Vehicle Cybersecurity Protections

The NHTSA has issued recommendations informed through its own internal research. These recommendations are offered to help companies secure automotive computing systems and include: limiting developer/debugging access in production devices, protecting control keys, limiting diagnostic features, employing good security coding practices, and limiting use of network services to essential functionality.

Additional Cybersecurity Recommendations

The NHTSA Guidance concludes with three additional recommendations for the automotive industry. First, the NHTSA recommends that the automotive industry participate in cybersecurity education activities for its current workforce, but also future workforce and nontechnical individuals. Second, the guidance document encourages companies to consider aftermarket devices and equipment that may be brought into cars and connected with vehicle systems. Finally, the NHTSA recommends that implemented cybersecurity protections should not unduly restrict access by authorized third-party service repairers.

Key Takeaways and Next Steps

The NHTSA is accepting public comments on the NHTSA Guidance until November 23, 2016, after which it may revise its guidance or seek to address other related topics. Whatever the final result, the NHTSA Guidance — or its successors — will likely become a benchmark against which the automotive industry's cybersecurity efforts are measured.

Return to Table of Contents

District Courts Dismiss Data Breach Suits Where No Actual Harm Was Alleged

In re Barnes & Noble Pin Pad Litigation, an Illinois district court dismissed a class action complaint for failure to allege cognizable damages, even though the plaintiffs had established "substantial risk of harm" for Article III standing purposes. In _Kamal v. J. Crew Group, Inc._, a New Jersey district court dismissed a class action complaint for failure to establish Article III standing where no actual harm,

In re Barnes & Noble Pin Pad Litigation

On October 3, 2016, the U.S. District Court for the Northern District of Illinois dismissed a class action complaint asserting common law and statutory claims based on a data breach at Barnes & Noble retail stores, holding that the complaint failed to plead cognizable damages even though the plaintiffs sufficiently pleaded Article III standing based on allegations they faced a substantial risk of harm. This decision makes clear that alleging substantial risk of harm to establish Article III standing is not, in itself, sufficient to survive a motion to dismiss.

Background and Claims

In September 2012, certain individuals tampered with PIN pad terminals used to process credit and debit card payments in 63 Barnes & Noble retail stores across nine states. Weeks after learning of this potential data breach, Barnes & Noble publicly announced that the individuals may have stolen customer credit and debit card information. The plaintiffs were customers of the 63 stores during the time when the data breach occurred.

On March 25, 2013, the plaintiffs filed a complaint asserting causes of action for: (1) breach of contract; (2) violation of the Illinois Consumer Fraud and Deceptive Business Practices Act; (3) invasion of privacy; (4) violation of the California Security Breach Notification Act; and (5) violation of California's Unfair Competition Act. Barnes & Noble moved to dismiss the complaint for lack of standing and failure to state a claim under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). The court granted the motion to dismiss for failure to establish Article III standing.

On September 24, 2013, the plaintiffs filed an amended complaint asserting the same causes of action and alleging six additional paragraphs of factual allegations. Barnes & Noble moved to dismiss the amended complaint, again for lack of standing and failure to state a claim.

The Court's Decision

The court dismissed the amended complaint, but this time for failure to state a claim.

The court first addressed the issue of Article III standing, holding that the plaintiffs met their burden to plead injury in fact pursuant to the 7th Circuit's holding in *Remijas v. Neiman Marcus Group*.[5] In discussing *Remijas*, the court noted that the 7th Circuit held that allegations that hackers had targeted the plaintiffs' credit card information made it "plausible to infer that the plaintiffs have shown a substantial risk of harm," and that allegations of lost time and monetary cost to the *Remijas* plaintiffs to protect against future identity theft were sufficient to demonstrate a "substantial risk of harm." Based on Remijas, the court held that the plaintiffs' allegations that their personal identifying information had been taken from Barnes & Noble stores and used for unauthorized purposes, and that the plaintiffs had devoted time and money to preventing improper use of their personal identifying information were sufficient to establish Article III standing.

Next, the court addressed whether the amended complaint stated a plausible claim for relief. Regarding the breach of implied contract and statutory claims, the court held that the amended complaint failed to state a claim because it failed to plead any economic or out-of-pocket damages caused by the data breach. The court cited other cases holding that the loss of value of personal information cannot serve as damages in a breach of contract cause of action. The court also held that one of the plaintiffs' allegations of damages for subscribing to an identity protection monitoring service was insufficient to state a claim because he had previously subscribed to that service and did not allege the data breach was the cause of his decision to subscribe. With respect to the California Security Breach Notification Act claim, the court further noted that there were no allegations that the six-week delay in reporting the data breach caused any injury.

Regarding the invasion of privacy claim, the court held that the plaintiffs failed to allege a public disclosure of any of the plaintiffs' personal identifying information, a requirement for stating a claim. The court held that the information's accessibility by those who sold it and those who potentially purchased it was not sufficient to serve as a public disclosure. Moreover, the court noted that the stolen personal identifying information would not qualify as highly offensive to a reasonable person, an additional requirement to stating a claim.

Kamal v. J. Crew Group, Inc.

On October 20, 2016, the U.S. District Court for the District of New Jersey dismissed a class action complaint asserting a single cause of action for violation of the Fair and Accurate Credit Transactions Act (FACTA) based on the allegation that printing more than the last five digits of a customer's credit card number on receipts violated the statute. The court held that the complaint failed to establish Article III standing because no actual injury was alleged and the allegations of possible future harm, in contrast to "certainly impending" future harm, were not sufficiently "concrete" to qualify as an injury in fact.

Background and Claims

The defendants are a group of clothing stores and manufacturers known as J. Crew and parent company Chino's Holdings, Inc. The plaintiff alleged that in December 2014 and January 2015, he visited several of the defendants' stores and made purchases with a credit card. The plaintiff alleged that the receipts he was given contained the first six and last four digits of his credit card number. The plaintiff filed this action on behalf of customers, who, like the plaintiff, received receipts from the defendants that displayed more than the last five digits of their credit card numbers.

The complaint alleged a single cause of action for violating FACTA. The court denied a motion to dismiss under Rule 12(b)(6), holding that the plaintiff stated a claim for the willful violation of FACTA's credit card number truncation provision. The court then stayed the matter while *Spokeo Inc. v. Robins* was pending in the U.S. Supreme Court. Following the *Spokeo* decision and supplemental briefing, the court addressed whether the plaintiff had Article III standing.

[5] 794 F.3d 688 (7th Cir. 2015).

The Court's Decision

The court cited *Spokeo* for the propositions that (1) an "injury in fact" must be "concrete" in order to establish Article III standing; (2) although "injury in fact" may be "intangible," it must be "actual or imminent, not conjectural or hypothetical"; and (3) allegations of future harm must "entail a degree of risk sufficient to meet the concreteness requirement."

The court held that the plaintiff's allegations of printing 10, rather than five, credit card digits on a sales receipt were insufficient to establish Article III standing. The court reasoned that no allegations established (1) a sufficiently "actual or imminent" risk of future harm; (2) that anyone had accessed, attempted to access or will access the plaintiff's credit card information; (3) that any of the plaintiff's credit card information had been disclosed to third parties; or (4) any actual harm to the plaintiff's credit or identity. Instead, the court found that the allegations were more akin to an increased risk of a data breach sometime in the future, which the court held was not sufficiently "concrete" to qualify as an "injury in fact."

Accordingly, the court granted the motion to dismiss pursuant to Rule 12(b)(1) for failure to establish Article III standing.

Key Takeaways

The decisions make clear that while some circuits have lowered the bar for establishing Article III standing in the wake of *Spokeo*, courts will still closely analyze pleadings to determine whether plaintiffs have pleaded cognizable damages sufficient to establish Article III standing and sufficient to state a claim. As these cases show, establishing Article III standing does not guarantee sufficient damages to state a claim and stating a claim does not guarantee sufficient injury in fact to establish Article III standing.

Return to Table of Contents

Federal Banking Regulators Make Sweeping Cybersecurity Proposal for Large Banks and Related Critical Institutions

The Federal Reserve, Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation have jointly proposed creating a sweeping set of specific cybersecurity governance and operational requirements applicable to large banks and critical financial sector service providers.

On October 19, 2016, the Federal Reserve, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation issued a joint advanced notice of proposed rulemaking (ANPR) requesting comments on a sweeping set of cybersecurity rules for the nation's largest banks, as well as certain critical service providers. The ANPR does not propose specific rules, but is rather a discussion of the types of rules the agencies are considering, and an invitation for comments on specific aspects of those rules. As described in the ANPR, these rules would impose specific cybersecurity governance and operational procedural requirements on these institutions, which would be intended to ensure continuity of the U.S. financial system in the event of a cyberattack.[6]

Largest Institutions Affected

Overall, the agencies are considering applying the new rules to entities with total consolidated assets of $50 billion or more — as well as certain of their service providers — based on the risk an attack on these institutions would pose to the institutions themselves, other financial institutions and the U.S. financial sector overall. Each agency would apply the rules to entities within its own jurisdiction, and to those entities' service providers.

Furthermore, because an attack on one part of a financial institution could affect other parts, the rules would apply on an enterprisewide basis.

Needs to Address

The ANPR's proposed rules would require covered entities to meet enhanced cyberrisk management standards, which would focus on their need to:

demonstrate effective cyberrisk governance;

- continuously monitor and manage their cyberrisk within the risk appetite and tolerance levels approved by their boards of directors;
- establish and implement strategies for cyber resilience and business continuity in the event of a disruption;
- establish protocols for secure, immutable, transferable storage of critical records;
- maintain continuing situational awareness of their operational status and cybersecurity posture on an enterprisewide basis; and
- (for "sector-critical systems" only) substantially mitigate the risk of a disruption due to a cyber event to their sector-critical systems.

[6] The text of the ANPR is available here.

Five Categories of Standards

The standards proposed in the ANPR are organized into five general categories, and the ANPR goes into substantial detail (with specific questions) on each. We have summarized the key elements of the standards below.

1. Cyberrisk Governance

The ANPR describes a key aspect of cyberrisk governance as developing and maintaining a formal cyberrisk management strategy that is integrated into the overall strategic plans and risk governance structures of covered entities, as well as a supporting framework of policies and procedures to implement the strategy.

As part of this governance process, the agencies are considering a number of requirements, including the following:

- the covered entity's board of directors must approve the overall strategy and hold senior management responsible for implementing policies consistent with the strategy;
- the entity must establish its cyberrisk tolerances to be consistent with the entity's overall risk appetite and strategy, and manage risk appropriately;
- the entity must identify and assess cyberrisks;
- the entity's board of directors must have adequate expertise in cybersecurity, or maintain access to resources or staff with such expertise, so it can provide a credible challenge to management on these issues;
- senior leaders with responsibility for cyberrisk oversight must have direct, independent access to the board and must independently inform the board of cyberrisk exposures;
- the entity must implement enterprisewide reporting structures and expectations for risk management; and
- the entity must include in its risk management framework mechanisms for identifying and responding to cyber incidents.

2. Cyberrisk Management

Having established overall risk strategies and tolerances, the ANPR describes specific proposals the agencies are considering for implementing, managing and monitoring these strategies, broken down into three separate functions: business units, independent risk management and audit.

Business Units. As described in the ANPR, business units would be responsible for assessing, on an ongoing basis, the cyberrisks associated with their activities and all of their assets (including workforce, data, technology and facilities) and report those risks to senior management. In addition, business units would have to comply with policies and procedures necessary to adhere to the entity's overall risk management framework. In order to fulfill these duties, the business units should maintain — or have access to — resources and staff with the skill sets needed to assess and address cyberrisks.

Independent Risk Management. The ANPR suggests that covered entities would have to integrate cyberrisk management into their overall independent risk management function. This function would report to the entity's chief risk officer and board of directors regarding implementation of the entity's risk management framework throughout the organization. Risk management would analyze cyberrisk at the enterprise level and report to the CEO and board of directors if its assessment of cyberrisk differed from that of the business units. In addition, the ANPR suggests that companies may have to, at a holding company level, quantitatively measure the completeness, effectiveness and timeliness with which they reduce their aggregate cyberrisk and report this analysis to the appropriate level. (One of the questions on which the ANPR seeks input is how to develop a methodology to quantitatively measure these factors.)

In order to achieve these goals, the risk management function must have the appropriate independence, stature, authority, resources and board access to ensure that the entity's operations are consistent with its cyberrisk framework.

Audit. Finally, the ANPR proposes that cyberrisk be added to an entity's existing audit function. Entities should incorporate an assessment of cyberrisk management into their overall audit plan. This plan should include risk assessments of the entire security lifecycle, including penetration testing and vulnerability assessments as appropriate based on the entity's size and complexity.

3. Internal Dependency Management

The ANPR explains the agencies' proposals for entities to assess and manage the cyberrisks associated with their internal assets (such as their workforce, data, technology and facilities) throughout their lifecycles. These risks would include, for example, insider threats, data transmission errors and the use of legacy systems acquired through a merger. The agencies would expect entities to continuously assess and improve their effectiveness in mitigating these risks on an enterprisewide basis.

As part of the standards in this area, the ANPR suggests a number of requirements, including requiring entities to:

- have current and complete awareness of all internal assets and business functions, including an inventory of all business assets that is prioritized based on their criticality to the business function they support, the entity's mission and the financial sector;
- map the interconnections between these assets so as to understand how events impacting some assets could affect others;

- have controls in place to address the cyberrisks posed by their internal assets; and
- periodically conduct tests of back-ups to business assets to achieve resilience.

4. External Dependency Management

Parallel to assessing an entity's internal dependencies, the ANPR also describes how the agencies believe entities should manage risk associated with external dependencies. These external dependencies include, for example, vendors, suppliers, customers, utilities and other external organizations and service providers which the entities depend on, or that interact with important systems. Entities should identify these dependencies and understand the interconnections between the entity and these external parties.

As part of the external dependency management strategy, the agencies are considering requiring entities to establish effective policies, plans and procedures to identify and manage, in real time, the cyberrisks associated with these external dependencies, especially those that connect to sector-critical systems and operations.

As with the internal dependency management, the agencies make a number of proposals for standards in this area, including requiring entities to:

- maintain current, accurate and complete awareness of all external dependencies, and prioritize them based on their criticality to the business function they support, the entity's mission and the financial sector;
- map these dependencies and business functions, and be aware of how these external dependencies connect with each other; and
- review and analyze the risks associated with these external relationships, and periodically test alternative solutions in case an external partner fails to perform as expected.

5. Incident Response, Cyber Resilience and Situational Awareness

Standards within the incident response, cyber resilience and situational awareness category would be designed to ensure that entities plan for, respond to, contain and rapidly recover from disruptions caused by cyber incidents. The ANPR describes a number of specific proposed requirements in this area, including:

- entities must be able to anticipate, withstand, contain and rapidly recover from disruptions caused by cyber events, and be able to continue operating critical business functions in the face of a cyberattack;
- entities must maintain situational awareness of changes in the operating environment so that they can reliably predict, analyze and respond to those changes;
- entities must have in place cyber resilience and incident response programs that include escalation procedures, contagion containment procedures and communications strategies;
- the entity's cyber resilience and incident response program must include feedback processes to enable lessons learned in one attack to be applied back to the programs for the future;
- entities must establish protocols for secure, immutable offline storage of critical records, including daily transaction information, in order to preserve critical records in the event of a cyberattack; and
- entities must have plans in place to transition business to another entity or service provider within prescribed timeframes, in order to preserve critical records in the event of a cyberattack.

Higher Standards for Sector-Critical Systems

The ANPR suggests that different standards might apply to "sector-critical systems." While asking for guidance on how to define such systems more specifically, the agencies describe these as "systems of covered entities that are critical to the functioning of the financial sector," suggesting that entities will have a mix of sector-critical and other systems, and thus must have different policies for both.

Specifically, the ANPR proposes two specific requirements with respect to these sector-critical systems:

- entities should implement the "most effective, commercially available controls" to protect these systems from cyberrisks. This requirement suggests that entities and vendors may end up engaging in a rapid "race to the top" as security and other technologies improve.
- entities will have to design their processes to target a two-hour recovery time for these systems.

Interaction with Existing Policies and Guidance

The ANPR makes clear that the proposed rules are not intended to supersede existing policies and guidance applicable to these institutions. These existing policies and guidance include, for example:

- the Federal Financial Institutions Examination Council's (FFIEC) "IT Handbooks," which provide cybersecurity guidance for examiners reviewing financial institutions and their service providers;

- the Gramm-Leach-Bliley Act's safeguarding requirements providing general requirements for financial institutions for cybersecurity practices related to customer financial data;
- the NIST's Cybersecurity Framework, a voluntary framework for assessing and addressing cybersecurity risks across many industry sectors; and
- the FFIEC's Cybersecurity Assessment Tool, a voluntary self-assessment tool.

Rather than supplant these existing regimes, the new rules, as envisioned by the agencies, would supplement them by thus imposing higher standards on the largest institutions and the critical service providers.

Key Takeaways and Next Steps

Although the ANPR is not a specific proposal for cybersecurity rules, it clearly reflects the issues of concern to these three key federal regulators and what they see as best practices to address them. These rules, if enacted, would reflect the first set of specific enterprisewide requirements imposed by federal regulators on cybersecurity matters. This move follows closely on the heels of the New York Department of Financial Services' proposed cybersecurity rules for the financial sector, suggesting a growing trend towards greater specificity on cybersecurity matters.[7]

Answers to the ANPR's questions are due January 17, 2017, suggesting that any specific policy proposals from these agencies will not be released until sometime later that year. We will closely monitor these developments and provide updates in this newsletter as the situation evolves.

Return to Table of Contents

European High Court Rules that IP Addresses Can Be 'Personal Data'

The European Court of Justice has ruled that dynamic IP addresses can be "personal data" under the EU Data Protection Directive, even if the person storing the IP address does not have the information necessary to associate that data with a particular data subject.

On October 19, 2016, Europe's highest court, the European Court of Justice (ECJ), ruled that dynamic IP addresses can qualify as "personal data" under the EU Data Protection Directive, even if additional information from other data sources was required to identify the individual associated with such IP addresses. The decision in *Breyer v. Federal Republic of Germany* confirms what many pundits had asserted: that dynamic IP addresses were covered under the directive. While at least some IP addresses already were going to be deemed personal data under the new General Data Protection Regulation (GDPR) going into effect in 2018, the court's decision will have an immediate and significant impact on website and other internet service operators as well as on pseudonymization practices, and it suggests that the GDPR will be interpreted to apply to dynamic IP addresses as well.[8]

Static Versus Dynamic IP Addresses

The EU Data Protection Directive defines "personal data" as "any information relating to an identified or identifiable natural person." Static IP addresses — those that remain constant over time — were long believed to constitute personal data because they could be used to consistently identify a specific machine connected to the internet, and thus the user of that machine. With respect to dynamic IP addresses — which change every time the user reconnects to the internet — there was more ambiguity. While parties (such as internet service providers) held enough information to associate a specific dynamic IP address with a specific user at a specific time, many believed that if a party only held the IP address and did not have the other data necessary to associate that IP address with an individual, the IP address was not personal data under EU law.

Background of the Case

Patrick Breyer, a German privacy activist and member of Germany's Pirate Party, sought to stop the German government from registering and storing his dynamic IP address when he visited its web pages, claiming that such practices were a violation of data protection laws. Many websites operated by the German government store certain visitors' information, including IP addresses, search terms and access dates for purposes of preventing cyberattacks and identifying attackers.

Breyer argued that his IP address should be treated as personal data under the EU Data Protection Directive, which applies special protections to such information and which would prevent the German government from storing such IP addresses. The German government argued that dynamic IP addresses could not be considered personal data because an individual could not be identified by an IP address without obtaining additional information from a third party, such as the individual's internet service

[7] For a discussion of the New York Department of Financial Services proposal, see our September 15, 2016, supplement to the monthly *Privacy & Cybersecurity Update*, available here.

[8] A copy of the decision is available here.

provider. The case was referred by the German federal court to the ECJ to settle that question.

ECJ Ruling

The ECJ ruled that data may be deemed "identifiable" even if such information alone is not sufficient to identify the individual and additional means are required to do so. If a website operator could employ legal means, such as a request from a governmental authority, to require the internet service provider to provide additional information that could then be used together with the dynamic IP address to identify the individual, then the IP address in question should be considered personal data.

Effect of Ruling

The ECJ's ruling effectively broadens the definition of personal data used in the EU Data Protection Directive. Websites and other internet-enabled service operators routinely collect IP addresses from users, so now they will have to consider how they must reform their activities to comply with the Data Protection Directive's limits on the collection, use and storage of this data.

The ruling also may impact the scope of the GDPR, which goes into effect in May 2018. The GDPR generally uses a similar definition of personal data to that used in the Data Protection Directive, but expressly includes "online identifiers," a term that is generally believed to at least include static IP addresses. There was some question, however, whether dynamic IP addresses were within GDPR's scope, for the same reason as there was doubt under the directive. The ECJ's ruling with respect to the directive suggests it will apply the same standard under the GDPR.

Finally, the *Breyer* decision may also have implications for the practice of pseudonymization of personal data, which the GDPR suggests as a means to ensure data security and the lawfulness of data processing, or to enable research. The GDPR defines pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." The information held by the internet service provider in *Breyer* was kept separate from the website operator's information and was subject to technical and organizational measures to defeat attribution. These measures were seemingly in compliance with the GDPR definition but was nevertheless held to identify the individual in question. The ECJ's decision suggests that such pseudonymization will not be sufficient to escape the scope of the law's personal data definition.

Future Remains Uncertain

It remains to be seen whether the ECJ will take the same view under GDRP as it did under the Data Protection Directive, though it seems likely. The GDPR has not yet gone into effect, so there have yet been no cases posing the question. In the meantime, website operators will need to carefully examine their practices with respect to the collection and use of dynamic IP addresses now that those practices are more clearly subject to the directive.

Return to Table of Contents

G7 Cybersecurity Risk Experts Establish Framework Outlining Eight Elements of Cybersecurity for the Financial Sector

The G7 Cyber Expert Group has announced a framework to help public and private financial entities address cyberrisks. The framework adds to a growing body of recent guidance and proposed regulation in this area.

On October 11, 2016, the G7 Cyber Expert Group, comprised of representatives from the United States, Canada, France, Germany, Italy, Japan and the United Kingdom, announced a voluntary framework to help financial institutions address cyberrisks. The G7 framework comes amid moves by U.S. state regulators (such as New York's Department of Financial Services)[9] and federal regulators (such as the recent announcement by the Federal Reserve, FDIC and Office of the Comptroller of the Currency)[10] to address cyberrisk issues, and reflects policymakers' growing emphasis on cyber as a key issue to be addressed.

The G7 framework identifies eight elements as critical to assess and confront cyberrisks, and is intended to provide high-level guidance to help public and private financial entities address risks based on their risk profile and other binding legal and regulatory requirements. They also are intended to allow entities to engage in an evolving process of risk assessment and to encourage re-evaluation of responses, strategy and policies.

The eight elements identified in the G7 framework are set forth below. Each describes a specific action that public and private financial entities should take:

[9] For a discussion of the New York Department of Financial Services proposal, see our September 15, 2016, supplement to the monthly *Privacy & Cybersecurity Update*, available here.

[10] The Federal Reserve, FDIC and Office of the Comptroller of the Currency announcement is discussed elsewhere in this issue.

- **Element 1 – Cybersecurity Strategy and Framework:** Implement a cybersecurity strategy that is tailored to the entity's risk profile and is informed by international, national and industry standards and guidelines;
- **Element 2 – Governance:** Establish defined roles for personnel overseeing the cybersecurity strategy to foster accountability and communication, as well as to help establish proper resource allocation and access to decision-makers;
- **Element 3 – Risk and Control Assessment:** Evaluate the cyberrisks and the entity's existing controls to protect against such risk, as well as prioritizing the importance of the risk and identifying any relationships between the various risks;
- **Element 4 – Monitoring:** Establish a monitoring process that can detect cyber incidents and evaluate the effectiveness of the system quickly and on an ongoing basis. Such monitoring can be enhanced if it is performed by individuals who are independent from those personnel responsible for managing the cybersecurity program;
- **Element 5 – Response:** Implement incident response policies to allow the entity to timely assess a cyber incident, contain it, notify stakeholders and coordinate any joint response.
- **Element 6 – Recovery:** Achieve operational stability after a cyber incident and focus on returning critical economic and other functions while allowing for continued remediation.
- **Element 7 – Information Sharing:** Gather and share reliable cybersecurity information with internal and external stakeholders, both inside and outside of the financial sector, to increase the breadth of understanding of cyberrisks and ability of all entities to respond to such risks.
- **Element 8 – Continuous Learning:** Review and revise the cybersecurity framework regularly in order to identify and solve any issues, as well as to incorporate any lessons learned from any incidents.

The framework itself does not create any binding obligations. It simply sets forth guiding principles that financial institutions should take into account when establishing their cybersecurity framework and programs. Despite the high-level nature of the elements set forth in the framework, it is clear that companies need to thoroughly assess their own risk profile and cybersecurity preparedness on an individual basis in order to bolster the security of the international financial system.

Return to Table of Contents

Federal Regulators Issue Guidance on Use of Cloud Computing Under HIPAA; Cloud Service Providers are Deemed 'Business Associates'

The Department of Health and Human Services has issued guidance on the use of cloud computing services. While permitted under HIPAA, the cloud service providers will be business associates that must comply with HIPAA's privacy and security rules.

On October 6, 2016, the U.S. Department of Health and Human Services (HHS) issued new guidance on how to use cloud computing technology and also comply with HIPAA obligations relating to privacy, security and breach notification.[11] The guidance made it clear that the use of cloud service providers (CSPs) is permissible under HIPAA, provided that certain conditions are met. Specifically, the guidance clarifies that CSPs are considered "business associates" under HIPAA, even if the CSPs only have access to encrypted health information (and not the decryption key). The guidance also specifies that CSPs subcontracted by business associates also would be deemed to be business associates for the purposes of HIPAA.

HIPAA and Business Associates

HIPAA's regulations apply to health plans, health care providers and other entities that are involved in the health service industry, as well as business associates that perform services for those entities. Among its many requirements, HIPAA includes specific obligations with respect to the collection and use of protected health information (PHI). Business associates must enter into business associate agreements (BAAs) with the applicable covered entity, which set out the permitted uses and disclosures of PHI and contractually obligate the business associate to appropriately safeguard any PHI.

Application to Cloud Service Providers

Under the new HHS guidance, CSPs that provide services to covered entities (or to other business associates) are business associates under HIPAA. As business associates, the CSPs, in conjunction with the covered entities, must conduct risk analyses to identify particular threats and vulnerabilities to the confidentiality, integrity and availability of PHI passing through

[11] The guidance is available here.

their systems. According to the guidance, these risk assessments should include a review of the nature and structure of the cloud services being provided, such as whether the services are private or public cloud offerings.

In addition to their contractual obligations under the BAA, as a business associate CSPs must also comply with specific requirements of HIPAA. These include: (1) implementing appropriate internal controls to limit access to information systems that maintain PHI under the HIPAA Security Rule in order to protect the availability, confidentiality and integrity of the PHI; (2) only using the PHI as permitted by the HIPAA Privacy Rule; and (3) appropriately notifying customers of any breaches of PHI as required by HIPAA. These obligations apply even where a CSP only has access to encrypted PHI and does not have the ability to decrypt such information. However, if the information has been "de-identified" in accordance with the HIPAA Privacy Rule (which requires the removal of various types of information) then the CSP would not be deemed a business associate, and the associated restrictions and requirements would not apply.

Key Takeaways

In light of the new HHS guidance, HIPAA-regulated entities should reassess their use of cloud-based services and enter into BAAs where appropriate. CSPs also should ensure compliance with HIPAA in all circumstances where they are processing PHI. In addition, HIPAA-regulated entities and business associates (including CSPs) should ensure that they are appropriately conducting risk analyses and risk management in order to identify and manage risks associated with the use of cloud services.

Return to Table of Contents

New Study Indicates that Consumers May Not Benefit From More Cybersecurity Awareness

A NIST study suggests that efforts to give consumers more information and control over their security profile is driving consumers to engage in poor security practices. The study may push policymakers to fundamentally reform their approach to security matters.

A recent study from NIST suggests that a consistent thread in privacy and cybersecurity laws and guidance may be having the opposite effect than what was intended. The study, which was published in the September-October 2016 edition of the trade publication "IT Professional," found that the push to provide consumers with more information on security risks and impose rigid security requirements actually drives consumers to engage in poor security practices rather than improve their habits. Coming from such an influential source as NIST, these results may drive policymakers to fundamentally rethink how they require companies to communicate with consumers on security issues.

Security Fatigue

According to NIST, the study found that a majority of ordinary computer users experience decision fatigue regarding online security. The individuals in the study ranged in age from 20 to 60, worked in a variety of jobs, and lived in urban, suburban and rural areas. The interviewers asked participants about their professional and personal computer habits and their use of computer security, security terminology, security icons and tools.

In the interviews, many participants expressed feeling bombarded by the breadth of security protocols involved in their daily computer use, such as software updates and requirements to change passwords. Instead of facilitating safe online behavior, these initiatives have led to feelings of hopelessness, risk minimization and decision avoidance, behaviors NIST calls "security fatigue." The study found that warnings to stay alert and adopt safe online behavior overwhelmed the majority of typical consumer users. As a result, users avoided making decisions or based their decisions on immediate motivations and failed to follow security guidelines. Most subjects expressed frustration with understanding the complexity of various privacy policies and trying to remember different usernames and passwords, as well as needing to gain access to their personal accounts through additional security measures.

Assessing and Minimizing Risk

In addition to feelings of information and warning overload, interviewees also doubted that they would be the target of a cyberattack. Many participants felt they were not high-profile enough for someone to want to steal their information, stating they did not work for the government or a financial company. They also noted that they did not personally know anyone who had been the subject of a cyberattack.

Some participants also were skeptical of their ability to protect themselves online, referencing the fact that large corporations had expended tremendous sums of money on security and still suffered from computer hacks. Others felt it was the responsibility of larger companies, whether it be banks or online stores, to protect consumer data. These perceptions contribute to users' decisions as to whether to incorporate or disregard recommended security practices.

Moving Forward

NIST plans to interview employees in the technology field to assess their perceptions and thought processes compared to ordinary users. They will interview individuals with a range of responsibility, including cybersecurity professionals and midlevel employees with duties to protect personally identifiable information.

Key Takeaways

Cybersecurity risks are spreading as more users store sensitive information online through online banking, healthcare portals and other services. The NIST study suggests that to encourage users to adopt safe online habits and make informed decisions, service providers should limit the volume of decisions users need to make, streamline the process for choosing the right security action and create opportunities for consistent decision making.

NIST has historically been a key policy influencer in the U.S. government's efforts to provide guidance on cybersecurity. As a result, the NIST study's conclusions that current practices have been counterproductive are likely to carry significant weight. As policymakers continue to examine best practices for protecting consumer privacy and security, they are likely to take NIST's findings into account and may fundamentally rethink their strategies on these issues.

Return to Table of Contents

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Jennifer L. Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

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

Gregoire Bertrou
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@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

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