Skadden

# Privacy & Cybersecurity Update


1 DOJ Issues Cyber Preparation and Response Guidance

2 RadioShack's Plan to Auction Customer Data Highlights Issues Over Treatment of Such Data as an Asset

3 *Google v. Vidal-Hall and Others:* The English Court of Appeal Recognizes "Distress" as Damage

4 San Francisco Federal Court Dismisses Video Privacy Protection Act Claims Against Hulu

5 New Jersey Federal Court Dismisses Claims Against Horizon Healthcare Services Over Members' Data Breach

6 President Obama Expands US Cybersecurity Sanctions Regime

7 NY Department of Financial Services Highlights Concerns Over Data Practices of Third-Party Service Providers

8 The FCC Takes on a New Privacy Enforcement Role

10 NAIC Adopts Cybersecurity Principles, Continues Focus on Cyber Insurance Marketplace

10 Virginia Establishes First State-Level Information Sharing Organization


## DOJ Issues Cyber Preparation and Response Guidance

**As part of its ongoing attempts to engage more directly with the private sector on cybersecurity issues, the Department of Justice has released a set of best practices for small and medium businesses planning for and responding to cyber incidents.**

On April 29, 2015, the Department of Justice (DOJ) hosted a roundtable on cybersecurity breach preparation and response. Members of DOJ's Criminal Division and National Security Division and representatives from the FBI and the White House all offered government perspective on recent cybersecurity events and the threats faced by the private sector. Attorneys from the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and other DOJ representatives then discussed engagement with the private sector and the need to do more to combat cybersecurity threats.

Concurrently with the roundtable, DOJ released its recommendations for cyber response, the CCIPS Cybersecurity Unit's "Best Practices for Victim Response and Reporting of Cyber Incidents" Version 1.0.[1] The best practices consist of approximately a dozen pages of DOJ guidance and a two-page cyber incident preparedness checklist. CCIPS states that the best practices were "drafted with small, less-resourced organizations in mind; however, even larger organizations with more experience in handling cybersecurity incidents may benefit from it." DOJ has indicated that it intends to update the document as necessary.

Nearly half of the guidance portion of the best practices document discusses steps to take before a cyber incident occurs, including:

- identifying key systems, intellectual property and proprietary data;
- developing a cybersecurity incident response plan;
- having appropriate security technologies (*e.g.*, data backup and intrusion detection/prevention) in place in advance;

[1] Available at: http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

- obtaining authority from users to monitor systems in advance;
- ensuring organization policies are consistent with the incident response plan;
- engaging counsel familiar with technology and cyber incident management; and
- reaching out to law enforcement and industry information-sharing organizations.

Much of the post-incident response guidance focuses on two topics of particular interest to government cybersecurity investigators. The first is data collection and retention: The guidance discusses how to ensure that important information is logged or otherwise recorded while systems are restored to full functionality. The second is notification, most notably notice to the government: The guidance strongly recommends outreach to a number of different government parties under specified circumstances, including the FBI, U.S. Secret Service, state and local law enforcement, and the Department of Homeland Security.

Return to Table of Contents

## RadioShack's Plan to Auction Customer Data Highlights Issues Over Treatment of Such Data as an Asset

**RadioShack's attempts to sell its customer data as part of its bankruptcy process is an example of the difficulties companies can face with respect to the transfer of personal information.**

In conjunction with its ongoing bankruptcy proceedings, RadioShack plans to auction off its customer data, which includes the personal information of millions of its customers. In the face of objections from attorneys general and consumer groups, the company will auction the information on May 11, 2015, with bids due on May 6. The company's plans highlight the controversies that arise when a company seeks to treat its database of customer information as a fungible asset.

RadioShack pulled the customer data off the auction block in March, reportedly in response to public outcry against the sale of the data. However, on April 10, 2015, the financially troubled consumer electronics retailer announced that it intends to sell its customer data in an effort to satisfy its creditors. The data may include customers' email addresses, names and physical addresses.

Attorneys general from over 20 states, led by Texas Attorney General Ken Paxton, as well as AT&T and consumer protection bodies from over 30 states, have all voiced their opposition to RadioShack's proposed sale of customer information. The opposition points to RadioShack's privacy policy which clearly states that RadioShack "will not sell or rent [customers'] personally identifiable information to anyone at any time." In addition, Paxton has requested that a federal court reject the asset sale because the he believes RadioShack has failed to provide sufficient information regarding what will be sold.

The fact that this proposed sale is taking place in the context of a bankruptcy complicates the issues. In 2001, Congress amended the Bankruptcy Code to directly aid debtors who need to satisfy creditors when one of their valuable assets is their customer data. The amended code applies to debtors who had a privacy policy in place at the time the bankruptcy proceedings commenced that restricted the sale of personally identifiable information.[2] It prevents trustees from selling or leasing the information unless the bankruptcy court determines (1) the transaction complies with the privacy policy or (2) the transaction will not violate applicable nonbankruptcy law. In order to assess the latter, the court must appoint a consumer privacy ombudsman, hold a hearing and consider all the facts and circumstances surrounding the situation. Privacy ombudsman are disinterested third parties that are appointed to provide the bankruptcy court with information needed to assess the situation, the impact on consumer privacy and the costs or benefit to consumers, and to determine if there are other viable alternatives.[3] A privacy ombudsman was appointed early on in the RadioShack case and is expected to file a report and recommendations.

RadioShack is not the first company to sell customer data in financially troubled times. In 2000, before the Bankruptcy Code was amended, the Federal Trade Commission (FTC) filed a complaint against Toysmart.com after Toysmart advertised that its customer data was for sale. Toysmart's privacy policy promised to never share its customers' personal information with third parties. The FTC alleged the sale was a deceptive act in violation of Section 5 of the FTC Act as well as a violation of the Children's Online Privacy Protection Act (COPPA). Ultimately, the FTC's order allowed the sale to go forward in a restricted form. The data could only be sold to a "qualified buyer" as part of a sale of the whole website, and the qualified buyer was required to follow Toysmart's privacy policy.

More recently, in September 2011, Borders Group, Inc. auctioned off its customers' personally identifiable information. The data sold included purchase history and email addresses of millions of customers. Borders collected data under three different privacy policies over time — two contained a promise not to rent or sell the customer's data without obtaining consent,

[2] 11 U.S.C. § 363(b)(1).

[3] 11 U.S.C. § 322.

while a third allowed Borders to sell the data in connection with a merger or reorganization of the business. Ultimately, the bankruptcy judge allowed the auction of the customer data to move forward. In working with the consumer privacy ombudsman, Barnes & Noble (the successful buyer) and Borders agreed to email affected customers and give them 15 days to opt not to have their information transferred to Barnes & Noble.

RadioShack will not be the last business with valuable consumer data that encounters financial difficulty. The public outcry and the decision of RadioShack to move forward with the sale only highlights the tension between consumers and businesses over this valuable asset. Companies that could face similar issues in the future should review their privacy policies to confirm that they allow transfers of consumer information in connection with an acquisition of the company or relevant business line.

Return to Table of Contents

## *Google v. Vidal-Hall and Others*[4]: The English Court of Appeal Recognizes "Distress" as Damage

**An English appeals court has recognized a right for individuals affected by a privacy violation to recover damages without showing actual financial harm.**

At the end of March 2015, the English Court of Appeal handed down a decision that some commentators have called the "decision of a decade." While that might be an overstatement, the ruling from the Court of Appeal — which for the first time enables the victims of a breach of the Data Protection Act 1998 (DPA) to obtain damages (financial compensation) without also having to show a financial loss — is significant and provides a real remedy for individuals who suffer distress from a breach of the DPA.

In this action, a group of claimants asserted that Google's tracking and collation of information held on the Apple Safari browser about their use of the Internet without their consent:

- amounted to a misuse of their private information;
- breached their confidences; and
- breached Google's duties under the DPA to process their personal data fairly and lawfully, and to ensure that it is used only for the purpose for which it is given and that appropriate measures should be taken to prevent unauthorized or unlawful processing of the data and prevent its loss or destruction.

The claimants sought damages and injunctive relief but had suffered no financial loss.

### Remedy for a Breach of the DPA

Section 10 of the DPA enables individuals to prevent processing that causes damage or distress. Given this, and that financial loss in these circumstances can be difficult to demonstrate, the English cases seeking financial compensation for a breach of the DPA have been few and far between. Until *Vidal-Hall*, such case law as there was supported the position that financial compensation could not be awarded where the claimant could not also demonstrate a pecuniary loss. Most breaches of the DPA result in distress and little more, so this approach has provided little deterrent for data controllers and processors who might be tempted to risk a breach of the DPA.[5]

The European Data Protection Directive, from which the DPA derives, provides that the United Kingdom, as a member state of the European Union, should ensure that a person who suffers damage as a result of a breach of the DPA is entitled to receive compensation from the data controller for the damage suffered.

To implement this, Section 13(1) of the DPA sets out the right to damages for a breach of the Act that results in "damage." Damages may also be recovered for distress (Section 13(2)), but only where "the individual also suffers damage by reason of the contravention," or the contravention relates to the processing of information for certain "special purposes" that include journalism, literature and art. "Damage" has been interpreted in the English courts as financial damage only.

### What Has Changed?

In *Vidal-Hall*, the court found that the underlying purpose of the data protection legislation is to protect privacy rather than economic rights, so a financial remedy should be available to the victims of a breach of the DPA whether or not they have suffered a financial detriment as a result of the breach. The court applied principles of European law effectively to overrule Section 13(2) DPA as inconsistent with the Data Protection Directive's approach to remedies. As a result, individuals whose rights under the DPA are breached in the United Kingdom can now rely on distress alone to claim damages.

[4] [2015] EWCA Civ 311.

[5] English law provides that the damages (financial compensation) for a breach of the DPA should be assessed by reference to the damage suffered by the claimant, because a breach of the DPA would be a statutory tort.

The quantum of the damages they might be awarded is another question, however. The court did not address this in the *Vidal-Hall* case beyond acknowledging that the sums involved were "likely to be modest," although the "issues of principle are large." The sums awarded to date in cases involving special purposes have been limited (for example, the supermodel Naomi Campbell was awarded £2,500 for a claim combining breach of confidence and the DPA where a newspaper published a picture of her attending a private meeting), and we anticipate that individual awards are likely to be nominal.

### What Next?

This decision has been made against the backdrop of the 2013 Leveson Report into the English press, which recommended that the Section 13 DPA right extend to cases involving distress alone and that there be a review of damages generally for other media-related torts such as breach of privacy and confidence. We continue to anticipate the new Data Protection Regulation (intended to replace the directive). While that is likely to be a while coming, early drafts of the text for the new regulation refer to the right to compensation for "any person who has suffered damage, including non-pecuniary damage."

Whenever (and whether) such changes are made, we can expect an increase in the number of claims for compensation and the potential for group litigation (for example, where an organization's breach, like losing or disclosing personal data, affects a large number of people) is significant. The cost of a large number of nominal awards can add up very quickly.

Return to Table of Contents

## San Francisco Federal Court Dismisses Video Privacy Protection Act Claims Against Hulu

**A Video Privacy Protection Act case based on Hulu's transmission of information to Facebook has failed because Hulu did not know that Facebook would connect users to specific viewing choices when the data was transmitted separately.**

In *In re: Hulu Privacy Litigation*,[6] a federal magistrate judge granted summary judgment as to claims alleged against Hulu for its transmissions of alleged personally identifiable information (PII) to Facebook under the Video Privacy Protection Act, 18 U.S.C. § 2710 (the VPPA). PII is defined under the VPPA to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The VPPA generally prohibits videotape service providers from knowingly disclosing PII without the written consent of the consumer and permits a court to award punitive damages and attorneys' fees, in addition to statutory damages of at least $2,500 per violation.[7]

The court previously denied a motion for summary judgment by Hulu in April 2014 on the question of whether the information transmitted to comScore and Facebook constituted PII — *i.e.*, whether it linked a particular person and the video selected by that person, as discussed in our May 2014 issue.[8] The court's previous decision was based in part on the fact that the motion was brought early in the discovery process and the court noted specifically that "[i]f Hulu did not know that it was transmitting both an identifier and the person's video watching information, then there is no violation of the VPPA."

In its March 2015 opinion, the court ruled that the plaintiffs had failed to present any issue of material fact to suggest that Hulu actually knew that Facebook might combine information that identified Hulu users with separate information specifying which video that user was watching so as to "identif[y] a person as having requested or obtained specific video materials" under the VPPA. Thus, the court dismissed the plaintiffs' Second Amended Complaint with prejudice because Hulu did not *knowingly* disclose any PII to Facebook.

### Background

Hulu is an online video streaming service that allows registered users to view TV episodes or movies on-demand through its website. To register for a Hulu account, users supply a first and last name, date of birth, gender and email address. Hulu assigns each registered user a unique numerical identifier (Hulu User ID).

Videos on hulu.com are displayed on a video player that appears on a webpage called a "watch page." In August 2010, Hulu added a Facebook "like" button to each hulu.com watch page. It did so with code that caused the user's web browser to send a request to Facebook to load the button on the Hulu page so that the user would have the option to "like" the video on Facebook. In addition, if the Hulu user had logged into Facebook using certain settings within the previous four weeks, the "like" button would cause a "c_user" cookie to be sent to Facebook. This cookie was associated with the Facebook.com domain and contained (among other things) the logged-in user's Facebook user ID expressed in a numeric format that Facebook can identify as a particular Facebook user.

[6] No. C 11-03764 LB (N.D. Cal. Mar. 31, 2015).

[7] 18 U.S.C. § 2710(c)(2).

[8] Available at: https://www.skadden.com/insights/privacy-cybersecurity-update-may-2014.

This transfer of information occurred automatically when the user loaded the watch page; no action by the user (such as clicking the "like" button) was required. Hulu never sent Facebook a user's name or Hulu ID. There is no evidence that Facebook took any action with the c_user cookie. Nevertheless, the plaintiffs alleged that Hulu violated the VPPA by disclosing users' PII to Facebook.

### The Court's Ruling

The court explained that the "knowingly" requirement of the VPPA means "consciousness of transmitting private information." Magistrate Judge Laurel Beeler rejected the plaintiffs' argument that a defendant's being "aware of what he or she is doing ... and not act[ing] because of some mistake or accident" would suffice to meet this "knowingly" requirement. For liability under the VPPA, a video provider must have knowingly disclosed (1) the consumer's identity, (2) the identity of specific video material, and (3) the fact that the person identified "requested or obtained" that material.

In this case, the court held that the identity of the user and the video material was transmitted separately (albeit simultaneously). Thus, if Hulu did not actually know that Facebook might read the c_user cookie and video title together, then there cannot be a VPPA violation. The court found that the plaintiffs identified no proof that Hulu knew that Facebook might combine those two discrete factors to reconstruct PII. Hulu, on the other hand, introduced affirmative proof that it did not know what, if anything, Facebook would do with the user-identifying information in the c_user cookie and the video title that could be gleaned from the watch-page addresses. Accordingly, the court held that plaintiffs did not have a triable claim under the VPPA.

The court also rejected the plaintiffs' novel theory that the filing of the complaint alone gave Hulu the knowledge that it was violating the VPPA to satisfy a requirement of the VPPA statute.

### Practice Points

While the court's decision is encouraging to companies, it was ultimately based on the good facts uncovered in this case. The holding is unlikely to discourage plaintiffs' attorneys from filing future VPPA lawsuits, because such facts are not available at the outset of a litigation. However, going forward, companies may be able to facilitate early resolution of such cases by obtaining representations and warranties from third parties that they are not able to or will refrain from using information shared with them to identify specific users' browsing history.

The decision also underscores the importance of companies conducting due diligence to determine the capacity for the data recipient to reverse-engineer or "de-anonymize" transmitted consumer data. While Hulu was able to escape liability because it did not have knowledge of the functionality of Facebook's c_user cookie, the opinion itself, with its detailed and intricate analysis of Facebook's c_user cookie, arguably puts future companies on notice that they cannot protect themselves from VPPA liability by simply refraining from asking too many questions about their counterparties' technology. Especially in light of the current regulatory climate pushing companies to exercise more oversight over vendors and publishers on their sites, companies would be better served by proactively taking steps to understand a counterparty's technology and securing the appropriate representation and warranties to confirm their understanding.

Return to Table of Contents

## New Jersey Federal Court Dismisses Claims Against Horizon Healthcare Services Over Members' Data Breach

**A federal district court dismissed FCRA and related claims based on findings that the plaintiffs had not presented sufficient evidence of harm.**

On March 31, 2015, in *In re Horizon Healthcare Services, Inc. Data Breach Litigation*,[9] a federal district judge granted Horizon's motion to dismiss the plaintiffs' putative class action asserting Fair Credit Reporting Act (FCRA) and related state law claims alleging that Horizon failed to safeguard its members' personal and medical information on the grounds that the plaintiffs lacked Article III standing.

### Background

Horizon Healthcare Services, Inc. d/b/a Horizon Blue Cross Blue Shield of New Jersey is a company that provides health insurance products and services to approximately 3.7 million members.

During the weekend of November 1-3, 2013, an unknown thief stole two password-protected laptop computers containing personal, medical and insurance information of more than 839,000 members from Horizon's office. On December 6, 2013, Horizon notified potentially affected members of the theft via letter and press release. Horizon informed its members that the laptops may have contained files with differing amounts of

[9] No. C 11-03764 LB (N.D. Cal. Mar. 31, 2015).

member information and that due to its configuration, Horizon was not certain that all of the member information contained on the laptops was accessible. Horizon offered free credit monitoring and identity theft protection to the affected members.

### The Court's Ruling

Only one of the four named plaintiffs alleged specific harm in the form of a fraudulent tax return and an attempted fraudulent use of his credit card. The three other plaintiffs alleged that they suffered harm based on (1) economic injury, (2) violation of common law and statutory rights and (3) an imminent risk of future harm. The court rejected all three theories of harm.

**Economic Harm.** Citing the 11th Circuit case *Resnick* v. *Avmed*, the plaintiffs asserted standing based on a theory of economic harm. The plaintiffs claimed that they received less than what they bargained for because part of the insurance premium they paid was allegedly allocated for data protection and Horizon did not encrypt all computers.

The court distinguished the case from *Resnick* because the *Resnick* plaintiffs alleged that they were careful in guarding their sensitive information and had never been victims of identity theft before the laptops containing members' personal information was stolen from the defendant corporation in that case. However, within a year of the laptop larceny, the *Resnick* plaintiffs became victims of identity theft. Here, the three plaintiffs did not allege they were careful in guarding their sensitive information, nor did they suffer any other injuries such as identity theft, identity fraud, medical fraud or phishing. Thus, these plaintiffs suffered no economic injury sufficient for standing.

**Violation of Common Law and Statutory Rights.** The plaintiffs also argued that they had standing based on the alleged violation of their common law and statutory rights. The court held that the proper analysis of standing in the Third Circuit is whether the plaintiff suffered an "actual injury" and not whether a statute was violated. Because three plaintiffs alleged no specific harm as a result of Horizon's stolen laptops, they could not rely on mere violations of statutory and common law rights to maintain standing.

**Imminent Risk of Future Harm.** The plaintiffs also claimed that because identity theft could occur at any moment, they faced an imminent risk of future harm sufficient to confer standing. Citing *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), the court held that, by itself, "an increased risk of identity theft resulting from a security breach is insufficient to secure standing" because it relied on the "conjectural conduct of a third party bandit."

The final plaintiff, plaintiff Rindner, alleged that he suffered actual injury because thieves submitted a fraudulent tax return in his and his wife's names and stole their 2013 income tax return. He also allegedly suffered unauthorized charges to his existing credit and debit cards. The court rejected Rindner's standing arguments.

With respect to the joint tax return, the laptop did not contain the personal information of Rindner's wife such that data thieves could have filed a fraudulent joint tax return based on information on the Horizon laptop. While thieves could have conceivably pooled Rindner's personal information with his wife's, obtained from other means, to file the tax return, the court found that Rindner did not plausibly demonstrate a causal connection adequate for standing because he was the only identity theft victim (out of 839,000 members). Rindner's claim also failed on the prong of redressability because he did in fact receive his 2013 tax refund. Thus, Rindner's allegations of false tax returns did not confer standing.

Similarly, the court found that the allegations of fraudulent credit card use failed to establish standing because Rindner did not contest that current credit card information was not on the stolen laptops. Thus, any fraudulent use of those credit cards was not fairly traceable to Horizon.

Therefore, all of the plaintiffs' FCRA claims failed for lack of standing. Because the court lacked discretion to retain supplemental jurisdiction of state law claims without a viable federal claim, the court also dismissed the plaintiffs' state law claims.

### Practice Points

*Horizon* continues the emerging trend of cases holding that generalized allegations of an "increased risk of identity theft" is insufficient to confer standing without evidence indicating that there actually is any imminent use of stolen data. The case also demonstrates that allegations of fraudulent charges and identity theft are not enough. A plaintiff must plead enough evidence to establish a plausible causal connection between the injury and the data breach.

Return to Table of Contents

## President Obama Expands US Cybersecurity Sanctions Regime

**The president's order to enhance the government's ability to punish cyberattackers is another signal that the United States views cyberattacks as a serious threat.**

On April 1, 2015, President Barack Obama issued an executive order authorizing sanctions against foreign individuals or entities engaged in malicious cyberattacks on critical infrastructure. The order responds to a presidential finding that malicious cybe-

ractivities are an "unusual and extraordinary threat to national security, foreign policy and the economy" and is a further demonstration of the administration's concern over cyberthreats against the United States.

The executive order allows the U.S. government to block assets of persons and entities located outside of the U.S. if they are involved in cyberactivities that could threaten U.S. national and economic security interests. The secretary of the Treasury may impose sanctions on persons "responsible for or complicit in, or ... [having] engaged in, directly or indirectly" certain cyberactivities including (1) harming computers that support critical infrastructure, (2) significantly compromising services by a critical infrastructure entity, (3) significantly disrupting the availability of a computer or network, and (4) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers or financial information for commercial advantage or financial gain.

While the president's order may seem broad, its scope is limited by several requirements, including that the cyber-enabled activities must (1) originate from outside the U.S., (2) be "reasonably likely to result in, or have materially contributed to a significant threat" to U.S. national security, foreign policy, economic health or financially stability and (3) be considered "significant." Ultimately, the order is designed to limit its impact on legitimate activities by focusing on the most significant cyberactors. The impact of the sanctions also may be limited by the government's need to keep its sources and methods of uncovering these activities confidential.

For further information and in-depth analysis of the order, see our April 7, 2015, article "President Obama Announces New Cybersecurity Sanctions Regime."[10]

Return to Table of Contents

## NY Department of Financial Services Highlights Concerns Over Data Practices of Third-Party Service Providers

**The Department of Financial Services has reported wide variation in banking institutions' practices, which may spur regulation in this area.**

In early April 2015, the New York State Department of Financial Services issued an update to an earlier report on cybersecurity in the banking sector, focusing on banking institution cybersecurity practices with respect to their third-party service providers. The department has indicated in the past that it views the relationships with third-party vendors as a key "weak link" in financial institutions' cybersecurity efforts, and it likely will use some of the results of the survey to bolster its arguments for issuing requirements in this area.

In preparing the update, the department analyzed the results of its October 2014 survey of banking institution practices[11] and compared that analysis with the National Institute of Standards and Technology's cybersecurity framework, which it identified as a set of baseline principles for cybersecurity issues. The department concluded that, while a large majority of the surveyed institutions indicated that they were taking steps to incorporate the NIST's principles into their policies and practices, progress varied widely. Some of the key findings with respect to the surveyed institutions were:

- In their due diligence of third-party vendors, nearly all have policies requiring a review of the vendor's information security practices, but fewer than half require any on-site assessments, and only 35 percent require periodic on-site assessments of their high-risk vendors.
- 90 percent have information security requirements for vendors, but only some have specific requirements on subjects such as encryption, access controls and data classification, while others merely require compliance with more general standards.
- 21 percent do not require vendors to represent that they have established minimum information security standards, and only 36 percent require that those standards be extended to the vendor's subcontractors.
- 44 percent do not require a warranty that the vendor's products are free of viruses.
- 21 percent do not require a right to audit their third-party vendors.
- 30 percent do not require their vendors to notify them of an information security breach.
- 90 percent use encryption for data transmitted to or from third parties, but only 38 percent use it for data "at rest."
- 63 percent carry insurance that would cover cybersecurity incidents, but only 47 percent have policies that explicitly cover incidents experienced by their third-party vendors.

The department's update does not take a position on whether all or only some of the identified issues would need to be addressed in any future regulation, or whether any of the surveyed institutions were acting improperly. However, the areas of focus by the

[10] Available at: http://www.skadden.com/insights/president-obama-announces-new-cybersecurity-sanctions-regime.

[11] We discussed the survey in our October 2014 issue, available at: http://www.skadden.com/insights/privacy-cybersecurity-update-october-2014.

department highlight key areas of vendor management on which all companies should focus.

Return to Table of Contents

## The FCC Takes on a New Privacy Enforcement Role

**The FCC is becoming more active in privacy enforcement matters, levying a significant fine against an AT&T subsidiary and beginning a rule-making process for the treatment of certain types of customer information.**

On April 8, 2015, the Enforcement Bureau (Bureau) of the Federal Communications Commission (FCC) released an order in which AT&T Services, Inc., a subsidiary of AT&T, agreed to enter into a consent decree with the Bureau over its failure to protect the confidentiality of customer proprietary network information (CPNI). Under the consent decree, AT&T will be required to pay a civil penalty of $25 million and to develop and implement a compliance plan to ensure that it appropriately protects CPNI from future data breaches.

Separately, on April 28, 2015, the Wireline Competition and Consumer & Governmental Affairs Bureaus held a public workshop to explore the application of statutory CPNI protections to broadband Internet access service in light of the FCC's recent net neutrality order.[12] In the order, the FCC reclassified broadband service as a telecommunications service subject to a selected set of FCC rules, among them Section 222 of the Communications Act, as amended, (Section 222) which requires providers to protect CPNI. The workshop was the first step in a planned rulemaking that will revise the FCC regulations regarding CPNI to make them applicable to broadband service providers.

Together, these two events highlight noteworthy shifts in the FCC's approach to privacy oversight and enforcement that could have wide-ranging implications for companies across every layer of the Internet, including Internet service providers, providers of online and cloud services, app developers, content distributors, and others.

### AT&T and CPNI Enforcement

According to Section 222, CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service" and "information contained in the bills pertaining to telephone exchange service or telephone toll service." Examples would include calling records or account information. CPNI is specific to individual customers of a carrier. In the AT&T case, three call center employees accessed thousands of customer accounts without authorization in order to acquire cellular handset unlock codes (unlocking phones is often required for secondary market resale). The employees used customer names and the last four digits of the customers' Social Security numbers to obtain the required codes.

The AT&T consent order provides for the largest fine levied by the FCC to date with respect to a CPNI-related offense and demonstrates the new emphasis on CPNI enforcement at the FCC. Alongside the $10 million Notice of Apparent Liability (NAL) issued by the Bureau to two smaller providers that failed to secure CPNI against public Internet access,[13] and the $7.4 million consent order that Verizon agreed to in September 2014 for using CPNI in marketing campaigns without consumer consent, the $25 million AT&T fine demonstrates the Bureau's new, aggressive approach.

In addition to the fine, the AT&T consent order went beyond previous FCC-imposed privacy regimes. While previous consent orders, such as the Verizon order, focused on compliance with CPNI regulatory obligations, the AT&T order required the company to complete a risk assessment and develop an information security program to protect both CPNI and other categories of consumer personal information. Specifically, the order required AT&T to:

- notify affected customers and offer remediation services;
- designate a senior corporate manager to serve as a CPNI compliance officer;
- within 90 days, complete a risk assessment to identify internal risks of unauthorized access, use, or disclosure of personal information and CPNI by certain employees and vendors;
- within 90 days, develop an information security program designed to protect personal information and CPNI, including administrative, technical and physical safeguards, access controls, breach response plans and vendor-access-specific protections;
- begin ongoing monitoring of compliance with the information security program, including formal compliance reviews;
- improve the information security program where deficiencies are identified, and report non-compliance and future data breaches to the FCC;

[12] This order is more fully described in a Skadden *Insights* article from April 2015 available at: https://www.skadden.com/insights/fcc-acts-again-net-neutrality-awaits-court-challenges.

[13] Discussed in greater detail in our October 2014 issue, available at: https://www.skadden.com/insights/privacy-cybersecurity-update-october-2014.

- develop training materials and a training program for employees addressing the information security program and the company's CPNI obligations; and
- file compliance reports with the FCC at specified milestones over the next three years.

### The Redefinition of CPNI

Meanwhile, in its recent net neutrality order, the FCC stated that Section 222 "remains necessary for the protection of consumers" of telecommunications services, including consumers of both fixed and wireless broadband services. However, it also found that the current rules have focused on concerns associated with voice service. The order is an example of regulations that provide certain enhanced protections for "call detail information," which includes "[a]ny information that pertains to the transmission of specific telephone calls, including [phone number, time, location, or duration of any call]." For this reason, the FCC stated that Section 222 obligations would apply to broadband providers, but refrained from applying the existing regulations until they are appropriately revised to accommodate those technologies.

In the order, the FCC indicated that new CPNI rules should address the many "types of sensitive information to which a provider of broadband Internet access service is likely to have access, such as (to cite just one example) customers' web browsing history." Broadband providers have expressed concerns that the Section 222 definition is broad enough that revised CPNI regulations could impact various uses of customer data, including behavioral advertising. Those providers believe that access to information regarding, for example, web browsing, app usage or network connection history should not be treated in the same manner as call detail information, and that revised CPNI rules should take into account the different business models that prevail in the online economy.

The April 28 meeting began the process through which those revised rules will be drafted. FCC Chairman Tom Wheeler began the session with a brief statement, noting that Congress had given the FCC explicit instructions to protect the privacy of consumer information collected by networks. After a brief technical presentation, two panels followed. In the first, privacy experts discussed the need to apply CPNI regulation to broadband with representatives from consumer groups, academia, and federal and state governments. AT&T argued that broadband providers have less information than many other providers in the Internet ecosystem, and that they need the freedom to be able to provide an advertising-supported business model to compete. The Open Technology Institute, however, suggested that broadband providers are uniquely situated gatekeepers and that unlike, *e.g.*, application providers, consumers have limited ability to choose a provider of broadband services. The panelists discussed a number of practices of potential concern that could be the focus of new CPNI regulation, including deep packet inspection for advertising targeting and Verizon's use of supercookie injection (*i.e.*, inserting a unique user ID into its users' web traffic).

The second panel focused on translating Section 222 into a broadband environment. Industry, nonprofit and academic representatives discussed how to balance the flexibility required to maintain regulations in a rapidly changing technological environment with the need for clear guidance. Public Knowledge suggested that while there might be some difficult cases, the FCC should move expeditiously to provide regulatory protection for information in cases where the parties agree that data constitutes CPNI. Industry representatives, by contrast, argued for a notice of inquiry before any formal rulemaking to explore both the classification of data and ancillary issues such as de-identification standards.

While they were not represented at the initial FCC meeting, third parties that rely on the customer data that broadband providers collect may also now be subject to more stringent regulation. In particular, parties who partner with broadband providers to obtain consumer Internet metadata may be subject not only to provider privacy policies but also legal compliance obligations. For example, in 2013, the FCC issued a Declaratory Ruling finding that CPNI stored on consumer devices may be protected under Section 222 if that information is collected by or at the direction of the carrier and may be accessed or controlled by the carrier or its designee. In the mobile realm, where third-party service providers and app manufacturers often rely on information stored or collected by carriers, this means that any change in the scope of CPNI could require carriers to ensure those third parties' uses of information don't breach the carriers' CPNI compliance obligations.

### Takeaways

The Bureau has recently demonstrated an increasing willingness to pursue public cases against major companies for significant damages. The AT&T case shows that this appetite extends to CPNI cases, while the recent NAL cases show that the FCC is willing to pursue carriers not only for active misappropriation of CPNI but also for the failure to adequately secure that information against misuse by others.

At the same time, the FCC is preparing to consider a major redefinition of CPNI for fixed and mobile broadband. This redefinition, combined with increased enforcement, could subject a wide range of service providers to increased FCC privacy oversight. Service providers across the Internet ecosystem should prepare for the expected rulemaking proceeding in which the FCC will reconsider the scope of the current CPNI definition.

Return to Table of Contents

## NAIC Adopts Cybersecurity Principles, Continues Focus on Cyber Insurance Marketplace

**Insurance regulators have adopted a set of principles on cybersecurity and are seeking information on the types of cyber insurance policies and their coverage.**

While the availability and scope of insurance coverage for cyber losses remains a hot topic for policyholders and insurers alike, regulators also have taken notice and continue to step up their activity and oversight in this rapidly evolving arena. In November 2014, the National Association of Insurance Commissioners (NAIC) formed a special task force to help coordinate insurance issues related to cybersecurity. As described by the NAIC, the Cybersecurity (EX) Task Force is charged with making recommendations and coordinating NAIC efforts regarding the protection of information housed in insurance departments and the NAIC, the protection of consumer information collected by insurers, and the collection of information on cyber-liability policies being issued in the marketplace.

On April 16, 2015, the NAIC adopted the Principles of Effective Cybersecurity Regulatory Guidance.[14] Developed by the Cybersecurity (EX) Task Force and first released in March in draft form for public comment, these principles are intended to help state insurance departments identify uniform standards, promote accountability across the insurance sector, and provide access to essential information.

Citing "ever-increasing cybersecurity issues," in final form, the 12 principles call for the protection of confidential and "personally identifiable consumer information held by insurers, producers and other regulated entities … from cybersecurity risks," mandates "that these entities have systems in place to alert consumers in a timely manner in the event of a cybersecurity breach," "risk-based" regulatory guidance, "minimum … cybersecurity standards … for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks," "appropriate regulatory oversight," including "risk-based financial examinations and/or market conduct examinations regarding cybersecurity," "planning for incident responses by insurers, insurance producers, other regulated entities and state insurance regulators," use of "an information-sharing and analysis organization (ISAO) to share information," and "training … for employees of insurers and insurance producers, as well as other regulated entities and other third parties, regarding cybersecurity."

In tandem with the draft version of the principles, last month the NAIC also released the draft Cybersecurity Insurance Coverage Supplement, developed by the NAIC's Property and Casualty Insurance (C) Committee.[15] In its current form, that document seeks to elicit various information from insurers that write cyber coverage, including, for example, information regarding the number of policies in force (and whether those polices are "claims made" or "occurrence" based), whether policies are provided on a standalone and/or "package" basis, the range of limits offered, premiums written and earned, losses paid and incurred, defense and containment costs paid and incurred, and the availability of "tail" (or run-off) coverage.

The effect of the NAIC's recently adopted Principles of Effective Cybersecurity Regulatory Guidance and final form of the draft Cybersecurity Insurance Coverage Supplement remain to be seen. However, to the extent the NAIC is able to promote the implementation of uniform and even-handed standards, the sharing of essential data while balancing the need to protect sensitive consumer information, and the development and maintenance of a stable marketplace, cyber policyholders and insurers both stand to benefit.

Return to Table of Contents

## Virginia Establishes First State-Level Information Sharing Organization

**Virginia's initiative highlights the growing use of ISAOs as important tools for fighting cyberattacks.**

On April 20, 2015, Gov. Terry McAuliffe announced that Virginia was establishing the United States' first state-level Information Sharing and Analysis Organization (ISAO). ISAOs are intended to act as forums for companies and others to share information on cyber threats and thereby enable the community at large to better identify trends and prepare itself to defend against common attacks. While similar organizations exist at the federal level in the United States — with more likely to come — Virginia is the first state to create its own ISAO to complement existing bodies.

[14] Available at: http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

[15] Available at: http://www.naic.org/documents/committees_c_150312_blanks_proposal.pdf.

Information sharing has become an increasing priority at both the federal and state levels in the United State. As we reported in our February 2015 update, President Obama recently announced a plan to create a federal Cyber Threat Intelligence Integration Center to complement the existing array of ISAOs and also issued an executive order directing the secretary of homeland security to encourage the development and formation of ISAOs.

Virginia's actions to establish its own ISAO reflect a growing trend. Various states — including New York and California — have shown increasing initiative in this area through their regulatory regimes and other means. As national and state policymakers continue to see benefits in promoting the sharing of information, it seems likely that other states will follow Virginia's lead and create their own ISAOs.

Return to Table of Contents

## Contacts in the Privacy and Cybersecurity Group

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

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

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

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

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

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

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

**Helena J. Derbyshire**
Partner / London
44.20.7519.7086
helena.derbyshire@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