GIBSON DUNN

September 15, 2015

U.S. FEDERAL TRADE COMMISSION PROVIDES GUIDANCE ON CYBERSECURITY ENFORCEMENT PRIORITIES

To Our Clients and Friends:

Last week Federal Trade Commission Chairwoman Edith Ramirez opened the agency's "Start with Security" conference series by describing three aspects of the agency's approach to assessing companies' data security practices. Chairwoman Ramirez highlighted that companies should (1) consider security when designing new products and services; (2) test their systems for security vulnerabilities; and (3) implement robust processes for reviewing, addressing, and internally escalating security-related red flags. Chairwoman Ramirez's comments provide further information regarding the data security practices the FTC views as "reasonable"--that is, the practices the FTC views as passing muster under Section 5 of the FTC Act, which forbids actions that are "deceptive" or "unfair" to consumers.

The History of the FTC's Cybersecurity Enforcement Program

Section 5 of the FTC Act states that "unfair or deceptive acts or practices in or affecting commerce, are . . . unlawful."[1] The FTC has long taken the position that Congress intended "unfair" practices to be defined broadly and flexibly to allow the agency to protect consumers as technology develops.[2] Since the FTC first asserted its authority to investigate and prosecute companies for insufficient data security procedures under Section 5 in 2002, the agency has pursued and negotiated consent agreements in over 50 enforcement actions alleging inadequate data security practices.[3] We overviewed the history of the FTC's data security enforcement program in detail in our recent Client Alert, *The Third Circuit Upholds the U.S. Federal Trade Commission's Authority to Regulate Cybersecurity*.

The FTC's Guidance on Its Cybersecurity Enforcement Priorities

The FTC summarizes its approach to evaluating data security practices as hinging on "reasonableness." Specifically, the FTC has indicated that it believes a company's data security measures "must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[4]

To state the obvious, these general pronouncements provide companies with little practical guidance when evaluating whether a particular investment in cybersecurity is required by the FTC Act. As a result, the FTC has for years faced calls to provide more detailed and useful guidance to businesses. The FTC's efforts to respond to these requests include issuing a "Start with Security" guide

for business in June 2015, providing a list of best practices for companies whose operations touch on the Internet of Things in January 2015, and publishing annual reviews of its privacy and data security enforcement efforts.

The Start with Security conference series attempts to build on these efforts. The FTC held its first conference, which targeted small and medium businesses in the software industry, in San Francisco on September 9, 2015. At the conference, Chairwoman Ramirez laid out three "key steps" that companies can take to integrate security into their products and practices:

First, "think about privacy and security as you design your product – embed it into the development process." Specifically, "when you develop an application, consider what information it will collect, how long you will retain it, how you will use it, and how you will secure it." In addition, "train your engineers in secure coding to avoid vulnerabilities in the design of your software."

Second, "test your product" and "make sure your security is ready before you launch." Ask yourself, "[a]re security defaults operating as intended? Are the choices that you offer to consumers working? Are the controls you have implemented secure? Evaluate your product in scenarios that replicate how consumers will use it in the real world."

Third, while "bugs are inevitable . . . companies must have effective strategies for managing, addressing, and learning from vulnerability reports." Companies should "[c]onsider setting up a bug bounty program or a contact point for receiving vulnerability disclosures from the security community."

Using Ramirez's framework, the FTC invited tech industry participants to speak about security by design, common security vulnerabilities, and strategies for secure development, and vulnerability response. In particular, the FTC invited these participants to focus on building a "security culture," establishing continuous threat modelling, embracing secure technologies, scaling security via training, leveraging existing resources, and discovering and responding to bugs. While many open questions remain regarding which data security practices (or combination of practices) satisfy Section 5's requirements, Chairwoman Ramirez's statements presumably highlight practices that weigh heavily in the FTC's assessment of the "reasonableness" of a company's approach to data security. Therefore taking one or more of these steps may help to reduce, at least somewhat, the risk of an FTC enforcement action.

The second Start with Security conference is scheduled for November 5, 2015, in Austin, Texas, and according to the FTC "will continue the FTC's work to provide companies with practical tips and strategies for implementing effective data security."[5] In addition, an ongoing FTC order enforcement action against LifeLock, Inc. may provide further insights into the data security practices the FTC views as "unfair" to consumers.[6] Although much of the docket remains under seal, the Commission has alleged that LifeLock violated a 2010 FTC consent order by "failing to establish and maintain a comprehensive information security program to protect its users' sensitive personal data."[7] Litigating this allegation may require the Commission to provide substantial detail, including

technical details, regarding what constitutes a "comprehensive information security program" and how LifeLock's program allegedly fell short.

---

[1] 15 U.S.C. § 45(a)(1).

[2] *See Wyndham*, 2015 WL 4998121, at *3–5.

[3] FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement" (Jan. 31, 2014).

[4] FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement" (Jan. 31, 2014).

[5] FTC, "Start with Security – Austin" *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/start-security-austin.

[6] *Federal Trade Commission v. LifeLock, Inc.* CV-10-00530-PHX-MHM, Dkt. No. 20 (complaint filed July 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/072-3069-x100023/lifelock-inc-corporation.

[7] *Id.* at Dkt. No. 20, *available at* https://www.ftc.gov/system/files/documents/cases/150721lifelocknotice.pdf

The following Gibson Dunn lawyers prepared this client alert: Sean Royall, Ryan Bergsieker, Richard Cunningham, Eric Vandevelde and Lindsey Young.

Gibson, Dunn & Crutcher's lawyers are available to assist with any questions you may have regarding these issues and have substantial experience counseling companies on data security issues, developing data breach response plans, responding to data breaches, navigating FTC investigations, and litigating against both private plaintiffs and government enforcers. For further information, please contact the Gibson Dunn lawyer with whom you usually work or any of the following members of the firm's Privacy, Cybersecurity and Consumer Protection Group:

United States

M. Sean Royall - Co-Chair, Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Alexander H. Southwell - Co-Chair, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang - Co-Chair, Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)

Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Joshua A. Jessen - Orange County and Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)

Europe
James A. Cox - London (+44 207 071 4250, jacox@gibsondunn.com)
Andrés Font Galarza - Brussels (+32 2 554 7230, afontgalarza@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan - Paris (+33 1 56 43 13 00, bgrinspan@gibsondunn.com)
Alejandro Guerrero Perez - Brussels (+32 2 554 7218, aguerreroperez@gibsondunn.com)
Jean-Philippe Robé - Paris (+33 1 56 43 13 00, jrobe@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)

China
Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)

India
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)