WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

The New Administration: Potential Cyber and Privacy Issues

December 21, 2016

AUTHORS

Daniel K. Alvarez | **Elizabeth J. Bower** | **Elizabeth P. Gray**

In the cybersecurity and privacy world, 2016 has been an eventful year. From Privacy Shield to presidential debates, from data breaches to denial-of-service attacks, from SEC enforcement to FTC roundtables to FCC rules, rarely has a day gone by when cybersecurity and privacy issues have not been front and center in the national discussion. As we turn the page to 2017 and a new administration, there is no reason to believe that this will slow down.

In this memo, we highlight some of the major issues that are likely to impact the cybersecurity and privacy legal and policy landscape in 2017:

- Privacy Shield and Trans-Atlantic Data Flows
- LabMD, Data Security and the FTC's Unfairness Authority
- The SEC and Cybersecurity Enforcement
- SEC and CFTC Cybersecurity Rulemakings
- Increasing State Role in Cybersecurity and Privacy Regulation

- The Common Carrier Exemption and FTC Jurisdiction
- National Data Breach Legislation
- Privacy and Security and the "Internet of Things"

Privacy Shield and Trans-Atlantic Data Flows

The EU-U.S. Privacy Shield Framework provides companies with a mechanism to transfer personal data from the European Union to the United States. The framework came into effect on August 1, 2016, but is already on shaky ground. In October 2016, Digital Rights Ireland filed a complaint with the EU's General Court contesting the European Commission's adequacy decision. The new administration will have an opportunity to join the case to support the adequacy finding, but we do not know whether it will continue to support Privacy Shield or uphold the national security commitments that were a critical part of the adequacy decision. EU Justice Commissioner Věra Jourová has said the EC will "closely monitor the respect of protection standards and the correct implementation" of Privacy Shield "under the new U.S. leadership."[1]

Moreover, EU regulators in Ireland and elsewhere are questioning the validity of the EU's Model Contractual Clauses to provide adequate data protection for data transfers. Invalidation of both Model Clauses and Privacy Shield would create significant uncertainty regarding the ability of companies to transfer data from the EU to the United States.

LabMD, Data Security and the FTC's Unfairness Authority

In recent years, the Federal Trade Commission ("FTC") has been expanding its authority to enforce data security standards through a series of consent decrees under Section 5 of the Federal Trade Commission Act ("FTC Act"). When LabMD challenged the FTC's authority rather than submit to a consent decree, the FTC issued an Opinion and Final Order finding against LabMD, explaining that "subjective types of harm" including unique privacy and reputational harms associated with health data are substantial and that future harm need only pose a "significant risk" to be unfair. But when LabMD appealed the FTC's decision to the Eleventh Circuit, the court stayed the FTC's order, suggesting that the court saw merit in LabMD's substantive arguments.

Despite this setback, the FTC has continued to move forward with data security enforcement, as evidenced by the consent decree the FTC reached earlier this week with the operators of AshleyMadison.com. Nevertheless, a court decision in favor of LabMD may diminish the FTC's ability to use its unfairness authority in data security and privacy matters. This could hamper the FTC's ability to enforce in the data security and privacy realm and may leave privacy advocates, and the FTC, asking Congress to grant the FTC clearer privacy and data security authority. With a potential

[1] Speech of Commissioner Věra Jourová at the 7th Annual European Data Protection and Privacy Conference, Dec. 1, 2016, *available here*.

gap in the enforcement of data security practices and the risks of data breaches growing, the new Administration and Congress may need to grapple with questions about the FTC's authority in this area.

The SEC and Cybersecurity Enforcement

For some time now the Securities and Exchange Commission ("SEC") has prioritized the oversight of cybersecurity risk in the financial services industry by leveraging its enforcement, examinations, and rule-making authority. The agency has filed enforcement cases and fined financial institutions based on violations of cybersecurity-related rules, namely Regulations S-P (Safeguards Rule) and S-ID (Identify Theft Red Flag Rule); we expect that trend to continue under the Trump Administration.[2] In fact, we anticipate that the SEC may increase its focus on public company disclosures of cybersecurity risks and incidents.

The SEC's Office of Compliance, Inspections, and Examinations ("OCIE") has placed cybersecurity at the top of its examination priorities for Market-Wide Risks for which it examines broker-dealers and investment advisers. We expect that OCIE's priorities for 2017, typically issued in January of each year, will once again include cybersecurity at the top of the list. We also expect that OCIE will continue last year's focus of testing and assessment of firms' implementation of cybersecurity policies, procedures, and controls. OCIE currently refers significant deficiencies identified during examinations to the Division of Enforcement for investigation. Signs of how the Trump administration intends to approach SEC enforcement may be found in the number and types of cases that OCIE refers to the SEC's Division of Enforcement and that Enforcement chooses to investigate. These new cases could be an early indication of a continuation of prior practices, or re-aligned examination and enforcement priorities.

SEC and CFTC Cybersecurity Rulemakings

One area where we may see a significant difference between the Obama and Trump Administrations is with respect to new rules. Both the SEC and the Commodity Futures Trading Commission ("CFTC") have been actively pursuing cybersecurity-focused rulemakings, but it is unclear whether these will move forward. For example, the SEC has proposed the new Business Continuity Rule that would require SEC-registered investment advisers to adopt and implement written business continuity and transition plans reasonably designed to address risks related to a significant disruption in the investment adviser's operations, including those related to cybersecurity breaches.[3] The comment period for the proposed rule has closed, so the Trump administration will be presented with the option of moving forward with the rulemaking or deferring any action.

---

[2] See, e.g., *In the Matter of Morgan Stanley Smith Barney LLC*, Administrative Proceeding File No. 3-17280, Securities Exchange Act of 1934 Release No. 78021 (June 8, 2016); *In the Matter of R.T. Jones Capital Equities Management, Inc.*, Administrative Proceeding File No. 3-16827, Investment Advisers Act of 1940 Release No. 4204 (Sept. 22, 2015).

[3] See *Adviser Business Continuity and Transition Plans*, Advisers Act Release No. 4439 (June 28, 2016).

Likewise, the CFTC recently adopted amendments to its System Safeguard Rules that apply to derivatives clearing organizations[4] and designated contract markets, swap execution facilities, and swap data repositories.[5] The final rules clarify existing cybersecurity requirements relating to testing and system safeguards risk analysis, explain five types of cybersecurity testing essential to a sound system safeguards program, and implement testing frequency requirements for specified registrants.[6]

At the CFTC, at least, there appears to be bipartisan agreement that cybersecurity and overall system security is one of the most important issues facing markets today.[7] For example, Commissioner J. Christopher Giancarlo has called for a principles-based, "bottom-up" approach to combatting cybersecurity threats, arguing that this is the only effective way for a regulatory agency to keep current with continuous trading automation advances.[8] The extent to which agencies like the CFTC and the SEC will facilitate or encourage these "bottom-up" efforts through rulemakings, however, remains to be seen.

Increasing State Role in Cybersecurity and Privacy Regulation

For some time, state regulators have aggressively pursued a role in regulating businesses via state data security, privacy, and consumer protection statutes. The cybersecurity rules proposed by the New York Department of Financial Services ("NY DFS") are a prime example of that effort, and have positioned the regulator as a leader in aggressive cybersecurity regulation and enforcement efforts in the financial services sector. As we explained in a client memo earlier this year titled "Increased Financial Regulatory Focus for Enhanced Reporting of Cyber-Events and Cyber-Enabled Crime," NY DFS proposed new cybersecurity regulations imposing new obligations on all entities supervised by NY DFS, including major banks, insurance companies, mortgage brokers, credit unions, holding companies, and investment companies, as

---

4 CFTC, System Safeguards Testing Requirements for Derivatives Clearing Organizations, 17 C.F.R. § 39, *available here*.

5 CFTC, System Safeguards Testing Requirements, 17 C.F.R. §§ 37, 38, 49, *available here.*

6 Additionally, the final rules clarify provisions concerning the scope of system safeguards testing, internal reporting and review of testing results, and remediation of identified vulnerabilities and deficiencies. CFTC, Fact Sheet – Final Rules on System Safeguards Testing Requirements (Sept. 8, 2016), *available here.*

7 Statement of Commissioner J. Christopher Giancarlo Regarding Proposed Rule on System Safeguards Testing Requirements (Dec. 16, 2015), *available here.*

8 Guest Lecture of Commissioner J. Christopher Giancarlo, Harvard Law School, Fidelity Guest Lecture Series on International Finance (Dec. 1, 2015), *available here* ("The only effective way for a regulatory agency to stay abreast of the rapid advances of trading automation is to be informed through an ongoing bottom-up process. That is, through industry working groups composed of leaders of automated trading firms setting industry best practices and procedures. Such best practices should then be set as standards and routinely updated by market self-regulatory organizations. Regulatory frameworks for automated trading must enhance, not stifle, industry best practices. They must be informed by technological innovation and improvement, not media headlines, best-selling books or political campaign agendas.").

well as smaller entities like check cashiers and budget planners. The proposed regulations impose new obligations with respect to entity organization and compliance, technology in place to protect personal information, recordkeeping, and reporting.

Although NY DFS's proposed regulations have been heavily criticized by banking and insurance groups, other state regulators may follow suit by taking a more active role in cybersecurity enforcement. In particular, we expect that any perception that the new administration is easing regulatory oversight and federal enforcement on the data privacy and cybersecurity front is likely to accelerate this trend and may force companies to contend with a variety of different, and potentially contradictory, set of industry-wide requirements.

The Common Carrier Exemption and FTC Jurisdiction

The FTC's authority also was undercut earlier this year when the Ninth Circuit held, in *FTC v. AT&T Mobility LLC*,[9] that common carriers are categorically exempt from Section 5 of the FTC Act, even for activities unrelated to common carriage. In contrast, the FTC has long held that the "common carrier exemption"[10] is activity-based and not status-based.[11] The FTC has requested a rehearing en banc, challenging the Ninth Circuit's decision. The court's ultimate decision, particularly in light of the ongoing LabMD litigation, may prompt administration and Congressional action to address the FTC's authority in the privacy and data security realm, and specifically to amend or even repeal the common carrier exemption.

National Data Breach Legislation

Data breach notification in the United States is currently governed by a patchwork of state and federal statutes that has resulted in significant inconsistencies across jurisdictions and imposes high compliance costs on businesses, particularly those with operations or customers in multiple states. In recognition of these perceived inconsistencies and inefficiencies in the current framework, there have been numerous attempts to introduce comprehensive national data breach legislation, with little success. Nevertheless, the push for comprehensive reform at a national level is unlikely to abate, given the increasing number and profile of data breaches. With Republicans controlling both the new administration and both houses of Congress, this may be a prime opportunity to address comprehensive data breach notification legislation.

---

9 No. 14-04785 (9th Cir. Aug. 29, 2016).

10 15 U.S.C. § 45(a)(2).

11 A November 2015 Memorandum of Understanding between the FTC and the FCC solidified this view, stating "[t]he agencies express their belief that the scope of the common carrier exemption in the FTC Act does not preclude the FTC from addressing non-common carrier activities engaged in by common carriers." FTC-FCC Consumer Protection Memorandum of Understanding, signed Nov. 16, 2015, *available here*.

Privacy and Security and the "Internet of Things"

The "Internet of Things" ("IoT")—a growing network of seemingly ordinary objects that connect to the Internet and collect, receive, or transmit data—is attracting significant attention on the subject of privacy and cybersecurity. The FTC and the FBI have both highlighted privacy and data security concerns with respect to the IoT.[12] Following a massive distributed denial of service attack in October 2016 that knocked out Internet access throughout the United States, and which was fueled by malware surreptitiously installed on connected, IoT devices, Congress took up the issue via hearings on IoT security.[13] This attention from lawmakers and regulators, coupled with the growing number of connected devices doing everything from vacuuming our floors to heating our homes and driving us to work, should continue to make IoT-related privacy and cybersecurity issues a high priority during the next administration.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125, dalvarez@willkie.com), Elizabeth J. Bower (202-303-1252, ebower@willkie.com), Elizabeth P. Gray (202-303-1207, egray@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

December 21, 2016

Copyright © 2016 Willkie Farr & Gallagher LLP.

This memorandum is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum may be considered advertising under applicable state laws.

---

[12] FTC, Internet of Things: Privacy & Security in a Connected World (Jan. 2015); FBI, Cyber Tip: Be Vigilant With Your Internet of Things (IoT) Devices (Oct. 13, 2015).

[13] Understanding the Role of Connected Devices in Recent Cyber Attacks, Committee on Energy and Commerce (Nov. 16, 2016), *available here*.