Skadden

Privacy & Cybersecurity Update

FCC Prepares to Issue Rulemaking on Privacy for Internet Service Providers

The Federal Communications Commission is preparing to rework the privacy rules that apply to providers of broadband services, making good on a promise made in its net neutrality order over a year ago.

On March 31, 2016, at its open meeting, the Federal Communications Commission (FCC) voted 3-2 along party lines to launch a notice of proposed rulemaking (NPRM) to establish privacy rules for broadband Internet service providers (ISPs). The NPRM is expected to be issued in the coming weeks and will lay the groundwork for a new privacy regime applicable to ISPs under the auspices of the FCC's authority to regulate access to customer proprietary network information (CPNI). Under the FCC's rules, CPNI is information collected by a service provider relating to a customer's use of a service (*e.g.*, session data, etc.). The extension of CPNI regulations to broadband services providers would represent a stark departure from the scope of the FCC's current regulations, which apply only to providers of traditional telephone voice services. The proposed FCC CPNI rules are expected to require ISPs to disclose how CPNI is used, take steps to protect that information and notify affected customers within 10 days of discovering a data breach. Once an order is issued, the new FCC rules can be expected to be significantly more stringent than the current privacy rules for ISPs overseen by the Federal Trade Commission (FTC).

Background

In the FCC net neutrality order in February 2015, in which the agency extended its authority to broadband providers, the commission left open the applicability of a number of its rules to ISPs. The FCC wrote in the order that CPNI rules "remain[] necessary for the protection of consumers," including consumers of both fixed and wireless broadband services. However, because existing rules had been written to protect consumers of traditional telephone voice services, the FCC refrained from applying existing CPNI rules to broadband providers at that time. The agency has spent the last

year holding hearings, studying the issue and preparing to revisit its regulations to accommodate broadband technologies.[1]

The NPRM

FCC Chairman Tom Wheeler circulated drafts of the NPRM in preparation for the March 31, 2016, meeting for the last several weeks. In a fact sheet released on March 10, 2016, he laid out the framework of his proposal. In brief, it would:

- **Separate the customer usage data collected by ISPs into three broad categories, each with its own rules for sharing and use.** Customer data necessary to provide service and data that broadband providers use to market the same types of broadband services purchased by the consumer would be deemed usable by ISPs at all times. Customer data used by broadband providers and shared with their affiliates for the purpose of marketing other communications-related services would be useable by ISPs unless the customer opts out. All other uses and sharing of customer data by ISPs would be permitted only if the customer expressly opts in.
- **Require broadband providers to take reasonable steps to safeguard customer information from unauthorized use or disclosure.** At a minimum, Chairman Wheeler's proposal would include adoption of risk management practices, personnel training practices and authentication requirements; identification of a senior manager responsible for data security; and allocation to ISPs of responsibility for use and protection of customer information when shared with third parties.
- **Require ISPs to notify customers and federal agencies of breaches.** The chairman's proposal would require ISPs to notify affected customers of data breaches within 10 days, and to notify the FCC, FBI and Secret Service within seven days of any breach affecting more than 5,000 customers.

In the fact sheet, Chairman Wheeler specifically disclaimed any intent to regulate edge service providers, such as Google, Facebook and Twitter, which remain under the authority of the FTC. Broadband providers had likewise suggested that the FCC follow the FTC's lead in drawing up its new CPNI rules. Specifically, the industry had suggested that the FCC identify privacy goals and then pursue providers for unfair or deceptive conduct inconsistent with those goals. However, the fact sheet suggests the chairman's belief that additional privacy protections are necessary vis-à-vis ISPs because of the special relationship they have with consumers: "Consumers can move instantaneously to a different website, search engine or application. But once they sign up for broadband service, consumers can scarcely avoid the network for which they are paying a monthly fee."

[1] The FCC statement in the order and the related hearings are discussed in greater detail in our April 2015 *Privacy & Cybersecurity Update*.

Next Steps

The NPRM will reshape the privacy rules that apply to ISPs, but it is only the first official stage of a multiyear process. The NPRM will be followed by a comment period and a reply comment period, and the commission's final rulemaking will likely not appear for at least several months. The effectiveness of the commission's order will be conditioned upon the FCC's success in the ongoing lawsuit over the net neutrality order itself, which permitted the FCC to apply its CPNI authorities to ISPs. Moreover, given the contentiousness of the privacy issue, the final commission order can be expected to be appealed independently.

Return to Table of Contents

European Governing Bodies Begins to Consider Privacy Shield

Although the Privacy Shield was drafted by representatives from the EU and U.S., the complex — and possibly controversial — process of having it approved by EU authorities remains.

As we have discussed in our previous mailings, the newly developed "Privacy Shield," which will replace the U.S.-EU Safe Harbor for transfers of personal data from Europe to the U.S., must still be approved by the EU. For the Privacy Shield to become law, a qualified majority of the Article 31 Committee, composed of EU member state representatives, must issue a binding opinion approving the "adequacy decision" that the European Commission released on February 29, 2016, after which the EU College of Commissioners must formally adopt the decision. On March 17, 2016, the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) held the first round of public hearings on the Privacy Shield. Although European Parliament approval is not a necessary step in the approval process, the LIBE Committee's views are seen as highly influential.

The hearings followed an expected course, with EU and U.S. negotiators stating why the Privacy Shield provided adequate protection for EU residents, and various privacy advocates asserting that the new framework fell well short of its stated goals. Among those challenging the Privacy Shield was Max Schrems, who brought the case against Facebook that ultimately resulted in the invalidation of the Privacy Shield by the Court of Justice of the European Union.

In addition to the LIBE Committee meetings, the Article 29 Working Party, which is comprised of the representatives from the data protection authorities of each EU member state, has

begun its review of the Privacy Shield. The group's nonbinding opinion is expected in mid-April 2016. The group has already signaled two areas of concern regarding the Privacy Shield: first, that there are no rules limiting data retention, and second, that the ombudsperson tasked with overseeing national security access to personal information lacks sufficient power and independence. A report also is expected from the European Data Protection Supervisor, which is an independent supervisory authority responsible for ensuring that European institutions respect privacy rights when they develop new policies.

The highly regarded Article 31 Committee is scheduled to commence its meetings on April 7, 2016.

Return to Table of Contents

Hamburg Data Protection Authority Takes Hard Line Stance on Companies Still Using Safe Harbor

While many expected the European data protection authorities to forego any regulatory action against companies that continued to rely on the Safe Harbor while the Privacy Shield is being debated, at least one German DPA is not taking that approach.

In October 2015, after the Court of Justice of the European Union invalidated the then-current Safe Harbor framework agreement between the EU and U.S. in Schrems v. Data Protection Commissioner, the European data protection authorities (through their Article 29 Working Party) announced that they would not take any enforcement action against companies that continued to rely on the Safe Harbor through the end of January 2016. This was to provide EU and U.S. officials with the opportunity to hammer out a replacement to the Safe Harbor. The resulting Privacy Shield is undergoing a review process through April 2016, and many assumed that the European authorities would formally or informally extend their nonenforcement commitments until the Privacy Shield was finalized or rejected. At least in Hamburg, Germany, this may not be the case.

Professor Dr. Johannes Caspar, an Article 29 Working Party member and head of the Hamburg data protection authority, has not only questioned the validity of the Privacy Shield but also asked the German Federal Ministry of Justice and Consumer Protection to introduce a regulation that would allow Germany's various data protection authorities to challenge the Privacy Shield in court. More importantly, the Hamburg data protection authority is reported to be imposing Safe Harbor-related fines on three companies and is in the process of investigating others. It is unclear whether these companies are being fined for simply relying on the Safe Harbor or have violated the terms of that now-invalidated law. According to reports, the data protection authority of the German state of Rhineland-Palatinate also is investigating companies that continue to rely on the Safe Harbor.

What Should Companies Do?

To be sure, companies find themselves today in unchartered waters with respect to transborder data flow from the EU to the U.S. When the Safe Harbor was invalidated, most assumed a "grace period" during which there would be no enforcement activity until a replacement (the Privacy Shield) was found. These actions in Germany, and the growing independence of the data protection authorities, suggest that might not be the case. Nonetheless, for companies for which changing over to Standard Contractual Clauses or Binding Corporate Rules is too burdensome, waiting for the dust to settle on the Privacy Shield may still be the best course of action.

Return to Table of Contents

IRS Issues Alert on Phishing Scheme to Obtain Payroll Data

Hackers are using sophisticated phishing attacks to cause companies to disclose their employee and payroll tax data, according to an IRS alert.

The Internal Revenue Service (IRS) recently issued an alert regarding a phishing email scheme in which cybercriminals pose as governmental officials or company executives and request employee payroll and tax data, including W-2s and Social Security numbers, from company payroll and human resources professionals. Where successful, the cybercriminals then attempt to monetize the stolen information by filing fraudulent tax returns seeking refunds on behalf of the individual taxpayers whose data was compromised.

According to the IRS commissioner, this latest phishing scheme is "a new twist on an old scheme using the cover of the tax season and W-2 filings" to trick people into sharing personal tax data. Until recently, tax-based phishing emails largely have been directed at tricking individual taxpayers into releasing their information. By targeting corporations and partnerships holding taxpayer information, hackers can now potentially access far greater amounts of data with a single phishing attack. For companies that inadvertently disclose this information, the fallout can range from reputational harm to liability for damages.

The phishing emails in this scheme typically are drafted as urgent requests by either governmental officials or company executives designed to elicit an immediate response from company payroll and human resources employees. For example, the IRS notes that in some cases, the email will appear to come from the company CEO requesting that employees' W-2s and earnings summaries be forwarded for "a quick review." Like most phishing attacks, these emails appear legitimate, and many already have fallen victim to them.

Practice Points

Companies should — as always — be vigilant of phishing attacks and engage in comprehensive cybersecurity training. Employees who have access to taxpayer information should be directly informed of the IRS alert and instructed to verify any requests they receive for taxpayer information, regardless of how legitimate the message appears. Since these attacks likely will continue for as long as they prove successful, regular and ongoing training is crucial.

Our experience suggests that those engaging in this kind of attack are able to file false tax returns shortly after obtaining the ill-gotten taxpayer information, making it critical that employers take action during the first 24 to 48 hours after a successful cyberattack. While the IRS recently received additional funding to address cybersecurity issues and is focused on meeting this challenge, it remains severely resource-constrained, making it difficult, for example, for the IRS to independently assess the validity of tax returns. For this reason it is important to reach out quickly to the right contacts at the IRS to apprise them of the scam and work with them to flag potentially affected taxpayer accounts. We also advise companies to help individual employees whose information has been compromised seek tax-related identity theft protection, particularly under the IRS' new identity theft safeguards.

Return to Table of Contents

Consumer Financial Protection Bureau Issues First Consent Order Relating to Data Security

The CFPB issued its first consent order in the area of cybersecurity, finding that a firm that allowed money transfers over the Internet had failed to implement adequate data security protections to safeguard sensitive consumer information.

In its first consent order in a data security matter, the Consumer Financial Protection Bureau (CFPB) settled allegations that Dwolla, Inc. was deceptive as to its data security representations and failed to implement adequate data security protections to safeguard sensitive consumer information. Dwolla was required to pay a civil penalty of $100,000 and take other specified actions for a five-year period.

Background

Dwolla is a website through which users can send money to others over the Internet. According to the order, Dwolla stores consumers' sensitive personal information, including users' names, addresses, birthdates, phone numbers and social security numbers. The order stated that Dwolla had approximately 653,000 members and had transferred as much as $5 million per day as of May 2015.

The CFPB is authorized under the Dodd-Frank Act to take action against institutions engaged in unfair, abusive or deceptive acts or practices, or that otherwise violate federal consumer financial laws. The CFPB concluded that Dwolla's statements constituted deceptive acts or practices in violation of the Consumer Financial Protection Act. Specifically, according to the order, the CFPB found that Dwolla misrepresented to consumers that its transactions, servers and data centers were compliant with PCI Security Standards Council standards; failed to employ reasonable and appropriate measures to protect consumer data from unauthorized access; did not encrypt all sensitive consumer information in its possession; did not conduct adequate, regular risk assessments; and did not properly train its employees on data training.

The CFPB issued the consent order despite the fact that no security breach or other data security incident actually occurred, demonstrating that the CFPB is focusing on false representations about data security practices rather than security failings themselves. This is consistent with the approach the FTC — which, to date, has been the most active federal agency in the data security space — has adopted.

Pursuant to the consent order, Dwolla is enjoined from misrepresenting its data security practices and has been required to implement data security measures to properly protect consumers' personal information on its computer networks and applications. Dwolla also is required to enact specific measures to protect such data, including:

- designating a qualified person to coordinate and be accountable for the data security program;
- conducting data security risk assessments twice a year to identify security risks and assess the adequacy of safeguards in place;
- conducting regular, mandatory employee training on data security policies; and

- obtaining an annual data security audit from an independent, qualified third party, using procedures and standards generally accepted in the profession.

Dwolla also is required to retain at least one qualified, independent person with specialized experience in data security to conduct an annual audit of Dwolla's data security practices to validate the effectiveness of the periodic risk assessments Dwolla is required to conduct and to verify that Dwolla has implemented reasonable and appropriate risk mitigation activities to sufficiently safeguard against any identified risks. That individual must provide a written report detailing the audit findings to present to Dwolla's board of directors. Based on the audit report, the board of directors must develop a compliance plan to (i) correct any deficiencies identified and (ii) implement any recommendations or explain in writing why a particular recommendation is not being implemented. The board must then submit both the report and the compliance plan to the CFPB, which the CFPB may accept or revise.

Return to Table of Contents

Department of Defense Releases Cybersecurity Discipline Implementation Plan

The Department of Defense has issued cybersecurity guidelines that, although specific to that government body, provide a useful framework for private companies as well.

In March 2016, the Department of Defense (DoD) published the DoD Cybersecurity Discipline Implementation Plan. The plan was originally issued in October 2015, updated in February 2016, and made public in early March 2016. The plan is organized into sections describing tasks commanders and supervisors are to accomplish along each of four "Lines of Effort." The plan further provides that commanders and supervisors are to measure and report the status of their efforts to implement the tasks based on certain criteria via the Defense Readiness Reporting System (DRRS). Although reporting criteria and DRRS are DoD-specific, the Lines of Effort and related tasks may provide a useful framework for private sector cybersecurity professionals.

The Four Lines of Effort

Strong Authentication

The first Line of Effort involves "[r]educing anonymity as well as enforcing authenticity and accountability for actions on DoD information networks" and "helps prevent unauthorized access, including wide-scale network compromise by impersonating privileged administrators." The principal task commanders and supervisors are directed to implement along this Line of Effort is to ensure 100 percent use of separate public key infrastructure-based authentication/credentials for "any login to a network infrastructure device."

Practice Point: While private companies may not all need such robust authentication methods, every organization should consider authentication a key building block of a cybersecurity program.

Device Hardening

The second Line of Effort directs commanders and supervisors to "prevent common exploitation techniques through proper configuration, vulnerability patching, and disabling active content in emails." Commanders and supervisors are directed to take measures that "are critical to thwarting an adversary's ability to escalate privileges and maneuver freely within a DoD enclave." These measures include ensuring that (i) all servers and network infrastructure devices are compliant with vulnerability patches, (ii) all systems running Windows XP and Windows Server 2003 operating systems are removed or upgraded to newer operating systems, and (iii) all HTML and rich-text formatting is disabled for Outlook email clients on DoD information networks and for government-provided email services on commercial mobile devices.

Practice Point: Companies should stay up to date with patches and cybersecurity updates. Failing to do so often leads to security vulnerabilities.

Reduce Attack Surface

The third Line of Effort is aimed at reducing the attack surface, which involves "eliminating Internet-facing servers from the [DoD Information Network] core, ensuring Internet-facing servers in DoD demilitarized zones (DMZ) are operationally required, and removing trust relationships with external authentication services." In particular, commanders and supervisors are directed to ensure the physical security of network infrastructure devices and to "disconnect all Internet-facing web services and web applications without an operational requirement." Commanders and supervisors are further directed to report any commercially provided Internet connections to the DoD's classified network, NIPRNet.

Practice Point: Companies should always evaluate whether all systems need to be connected to a network that allows remote access. Moreover, companies should limit the amount of sensitive data stored on portable devices, such as laptops.

Alignment to Cybersecurity Service Providers

The fourth and last Line of Effort seeks alignment to cybersecurity and computer network defense service providers "to mitigate cybersecurity threats and enable the provision of accurate, timely, and secure information to the warfighter." The implementation plan directs commanders and supervisors to "provide standardized information to the [service providers]" and directs service providers to "exercise response plans to validate the processes, subscriber documents, contact information, and communication mechanisms."

Specifically, DoD commanders and supervisors must ensure that policies or service agreements with service providers are executed and implemented. These policies or agreements will require that service providers update the following at least every six months: documentation of network diagrams, software and hardware inventories, any ports, protocols, and services listings, and points of contact. In addition, every six months, service providers are to conduct at least one exercise to test each DoD organization's cyber incident response plan and update the cyber incident response plan to reflect the results of the exercises and real world events.

Practice Point: All companies should have minimum cybersecurity standards for any vendor that connects to its network as well as audit compliance with those standards.

As more government agencies and regulators issue plans and guidance on cybersecurity, best practices are starting to emerge. For organizations that are developing or reviewing their own cybersecurity plans, the DoD Cybersecurity Discipline Implementation Plan and similar plans from other government agencies can serve as useful guideposts.

Return to Table of Contents

Demand for Cyber Insurance and Market Capacity Continue to Grow

Recent studies by three insurance brokers provide valuable insight into cyber insurance trends.

In the wake of the seemingly never-ending reports of high profile cyberattacks and the increasing awareness of cyberrisks, the demand for cyber insurance products continues to grow across virtually all industries, according to recent reports by insurance brokers Marsh & McLennan Companies (Marsh),[2] Arthur J. Gallagher & Co. (AJG)[3] and Willis Towers Watson (Willis).[4]

Marsh reports that its U.S.-based clients purchasing standalone cyber insurance policies increased 27 percent from 2014 to 2015, continuing the steady 20 percent to 30 percent annual increase in demand since 2012. AJG similarly reports that insurance carriers and brokers are experiencing a 20 percent to 60 percent growth in cyber insurance business year over year. Meanwhile, Willis reports an estimated 150 percent growth rate for cyber and privacy liability insurance in the next five years. The manufacturing industry had the largest increase in demand for cyber insurance in 2015, according to Marsh, with a 63 percent rise in demand. The following industries also saw strong increases in demand for cyber insurance in 2015: communication, media and technology (41 percent), education (37 percent), retail/wholesale (30 percent), and power and utilities (28 percent).

In addition to the increased demand for cyber insurance, Marsh reports that companies are seeking cyber coverage beyond privacy breach costs, in recognition of the strong reliance on technology for essential business operations and the concomitant need to protect against cyberrisks. In response, insurers have introduced more tailored solutions to cyberrisks and exposures, including coverage for disruptions of supervisory control and data acquisition systems, business income and extra expenses, failure to supply energy, and network security and privacy liability.

Marsh also reports that cyber insurance limit amounts rose in 2015, with limits averaging $16.9 million for companies of all sizes, up from $14.8 million in 2014. Also among companies of all sizes, those in the communications, media and technology industry as well as the financial institutions industry carried the highest policy limits in 2015, with limits averaging $43.3 million and $29.7 million, respectively.

According to Marsh, capacity remains abundant at more than $500 million, with most large insurance towers having limits between $200 million and $400 million. Nevertheless, Willis and AJG report that certain market segments perceived to be high risk — such as the health care and retail industries — may face difficulties obtaining adequate capacity and reasonable pricing. Moreover, some excess insurers have decreased capacity in an attempt to minimize high risk exposure, according to AJG.

[2] Marsh & McLennan Companies, "Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases," March 2016.

[3] Arthur J. Gallagher & Co., "Market Conditions," January 2016.

[4] Willis Towers Watson, "State of the Cyber Market," January 2016.

Both AJG and Willis also report premium and retention volatility and predict that premiums and retentions in the coming years will range from small decreases to significant increases, depending upon the industry, company size and extent of exposure to confidential information. AJG reports, for instance, that companies in the health care and retail sectors with revenues in excess of $1 billion can expect premiums and retentions to increase anywhere from 15 percent to 40 percent this year. With respect to other industries, AJG predicts that retentions will remain at the same level as last year, with premiums increases anywhere from 1 percent to 10 percent.

With the ever-present threat of cyberattacks looming over industries worldwide, an increasing number of companies are actively seeking stand-alone cyber insurance policies, including those providing coverage beyond privacy breach costs. Although carriers have been cautious in entering this arena, particularly for higher risk industries, both market capacity and tailored insurance solutions to cyberrisk are increasing, and more and more insurers are likely to join the market as they become better informed about cyberrisks and how to profitably underwrite a cyber insurance program. This should, in turn, eventually lead to increased market capacity, broader selection in cyber insurance products and the stabilization of insurance premiums.

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

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