LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security and Antitrust & Competition Practices

December 18, 2018 | Number 2424

FTC Hearings Discuss the State of Data Security in the 21st Century

Ninth hearing on Competition and Consumer Protection in the 21st century highlights challenges of addressing persistent threats to data security.

On December 11 and 12, the Federal Trade Commission (the FTC or the Commission) held its ninth installment in its series of 10 hearings on Competition and Consumer Protection in the 21st Century. This hearing featured panels focusing on issues such as emerging data security threats, trends in data breaches, the US approach to data security, and how companies are incentivized to invest in data security. Speakers at these panels included government officials (including FTC Commissioner Rebecca Kelly Slaughter and representatives from the FTC's Division of Privacy and Identity Protection), academics, and specialists from the private sector. Speakers discussed how companies currently protect consumers from data security incidents and what role the FTC can play in encouraging companies to adopt best practices for securing personal information.

Latham & Watkins is monitoring and sharing periodic insights on the FTC hearings, with a focus on significant statements from regulators, hints about where the FTC's enforcement priorities lie, and key points of disagreement among antitrust and consumer protection influencers. For prior analysis of the FTC hearings, please visit Latham's library of Thought Leadership.

Hearing #9's Big Idea: Data Security Programs Must Be Tailored to Each Company's Unique Risks

Security researchers kicked off the hearings with the oft-cited facts about the compounding, escalating nature of cyber threats — the number and the severity of security incidents continues to increase year-over-year. Because cyber risks constantly multiply and evolve, the only rational response is a risk and principles based approach — a programmatic approach to selecting and supporting the people, processes, and technologies needed to mitigate not only the risk of attacks, but the consequences to corporations and data subjects alike. According to panelists, this fundamental truth — that cyber risks will always expand and shift — should drive corporations to reconsider basic questions about the data they collect, why they collect data and how they use it, and to think programmatically about adopting and tailoring cyber risk management programs to one or more suitable, external standards.

There was substantial disagreement among panelists, however, regarding whether and how to compel or otherwise incentivize companies to bring cybersecurity programs to needed standards of rigor and

excellence. Some speakers, for example, Chris Calabrese and Michelle Richardson of the Center for Democracy and Technology, advocated for statutory mandates to perform risk assessments and draft tailored data security policies and procedures in light of the sensitivity of the collected data, the risk of exposure, and the cost to secure the company's systems that collect and store that data. Others, including academic Professor Daniel Solove of George Washington University, suggested that current consumer protection laws were sufficient to protect consumer data. Panelist Geoffrey Manne of the International Center for Law and Economics expressed deep skepticism that a hypothetical FTC uniform data security rule would have utility — *i.e.*, mitigate cyber risks and harms — across the diverse industries whose activities would presumably be the subject of such a rule.

Key Remarks

- ***"The FTC will not be retreating from its role as the nation's primary data security law enforcement agency. Digital data security becomes more important every day."*** Andrew Smith, Director of the FTC's Bureau of Consumer Protection.

FTC Bureau of Consumer Protection Director Andrew Smith opened the hearing by observing that the FTC would not be retreating from its role as the nation's primary data security law enforcement agency. While he expressed confidence that Commission's data security education efforts have helped deter some cyber adversaries, Smith noted that the FTC's law enforcement experience indicated that many companies had failed to achieve optimal data security. The current Commission therefore favors, and is pressing Congress for, new legal authority under the Administrative Procedure Act to promulgate formal, legally binding data security regulations to supplement the agency's current authority to seek sanctions against companies violating existing laws concerning data protection and data security. In the meantime, however, Smith stated that the Commission will continue to press its role as the nation's preeminent data security law enforcement agency and will use its authority to take action against companies that have unlawfully engaged in unfair or deceptive acts or practices. These comments come in the wake of the recent 11th Circuit decision in *LabMD v. Federal Trade Commission*, in which the appellate court found that the FTC's order requiring LabMD to establish and maintain a comprehensive data security program was impermissibly vague — due to the absence of a standard for reasonableness.

- ***"Every cyber line of defense at your company should report straight to the board of directors."*** Carolyn Holcomb, Partner, PwC.

A number of panelists were asked to speak about the components of a meaningful cyber defense program. Unsurprisingly, the critical "start at the top" principle was advanced as a minimum necessary starting point for reasonable security controls. The board should ensure that a mature information risk program is documented, staffed, and funded. A mature cyber risk management program maintains three "lines of defense" against cyber risk: 1) a dedicated security team working in conjunction with the business side to identify data that must be safeguarded; 2) a risk management team that may work with those responsible for assessing financial and legal risk to project the likelihood of a cyber incident and to insulate the company from that risk; and 3) an internal audit group to confirm sufficiency of data security measures.

Panelists discussed the benefits of establishing robust, formal reporting to the board from each of the three "lines of defense" to ensure that the board is fully engaged on cyber risk. Speakers agreed that a board needs accurate forecasts of cybersecurity risk to make informed decisions. Hence, panelists emphasized the importance of effective reporting that avoids technical jargon in favor of information about quantifiable risks associated with the cost of data breaches and reputational harm. With this information, board members can fulfill their fiduciary obligations by allocating resources to cybersecurity efforts,

altering certain aspects of the data model to minimize data collection, and empowering chief information security officers to implement new processes that reinforce a company culture that fosters data security. Even if the company cannot immediately invest in every recommended data security measure, establishing robust reporting protocols ensures that boards can effectively budget for data security needs and can plan for its cyber risks.

Several speakers advanced the Payment Card Industry (PCI) Standards as a compelling example (and perhaps model) of an external standard that has been widely implemented throughout the retail and payments ecosystem, resulting in material improvements in security. PCI security standards are a condition of every merchant's agreement by card association rules. On a sliding scale based on transaction volume, companies participating in the payments system must attest to, implement, and validate adherence to a set of rules and requirements. Companies work with outside assessors and experts who are expected to act as "coaches and advisors," not enforcers.

Security experts sounded another current theme around the imperative that all security risk management programs start from an understanding of what is collected, why, and where it is stored. As Troy Leach of the Payment Card Security Standards Council put it, "Requirement zero is being able to identify where all the data is." A corollary is understanding the necessity of sensitive datasets and capitalizing on opportunities to minimize or avoid such collection or storage altogether. "Most organizations don't ever need to see a credit card number" due to the prevalence of easy-to-use third-party tokenization solutions, for example, observed security consultant Tom McAndrew of Coalfire.

- ***"Data security is a journey, not an end point."*** Maneesha Mithal, Associate Director of the FTC's Division of Privacy and Identity Protection.

Speakers broadly emphasized the benefits of an external set of rules and standards, such as PCI, but most urged flexibility for companies to select and tailor the external control systems most suited to their data and business environment. Professor Lawrence Gordon of University of Maryland, College Park, thought that companies should only implement data security controls from external frameworks such as ISO 270001 or National Institute of Standards & Technology (NIST) in situations in which the benefits outweigh the costs. However, a number of speakers cautioned that there is strikingly little data available on the question of which security protocols work better than others at safeguarding personal information.

Panelists from the cyber insurance industry noted that insurers are seeking more information during the underwriting process than in previous years. Insurers want to understand whether the insured will be able to implement proper controls in light of the specific risks most likely to impact the company. Hence, the underwriting process may include attempts to understand how the company keeps an inventory of its systems, whether the company has had trouble patching vulnerabilities regularly, or whether the company has a large portfolio of end-of-life systems. A thoughtfully tailored data security program is likely to result in lower premiums.

- ***On the Internet of Things: "Not all security incidents involving consumer devices impact consumers directly — but they still matter."*** Justin Brookman, Director of Consumer Privacy and Technology Policy, Consumers Union.

Andrew Smith, the Director of the Bureau of Consumer Protection, indicated that the FTC is undertaking a new focus on the Internet of Things (IoT), taking time to note that the FTC is scheduled to confront D-Link at trial in early 2019 regarding the security of its Internet-connected devices. Panelists identified the IoT as a growing opportunity for cyber adversaries that seek to obtain unauthorized access to networks,

expose personal data, or commit other cybercrimes. Speakers noted that the risk posed by the IoT is amplified by the general inexperience of consumers with the way smart devices can imperil their privacy or financial security. Professor Kirsten Martin of George Washington University remarked that most consumers do not think to ask about data security protocols before purchasing a smart device. Other panelists agreed that even those who did ask about security could seldom find a clear answer. As cyber adversaries continue to adopt new methods, some panelists advocated for clearer norms for Internet-connected devices, including rules about how long a consumer can reasonably expect a smart device manufacturer to release patches to address vulnerabilities. In the absence of commonly accepted practices for addressing vulnerabilities, or even disclosing their existence, the speakers agreed that the growing ecosystem of Internet-connected devices poses a risk that is hard to mitigate.

- ***"Assess the data security risk of every vendor, not just IT vendors."*** Malcolm Harkins, Chief Security and Trust Officer, Cylance Inc.

Panelists also stressed the need to assess and manage risks posed by vendors who handle confidential customer data or otherwise contribute materially to vulnerabilities that can be exploited by cyber attackers. Speakers explained that many firms have historically tried to quantify the cyber risk associated with using a vendor based merely on how much money the company expended on the vendor's product or service. Panelists agreed that the better practice is to measure vendor risk based on the type and quantity of data a vendor can access or store, with the appreciation that low-tech insider threats can cause just as much damage as those with authorized access to a server. In order to manage the risks associated with vendors and any software related third-party interdependencies, panelists recommended that companies identify: 1) who is or will be responsible for managing vendor relationships; 2) what company data each vendor can access; 3) whether and when the vendor contact requires notification to the company of a breach or other incident that may relate to security; and 4) a process for monitoring each vendor based on the level of risk it poses.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, DC

Michael H. Rubin
michael.rubin@lw.com
+1.415.395.8154
San Francisco

Serrin A. Turner
serrin.turner@lw.com
+1.212.906.1330
New York

Hanno F. Kaiser
hanno.kaiser@lw.com
+1.415.395.8856
San Francisco

Scott C. Jones
scott.jones@lw.com
+1.202.637.3316
Washington, DC

Kelly Smith Fayne
kelly.fayne@lw.com
+1.415.646.7897
San Francisco

Amanda P. Reeves
amanda.reeves@lw.com
+1.202.637.2183
Washington, D.C.

Karen E. Silverman
karen.silverman@lw.com
+1.415.395.8232
San Francisco

Kandyce R. Jackson
kay.jackson@lw.com
+1.202.637.2290
Washington, DC

Jason M. Gerson
jason.gerson@lw.com
+1.202.637.2184
Washington, DC

You Might Also Be Interested In

DOJ to Withdraw Assent to Standards-Essential Patent Policy Statement
FTC Hearings Evaluate Enforcement Options for Minority Investments
Deep Dive on Deep Learning: FTC Considers Artificial Intelligence
FTC Hearing Evaluates Regulatory Oversight of Big Data and Privacy
Global Merger Regimes™ App
We've Got Washington Covered