ROPES & GRAY

ALERT

Privacy & Cybersecurity

December 20, 2017

Federal Trade Commission Holds Workshop on "Informational Injury"

Attorneys
Rohan Massey
Douglas H. Meal
Heather Egan Sussman
James S. DeGraw
Deborah L. Gersh
Seth C. Harrington
Laura G. Hoey
Mark P. Szpak
Michelle Visser
David T. Cohen
David Nordsieck
Joseph Santiesteban

For years, the Federal Trade Commission, the primary consumer protection agency in the United States, has been bringing enforcement actions against companies on the basis that their alleged failure to use specified privacy and data security measures was purportedly an "unfair" business practice prohibited by Section 5 of the Federal Trade Commission Act. But the FTC in fact has no authority under Section 5 to declare a practice "unfair" unless, among other things, it causes or is likely to cause substantial, unavoidable injury to consumers that is not outweighed by countervailing benefits. What (if anything), then, is a "substantial" injury in the privacy and data security context, how should its likelihood be measured, and how should one measure the benefits and costs of particular practices?

Last week, the FTC took a step closer to proposing a framework for analyzing these issues by hosting a "Workshop on Informational Injury" (the "Workshop"), where panelists discussed how to identify and measure consumer injuries that may result from privacy and data security practices. The FTC's response to the Workshop will likely provide businesses with more clarity concerning how they can comply with the FTC's expectations in this area, and a forthcoming judicial decision may bring the first definitive ruling on these matters from the courts. Companies that collect or use personal information should closely monitor these developments as they seek to minimize their exposure to an ever-rising tide of regulatory scrutiny and litigation surrounding privacy and cybersecurity.

The Workshop featured opening remarks by Acting Chairman Ohlhausen, four panel discussions, and closing remarks by Andrew Stivers, Deputy Director for Consumer Protection in the Bureau of Economics.

Acting Chairman Ohlhausen's Opening Remarks

In her opening remarks, Acting Chairman Ohlhausen discussed her goals for the workshop:

- better identify the qualitatively different types of injury to consumers and businesses from privacy and data security incidents;
- explore frameworks for how the FTC might approach quantitatively measuring such injuries and estimate the risk of their occurrence; and
- better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing, and using information.

She explained that "in making policy determinations, injury matters" because "if there are no harms, then data use restrictions impose only costs and no benefits."

Panel Discussion and Closing Remarks

The Workshop panelists included industry representatives, consumer advocates, academics, and government researchers. In their discussion, which Deputy Director Andrew Stivers highlighted in his closing remarks, they generally agreed that privacy and data security events can cause non-traditional, and as-yet unrecognized, harms, but there was little agreement on how to determine which of these harms should trigger regulatory action, and further, how to quantify these harms. Even the threshold question of whether a harm occurs at all from particular practices (let alone an actionable one) prompted varying responses. For instance, during the panel on identifying privacy injuries, the panelists disputed at what point an injury occurs in a hypothetical involving in-store tracking that reveals that a customer was looking at HIV tests and greeting cards. Some panelists suggested a privacy injury occurs when the consumer is exposed to a risk of being individually identified, while others argued that the societal benefit of the data collection must be taken into account before determining a harm has occurred. Notably, the panelists did not address whether these sorts of intangible injuries would be "substantial" as required for an unfairness claim under Section 5; no court has ever held that they are.

Implications

While the FTC for years has suggested that Section 5's substantial injury requirement is satisfied whenever, in the Commission's view, a company's underlying privacy or data security practices were unreasonable, Commissioner Ohlhausen is now conceding that the FTC "need[s] a framework for principled and consistent analysis of consumer injury in the context of specific privacy and data security incidents." Such a framework could potentially be announced shortly by the U.S. Court of Appeals for the Eleventh Circuit, where cancer detection laboratory LabMD, backed by amicus briefs from business and technology organizations, is challenging an FTC data security action that resulted in an FTC finding that the company's data security practices were an "unfair" practice under Section 5 of the FTC Act. Ropes & Gray represents LabMD in the appeal.

The resolution of these issues will have significant practical implications for businesses nationwide. Both as a matter of business administration and to ensure compliance with Section 5, organizations engage in cost/benefit analysis to determine whether additional or different measures should be incorporated into their business practices. To the extent Section 5 governs privacy and data security, as the FTC contends it does, the cost/benefit analysis depends in part on what if any "informational injuries" must be taken into account, as well as how large and likely those injuries must be to trigger liability. That being the case, companies that collect or use personal information should closely monitor the FTC's response to the Workshop and the guidance on these matters that may be forthcoming from the courts.

For more information regarding the Workshop on Informational Injury or to discuss privacy or cybersecurity practices generally, please feel free to contact Rohan Massey, Doug Meal, Heather Egan Sussman, Jim DeGraw, Debbie Gersh, Seth Harrington, Laura Hoey, Mark Szpak, Michelle Visser, David Cohen, Dave Nordsieck, Joe Santiesteban or another member of Ropes & Gray's leading privacy & cybersecurity team.