May 2015

Skadden

# Privacy & Cybersecurity Update



## Second Circuit Rules Patriot Act Does Not Authorize Bulk Metadata Collection; Congress Reconsiders Certain Patriot Act Authorities

**In *ACLU v. Clapper*, the Second Circuit holds that Section 215 of the USA Patriot Act does not permit the wholesale collection and storage of certain telecommunications metadata, calling into question the viability of existing intelligence collection programs as Congress prepares to revisit that portion of the statute.**

On May 7, 2015, amidst the ongoing Congressional debate surrounding reauthorization of three provisions of the Patriot Act, the Second Circuit decided in *ACLU v. Clapper* that Section 215 of the Act does not authorize the National Security Agency's (NSA) telephone metadata collection program. With all three provisions expiring on May 31, 2015, the Senate met that day to determine whether to let those authorities expire, modify them or extend those provisions briefly while the debate continues. As a result of a procedural block by Sen. Rand Paul of Kentucky, the authorities expired, but Congress is expected to vote again on these issues during the first week of June 2015.

The NSA program first came to light in June 2013 based on information leaked by former government contractor Edward Snowden. Under the program, telecommunications operators are ordered to produce to the NSA all telephone metadata for calls within the U.S. or from the U.S. to foreign points on a daily basis. This collection is performed pursuant to Section 215, which authorizes the government to collect "any tangible things" shown to be "relevant to an authorized investigation" of terrorism or espionage. The government then uses the resulting metadata database as the underlying source queried for information that it suspects is related to specific terrorist organizations.

The *Clapper* court vacated the district court decision upholding the program and found that the government's reading of the statute ignores the statutory requirement that Section 215 collection be relevant to an "authorized investigation." According to the court, this language "contemplates the specificity of a particular investigation — not the general counterterrorism intelligence efforts of the United States government." Bulk metadata collection, by contrast, allows the government to collect information and store it until there is a need to search the collected database "in connection with a hypothetical future

inquiry." This, the court said, is an "unprecedented and unwarranted" understanding of what constitutes relevance to an investigation.

In the wake of the *Clapper* decision, Congress has continued to debate reform of the existing metadata collection program. In mid-May 2015, the House of Representatives passed versions of the USA Freedom Act, a bill that would reform certain Section 215 collection authorities and allocate certain collection responsibilities to telecommunications carriers. The bill was supported by Democrats and libertarian Republicans but faced opposition from law-and-order Republicans and federal law enforcement and intelligence agencies. On May 23, 2015, the Senate failed to overcome a filibuster of the most recent version of the bill, leading to a rare Sunday legislative session on May 31, 2015, intended to broker a compromise. While the Senate voted 77-17 to take up the latest House bill, a procedural block by Sen. Paul ensured that the bulk data collection program will lapse, along with the other provisions up for renewal, until the bill itself can be voted upon during the first week of June 2015. Even assuming the Freedom Act passes, however, the *Clapper* decision will stand as a potential complication for other government bulk data collection programs going forward.

Return to Table of Contents

## SEC Issues Cybersecurity Guidance for Investment Companies and Advisers

**Registered investment companies and advisers should be conducting periodic cybersecurity assessments, taking measures to protect data and respond to data breaches, and memorializing these practices in written policies and procedures.**

In late April 2015, the Securities and Exchange Commission (the SEC) Division of Investment Management issued a guidance update[1] (the Update) identifying the cybersecurity of registered investment companies and registered investment advisers as an important issue and detailing measures that may be taken to address cybersecurity risks.

### Background

The Update is part of the SEC's ongoing Cybersecurity Initiative and draws from conversations with fund boards and senior management at investment advisers, the Office of Compliance Inspections and Examinations' review of investment adviser cybersecurity practices and the SEC's Cybersecurity Roundtable in March 2014.[2] The SEC noted that findings from its outreach efforts and cyberattacks on a number of financial services firms highlight how important it is that firms review their cybersecurity policies.

Earlier this year, the SEC completed its initial cybersecurity examination sweep of certain registered broker-dealers and registered investment advisers. On February 4, Vincente Martinez, chief of the Office of Market Intelligence in the SEC's Enforcement Division, indicated at the FINRA/SIFMA Cybersecurity Conference that the SEC will conduct additional exams focusing on IT controls of a smaller group of firms.

### New Guidance

The Update provides a number of specific measures firms may consider implementing to protect confidential information, including information about fund investors and advisory clients. The Update recommends that firms (1) conduct periodic assessments to identify cybersecurity threats and areas of vulnerability in order to prioritize and mitigate risk, (2) create a strategy designed to prevent, detect and respond to cybersecurity threats, and (3) adopt written policies and procedures to implement the strategy.

**Periodic Assessments.** The Update recommends that firms conduct periodic assessments in the following areas:

- the nature, sensitivity and location of information that firms collect, process and/or store, and the technology systems used;
- internal and external cybersecurity threats to, and vulnerabilities of, firms' information and technology systems;
- security controls and processes currently in place;
- the impact, should the information or technology systems become compromised; and
- the effectiveness of the governance structure for the management of cybersecurity risk.

**Strategy Elements.** The Update notes that a strategy to address cybersecurity threats could include:

- controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation, and system hardening;
- data encryption;

[1] The full text of the Update is available at http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[2] For a more in-depth discussion of the Cybersecurity Initiative, see page 3 of our April 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_April_2014.pdf. For a more in-depth discussion of the review, see page 4 of our February 2015 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_February_2015.pdf.

- protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data or other unusual events;
- data backup and retrieval;
- the development of an incident response plan; and
- routine testing of any strategy.

**Cybersecurity Policies and Procedures.** In order to implement a cybersecurity strategy, the Update recommends that firms adopt written policies and procedures and provide training to employees regarding the strategy. The Update also notes that firms may take a proactive stance toward investors and clients and educate them on ways to reduce cybersecurity threats to their accounts.

### Conclusion

The SEC views cybersecurity and a firm's compliance obligations under the federal securities laws as closely connected. Cybersecurity threats can impact a firm's ability to comply with certain federal securities laws, and as a result firms should examine their ability to respond to cybersecurity threats in that context. For example, policies and procedures that address cybersecurity threats as it relates to other compliance areas such as identity theft and data protection, fraud, and business continuity and other disruptions also may improve a firm's ability to meet its compliance obligations in those areas. The Update suggests that firms examine their cybersecurity vulnerability as it relates to the use of service providers and adopt protective measures as necessary.

Recognizing that every firm is different and vulnerabilities are inevitable, the SEC suggests that firms consider their particular circumstances and plan accordingly to develop a response capability to mitigate potential damage to investors, clients and compliance obligations. Cybersecurity will be a continuing area of SEC focus and concern, and firms should prepare accordingly.

Return to Table of Contents

## US Enters Into Cybersecurity Alliances with Japan, South Korea and Gulf Cooperation Council Member States

**White House focus on information sharing as a means of enhancing cybersecurity leads to pacts with Japan, South Korea and Gulf Cooperation Council member states.**

The United States has taken significant steps over the past two months to further its goal of establishing international partners in promoting Internet freedom and cybersecurity.[3] On April 28, 2015, the U.S. and Japan announced they had entered into a cybersecurity alliance. This new pact was quickly followed by two more. On May 14, 2015, the U.S. and the Gulf Cooperation Council (GCC), represented by Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates, pledged to work together on cybersecurity initiatives as part of a broader security pact.[4] And on May 18, 2015, the U.S. and South Korea committed to cooperating closely on cyberspace issues.[5]

In entering into these pacts, the White House cited the sophisticated cyberattacks mounted against the United States by China, Iran and North Korea. China has engaged in a substantial, systematic operation involving economic cyberwarfare and digital theft, with significant financial and security-related repercussions for the United States.[6] The U.S. government also identified North Korea as being responsible for the hacking of Sony Pictures Entertainment. Iran has similarly been identified as deploying cyberwarfare tactics against the United States and other nations, including the 2012 attack on the Saudi oil company Saudi Aramco.[7]

Given this context, Japan, South Korea and the GCC member states are strategic and logical choices to be cybersecurity allies in that, like the United States, all have a vested interest in stemming the waves of cyberattacks from threatening neighbors. Thus, in addition to consulting with GCC member states on best practices related to cybersecurity, the United States also will provide GCC member states with additional security assistance and guidance on establishing critical infrastructure related to cybersecurity. The U.S.-Japan alliance envisions an information exchange related to cyberthreats as well as ongoing collaboration to establish "cyber norms" to which nations worldwide can commit.[8] Such cyber norms will be directed toward promoting global stability in cyberspace.

[3] *See* White House Summit on Cybersecurity and Consumer Protection, "The Five Things You Need to Know: The Administration's Priorities on Cybersecurity," available at https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit.

[4] *See* "Annex to U.S.-Gulf Cooperation Council Camp David Joint Statement," available at https://www.whitehouse.gov/the-press-office/2015/05/14/annex-us-gulf-cooperation-council-camp-david-joint-statement.

[5] *See* text of Secretary of State John Kerry's remarks, "An Open and Secure Internet: We Must Have Both," available at http://iipdigital.usembassy.gov/st/english/texttrans/2015/05/20150518315742.html#axzz3bow9KEF5.

[6] *See* "FACT SHEET: U.S.-Japan Cooperation for a More Prosperous and Stable World," available at https://www.whitehouse.gov/the-press-office/2015/04/28/fact-sheet-us-japan-cooperation-more-prosperous-and-stable-world.

[7] *See* "Annex to U.S.-Gulf Cooperation Council Camp David Joint Statement."

[8] *See* "U.S.-Japan Cooperation for a More Prosperous and Stable World," available at https://www.whitehouse.gov/the-press-office/2015/04/28/fact-sheet-us-japan-cooperation-more-prosperous-and-stable-world.

In its domestic cybersecurity initiatives, the Obama administration has focused on information sharing among governmental agencies and consumer organizations. These pacts demonstrate that the administration is pursuing a similar cybersecurity strategy internationally.

Return to Table of Contents

## Court Denies Policyholder Coverage for Data Breach: *Recall Total Information Management, Inc. v. Federal Insurance Company*

**The Connecticut Supreme Court finds that loss of tapes containing personal data does not constitute a personal injury covered by a commercial general liability policy.**

In *Recall Total Information Management, Inc. v. Federal Insurance Co.*[9], the Connecticut Supreme Court affirmed and adopted an appellate court decision that a commercial general liability insurance policy did not cover costs incurred by the policyholder due to a data breach. This case is significant in that it is one of the first data breach insurance coverage cases to result in an appellate-level decision, but due to the unusual circumstances surrounding the breach, the decision may not provide clear guidance as to how insurance policies will be interpreted in relation to more typical data breaches. In this case, hackers did not gain unauthorized access to the information on a computer system. Instead, tapes containing the data fell out of the back of a truck and onto a highway and subsequently disappeared.

### Background

IBM had hired Recall Total Information Management, Inc., which later subcontracted with Executive Logistics, Inc., to transport and store electronic media for the company. In February 2007, Executive Logistics was transporting the tapes from an IBM facility to another location when a number of tapes containing IBM employee information fell out of the back of the Executive Logistics truck. Approximately 130 tapes containing the personal information of 500,000 past and current IBM employees were removed from the roadside by an unknown individual and never recovered. The information included the employees' Social Security numbers, birthdates and contact information. Following the breach, IBM notified the potentially affected individuals, established a call center and offered them one year of credit monitoring. IBM incurred over $6 million in expenses in its effort to mitigate any potential harm from the breach.

IBM and Recall entered into a settlement agreement pursuant to which Recall reimbursed IBM for certain costs arising from the breach, and Recall later sought to be indemnified by Executive Logistics. Executive Logistics filed an insurance claim against a $2 million commercial general liability policy and a $5 million umbrella liability policy. The insurers denied the claim and, after Executive Logistics assigned the policy claim to Recall, Recall brought suit against the insurers seeking recovery under the insurance policies, which both contained personal injury coverage provisions.

Recall claimed that the loss of the tapes constituted a personal injury under the policy. The definition of personal injury under the policies included "injury, other than bodily injury, property damage or advertising injury, caused by an offense of ... electronic, oral, written or other publication of material that ... violates a person's right to privacy." Recall asserted that the loss and later theft of the tapes by an unknown third party constituted a personal injury and Recall should be able to recover the cost of notifying the affected persons and providing credit monitoring services.

### Decision

The appellate court denied Recall recovery under the insurance policies. The analysis centered around whether the information was ever "published." The appellate court declined to decide what definition of publication would be proper to apply; however, the court did decide that access is a "necessary prerequisite" for publication. Because there was no evidence provided that indicated the tapes had ever been accessed, the court found that there could be no publication. The court further noted that IBM itself had stated that there was no indication that the information on the tapes were readable by personal computers or that they had been accessed by anyone for any improper use. The appellate court also declined to decide whether the data breach notification laws required IBM to provide affected individuals with assistance beyond notification (*e.g.*, credit monitoring). The court noted that merely triggering a notification statute did not create a personal injury.

### Conclusion

Ultimately, the unique fact pattern in *Recall Total Information Management, Inc.* may minimize its precedential value for future, more standard data breach cases in which a third party gains unauthorized access to personal data. However, the case does highlight the need for companies to consider potential data breach scenarios in light of their business practices and to carefully review their insurance coverage to assess whether their coverage applies to those scenarios.

Return to Table of Contents

[9] *Recall Total Information Management, Inc. v. Federal Insurance Co.*, No. 19291, 2015 WL 2371957 (Conn. May 26, 2015).

## California Insurer Alleges Failure to Follow Best Practices Invalidates Cyber Liability Coverage

**An insurance company alleges it has no obligation to provide coverage since the insured failed to take standard preventive actions as required under the policy.**

On May 7, 2015, Columbia Casualty Company filed one of the first lawsuits seeking to deny coverage under a cyberinsurance policy based on the inaction of the insured.[10] In connection with a 2013 data breach that left 32,500 confidential medical records accessible online, Cottage System settled a class action lawsuit for $4.125 million. Columbia Casualty agreed to fund the settlement but reserved all of its rights. It then filed suit against Cottage Systems. In its suit, filed in federal court in the Central District of California, Columbia Casualty seeks to recoup the settlement funds and attorneys' fees and costs paid out in connection with the suit.

### Background

Columbia Casualty claims it is not obligated to cover the costs due to an exclusion in Cottage's policy for "failure to follow minimum required practices." According to the complaint, the data breach was caused by the fact that Cottage failed to undertake standard preventive actions, including the following:

- regularly check and maintain security patches;
- regularly reassess its information security exposure and enhance risk controls;
- have a system in place to detected unauthorized access or attempts to access sensitive information on its servers; and
- control and track all changes to its network to ensure it remains secure.

The complaint also alleges that Cottage failed to "continuously implement the procedures and risk controls identified" in its insurance application, highlighting the importance of accuracy during the insurance application process.

### Takeaways

Many cyberinsurance policies include vague language requiring the insured to meet "minimum required standards." *Columbia Casualty* may be the first case to test what that standard actually means.

The case also highlights the importance of carefully reviewing cyberinsurance policies to ensure that these types of exclusions are eliminated entirely or defined more precisely. Companies should continuously monitor and ensure compliance with their own internal cybersecurity policies and procedures so that they satisfy their insurance requirements.

Return to Table of Contents

## FTC's Brill Claims Jurisdiction Over Internet of Things

**The FTC seeks to reinforce its claim of broad powers to regulate cybersecurity matters even in the absence of a specific mandate.**

In a keynote address at the EuroForum European Data Protection Days conference on May 4, 2015, Commissioner Julie Brill of the Federal Trade Commission (FTC) stated that the FTC's enforcement powers extend to addressing the data privacy risks that accompany the growing web of Internet-connected devices, known as the Internet of Things (IoT). As we have previously noted,[11] the Internet of Things includes all manner of physical devices that collect information and transmit it over the Internet — examples include heart monitors that post information to social media, thermostats that collect information on consumers' use of their home in order to better regulate heat and air conditioning use, and road sensors that collect and transmit traffic information to transportation agencies. Brill said that in the absence of a specific privacy law addressing the IoT, the FTC's powers under Section 5 of the FTC Act to prevent deceptive and unfair trade practices include the power to police the data collection, retention and protection practices of the IoT. Brill urged the industries that make up the IoT to develop their own best practices to avoid enforcement actions by the FTC.[12]

Brill identified some of the unique policing challenges posed by the IoT. For example, she noted that the sheer number of networked devices has exceeded 25 billion and is expected to reach 50 billion by 2020, and that the more devices there are, the more sensitive data they will collect. In addition, many devices increasingly lack a user interface, making it more difficult for consumers to know when data is being collected or to exercise control over that collection. These remarks echo the findings of the FTC in the report it released in January 2015 regarding the Internet of Things.[13]

[10] The case is *Columbia Casualty Company v. Cottage Health Systems*, Case No. 2:2015cv03432, Central District of California, filed May 7, 2015.

[11] See our January 2015 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_January_2015.pdf.

[12] A transcript of Brill's remarks can be found at https://www.ftc.gov/system/files/documents/public_statements/640741/2015-05-04_euroforum_iot_brill_final.pdf.

[13] For a more detailed discussion of this report, see our January 2015 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_January_2015.pdf.

### Dissent

Not all FTC commissioners agree with Brill's remarks. Soon after Brill gave the keynote address, Commissioner Joshua Wright, in a speech to the U.S. Chamber of Commerce, criticized the FTC for failing to conduct an appropriate cost/benefit analysis before imposing regulations (and their attendant costs).[14] Wright said that regulations should only be imposed when there is a specific harm to consumers, and that the approach currently being pursued by the FTC, which Wright called "regulat[ing] by slogan," will stifle innovation. Wright had also filed a dissenting statement to the issuance of the FTC's IoT report in January 2015 that identified these same concerns, noting that he dissented from publication of the report because it "includes a lengthy discussion of industry best practices and recommendations for broad-based privacy legislation without analytical support to establish the likelihood that those practices and recommendations, if adopted, would improve consumer welfare."[15]

### FTC Authority Under Fire

Given the apparent disagreement among some of the commissioners regarding the appropriate level of regulation of the IoT, some question why Brill chose to make such a strong statement with respect to the FTC's authority. There are at least two possible explanations.

First, the safe harbor program under the European Commission's Directive on Data Protection, which allows European Union (EU) data to be transferred to the United States under certain circumstances, is again under fire as a result of a case heard in March 2015 before the Court of Justice for the EU, in which the plaintiff, privacy activist Maximilian Schrems, alleges that U.S. laws and practices do not adequately protect the personal information of EU citizens. A nonbinding opinion by the court's advocate general is to be published on June 24, 2015, with a final verdict to be issued thereafter. The final verdict could have far-reaching implications for U.S. companies that rely on the safe harbor to conduct their business on a day-to-day basis. Brill may have been seeking to reassure her European audience that the U.S. does, in fact, have a robust data protection regime through the FTC's Section 5 enforcement regime.

Second, the scope of the FTC's powers in the cybersecurity area and, specifically, its authority to bring suits in federal court regarding new unfair or deceptive practices without having first promulgated formal regulations or pursued administrative resolution, continues to be questioned in the course of the FTC's case against Wyndham Hotels and Resorts, LLC, which is currently before the U.S. Court of Appeals for the Third Circuit.[16] The Third Circuit heard oral arguments in the case on March 3, 2015, and the outcome could have a significant impact on both the scope of the FTC's authority and companies looking for guidance with respect to that authority. While that case is pending, Brill's remarks regarding the IoT demonstrate her commitment to the position that the FTC does have the authority under Section 5 to define and bring actions against unreasonable cybersecurity practices even in the absence of having issued formal regulations regarding such practices.

Return to Table of Contents

## FCC Expects to Begin Broadband Privacy Enforcement Activities This Month

**The FCC issued an enforcement advisory indicating that it will not wait for revised privacy rules to begin reviewing the activities of broadband providers subject to the recent net neutrality order.**

On May 20, 2015, the Federal Communications Commission (FCC) Enforcement Bureau issued an enforcement advisory suggesting that broadband providers take "reasonable, good faith steps to protect consumer privacy." According to the FCC guidance, the agency expects to apply the provisions of Section 222 of the Communications Act to broadband providers when the agency's recent net neutrality order (the Order) goes into effect (which may be as early as June 12, 2015, barring a stay). As a result, failure to protect customer proprietary network information (CPNI) could result in enforcement actions against those providers.

Our April 2015 *Privacy & Cybersecurity Update* noted that the Order laid the groundwork for enforcement of Section 222 CPNI obligations against providers of "broadband Internet access service" — *i.e.*, providers of fixed and mobile broadband covered under the Order. Last month's newsletter also noted that the FCC has started requesting public input on a rewritten set of CPNI regulations that apply more directly to broadband-related information. However, the new enforcement advisory makes it clear that providers of broadband services cannot wait for the new CPNI rules to be promulgated; the Enforcement Bureau is preparing to engage with such providers as soon as the Order

[14] A transcript of Wright's remarks can be found at https://www.ftc.gov/system/files/documents/public_statements/644381/150521iotchamber.pdf.

[15] The text of Wright's dissent can be found at https://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf.

[16] For background on this case, see our *Privacy & Cybersecurity* updates from December 2013, February 2014, April 2014 and June 2014.

takes effect. Indirectly, third parties that rely on the customer data that such providers collect also now may be subject to more stringent privacy enforcement.

The new FCC guidance indicates that between the effective date of the Order and any subsequent guidance or adoption of regulations, the Enforcement Bureau will review broadband providers' reasonable, good-faith privacy protection activities to ensure that they employ "effective privacy protections in line with their privacy policies and core tenets of basic privacy protections." While prior decisions implementing the existing CPNI regulations will not necessarily be binding on broadband providers, the Enforcement Bureau expects to provide informal as well as formal guidance on broadband CPNI protections. In addition, as discussed in the Order, broadband providers may request advisory opinions from the Enforcement Bureau on their activities. According to the enforcement advisory, "the existence of such a request for guidance will tend to show that the broadband provider is acting in good faith."

Return to Table of Contents

## RadioShack Agrees to Limit Sale of Customer Information in Bankruptcy

**Deal reached with 38 state attorneys general strictly limits data that may be sold.**

RadioShack Corp. reached a deal this month that will allow it to sell a very limited portion of its customer data to General Wireless Inc. as part of its bankruptcy proceedings, subject to certain restrictions on the future use of such information by General Wireless.

As reported in our April 2015 *Privacy & Cybersecurity Update*, RadioShack had planned to auction off its customer data in an effort to satisfy its creditors but was met with strong opposition from numerous state attorneys general and consumer protection bodies, as well as the FTC's Bureau of Consumer Protection. Ultimately, 38 state attorneys general joined together to voice concerns about the sale. The opposition focused on the fact that the stringent privacy policy under which the data was collected stated that RadioShack "will not sell or rent [customers'] personally identifiable information to anyone at any time."[17]

The deal that was approved on May 20, 2015, by U.S. Bankruptcy Judge Brendan Shannon will allow the sale of email addresses provided by customers that have requested product information during the past two years; however, those customers will be given one week to opt out of the transfer of their data to General Wireless. In addition, once General Wireless receives the data of those customers who do not opt out, it is prohibited from selling or disclosing any of that data to any other entity, including Sprint Corp., with which General Wireless has said it intends to co-brand some of the RadioShack locations that it is also purchasing. This restriction on General Wireless is designed to fulfill the original promise RadioShack made to its customers when it collected the data. RadioShack must destroy all remaining data that it collected from some 117 million customers over the years, including credit card information, Social Security numbers, telephone numbers and dates of birth.

### Takeaways

While the RadioShack data sale takes place in the context of a bankruptcy, given the widespread participation by state attorneys general, other consumer protection organizations and the FTC, it is likely to serve as a precedent for other transactions in which consumer data may be sold, such as mergers and acquisitions. Accordingly, all companies should review their privacy policies to ensure that, in addition to accurately reflecting the company's current use of the data, the policy also preserves the company's flexibility to disclose the data in connection with any future sale of the related business, whether in bankruptcy or an acquisition. If a company has already collected consumer data under a policy that would not allow such a disclosure, the company should consider amending its policy or take measures to flag such data for different treatment in the event of a future sale.

Return to Table of Contents

## Nevada Expands Definition of Personal Information

**New definition includes information that can be used to access any type of online account.**

Nevada's data breach notification and data security law has been amended to expand the definition of personal information. Effective July 1, 2015, "personal information" includes (1) an individual's unencrypted first name or first initial and last name, plus (2) any of the following unencrypted data elements: an individual's medical identification number or health insurance identification number, or a username, unique identifier or email address in

[17] For further background, please see our April 2015 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_and_Cybersecurity_Update_April_2015.pdf.

combination with a password, access code or security question and answer that would permit access to an online account.[18]

With the amendment, Nevada joins California and Florida as states that define personal information for data breach notification purposes to include usernames and passwords that allow access to any type of online account. Many states define personal information to include unique identifiers and passwords that would permit access to online financial accounts but do not address information that would allow access to other types of online accounts.[19]

Return to Table of Contents

## Connecticut Enacts New Employee Online Privacy Law

**Employers may not require Connecticut employees or job applicants to provide access to personal online accounts.**

On May 19, 2015, Connecticut signed into law Public Act No. 15-6, titled "An Act Concerning Employee Online Privacy" (Online Privacy Act), which prohibits employers from requiring or requesting employees and job applicants to provide access to exclusively personal online accounts, including email, social media or retail-based Internet websites.[20] The law goes into effect on October 1, 2015. Connecticut joins at least 20 other states with similar statutes.

The Online Privacy Act, among other things, prohibits employers from requiring or requesting employees or applicants to: (1) provide usernames, passwords or other means to access a personal online account, (2) authenticate or access a personal online account in the presence of a representative of the employer, or (3) invite the employer, or accept an invitation from the employer, to join a group affiliated with the employee's personal online account. In addition, employers may not take adverse action against an employee or applicant for refusing to engage in, or for filing a complaint about, the prohibited activity. The Online Privacy Act contains an exception which allows employers to conduct investigations if the employer receives information regarding activity on a personal online account for the purpose of complying with applicable laws, regulations or prohibitions against workplace misconduct, or for protecting the employer's proprietary, confidential or financial information.

In the event of an employer's violation, employees or applicants may file a complaint with the commissioner of the Connecticut Department of Labor. The commissioner may levy fines of $500 for the first violation and $1,000 for each subsequent violation, order reinstatement, back pay, reinstatement of employee benefits and other relief as the commissioner deems appropriate. While employees and job applicants may not file a lawsuit in court, they may appeal the commissioner's decision to the Connecticut Superior Court.

### Takeaway

Companies should revisit their human resources policies and procedures and make revisions as necessary prior to October 1, 2015, to ensure they are in compliance with the Connecticut Online Privacy Act.

Return to Table of Contents

## Virginia Becomes First State to Mandate Enhanced Payment Security for State Transactions

**Virginia mandates use of chip technology for payment card transactions between citizens and state agencies.**

On May 5, 2015, Virginia Gov. Terry McAuliffe signed Executive Directive 5 — Securing Consumer Transactions, which mandates the use of payment technology designed to reduce fraud in transactions between citizens and state agencies and institutions.[21] The Executive Directive mandates that the state's main purchase card program use advanced chip authentication security features by December 2015.

[18] The text of Assembly Bill No. 179, which was signed into law on May 13, 2015, can be found at http://www.leg.state.nv.us/Session/78th2015/Bills/AB/AB179_EN.pdf.

[19] See, *e.g.*, Alaska, Iowa, Kansas, Massachusetts, Missouri, Nebraska, New York, North Carolina, North Dakota, Oregon, South Carolina, Vermont, Wisconsin and Wyoming.

[20] The text of Senate Bill No. 426, which was passed into law, may be found at http://www.cga.ct.gov/2015/FC/2015SB-00426-R000292-FC.htm.

[21] The text of the executive directive may be found at https://governor.virginia.gov/media/3811/ed-5-securing-consumer-transactions.pdf.

This requirement is in line with the standards set forth in President Barack Obama's executive order on Improving the Security of Consumer Financial Transactions issued in October 2014, which requires federal agencies to use chip and pin security features on payment cards for federal programs.[22]

The Virginia directive also mandates that by December 2015, all of the state's merchant and prepaid debit card programs include enhancements with respect to user authentication, confidentiality, cardholder reporting of suspected fraudulent transactions and data breach reporting and notification.

The executive directive makes Virginia the first state to align its state payment card security features with the federal standards.

Return to Table of Contents

[22] For further information on this executive order, see our October 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_and_Cybersecurity_Update_October_2014.pdf.

## FBI Creates New Role to Focus on Cybercrime

**New position functions as COO of the Criminal, Cyber, Response and Services Branch.**

The FBI announced that it has established a new role to coordinate its response to cybercrime: the associate executive assistant director for the Criminal, Cyber, Response and Services Branch (CCRSB). The FBI said in a statement that the position is the equivalent of the chief operations officer of the CCRSB, and one of the main responsibilities of the position will be coordinating with federal, state and local law enforcement agencies. The first person to serve in the position will be Joe Demarest, who was formerly the assistant director of the FBI's Cyber Division.

## Contacts in the Privacy and Cybersecurity Group

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

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

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

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

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

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

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

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

**James S. Talbot**
Counsel / New York
212.735.4133
james.talbot@skadden.com

**Joshua F. Gruenspecht**
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com



Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000