ROPES & GRAY

ALERT

Privacy & Data Security ▪ Technology, Media & Telecommunications

May 21, 2015

Nomi FTC Settlement Highlights Risks of Publicizing Company Privacy Policies

Attorneys
James S. DeGraw
Seth C. Harrington
David McIntosh
Douglas H. Meal
Mark P. Szpak
Michelle Visser
David T. Cohen

A closely divided Federal Trade Commission ("FTC" or the "Commission") has signaled support for the agency's recent focus on mobile device privacy. On April 23, 2015, the five-member Commission voted 3-2 to accept a proposed consent order that will settle claims arising from alleged misrepresentations in the online privacy policy of start-up Nomi Technologies, Inc. ("Nomi"). Although Nomi does not provide services to consumers, the majority reasoned that the Commission properly exercised its power to regulate deceptive acts or practices under Section 5 of the FTC Act ("Section 5") because certain representations in Nomi's consumer-facing online privacy policy—which Nomi was *not* required to post in the first place—allegedly turned out to be inaccurate. The decision thus serves as a stark warning to mobile and other companies as they contemplate whether and how to craft privacy policies that are available to the public.

As alleged in the FTC's complaint, Nomi's service provides brick-and-mortar retailers with aggregate data collected from consumers' mobile devices as the consumers shop in, or in some cases pass by, their stores. Specifically, the service collects media access control ("MAC") addresses, which are broadcast by devices as they search for WiFi interfaces. This information can be used to identify the general location of devices within stores at different dates and times, allowing retailers to improve store layouts and improve customer wait times. Although the service does not match MAC addresses to particular consumers' identities, it does save MAC addresses in a coded format so consumers' behaviors can be tracked over time. According to the FTC, the MAC is therefore a type of "persistent unique identifier" for a consumer's device.

The FTC's willingness to bring the action suggests the Commission may be prepared to recognize a broadened interest in privacy that goes beyond the "personally identifiable information" that has been at issue in many of the agency's privacy complaints. But, significantly, the FTC did not challenge the legality of Nomi's service itself. Instead, it alleged that Nomi made misrepresentations about the notice and the choices that would be provided to consumers about the collection and use of information about their devices. The allegedly offending statement, published in Nomi's online privacy policy for approximately one year spanning 2012 and 2013, stated that "Nomi pledges to . . . always allow consumers to opt out of Nomi's service on its website as well as at any retailer using Nomi's technology." The website-based opt-out was available to consumers and was utilized by approximately 3.8% of consumers who visited the site. However, consumers were not provided with means of opting out of the service at retailer locations. Nor were consumers put on notice at retailer locations that the retailers were using the service. The FTC challenged the online representation as false and misleading under Section 5.

According to the majority, the posited victims of Nomi's allegedly deceptive practices are "privacy-sensitive" consumers who may have viewed the privacy policy on Nomi's website but who, on the basis of representations in the policy, decided to delay opting out until they determined whether the stores they patronized used the service. The majority reasons that such consumers may have been deceived (i) because an in-store opt-out was not, in fact, available, and (ii) because stores did not notify consumers that they were using Nomi's tracking service despite Nomi's "implied promise" that such notification would be provided.

The latter point—based on the majority's conclusion that "the express promise of an in-store opt-out necessarily" implies that "retailers using Nomi's service would notify customers that the service was in use"—serves as a reminder that the FTC views implied representations to be just as actionable as express representations under Section 5.

In voting to accept the proposed consent decree negotiated by Nomi and the FTC staff, the majority concluded that the allegedly false statement in the privacy policy was material within the meaning of Section 5 and therefore an appropriate target for the Commission's deception authority. Invoking the posited "privacy-sensitive" consumer, the majority stated that Nomi's representations were material because they "go to the very heart of consumers' ability to make decisions about whether to participate in these services." But dissenting Commissioner Joshua D. Wright argued that, in order for deception to be material, it must "cause[] consumers to make choices *to their detriment* that they would not otherwise have made." (Emphasis added.) In this case, Wright explained, there was no such injury because consumers who viewed the policy and wished to opt out would have done so successfully via the website. Both he and dissenting Commissioner Maureen K. Ohlhausen also argued that, given this absence of consumer injury, the FTC staff should have exercised its prosecutorial discretion to refrain from bringing an action against Nomi. Underscoring the lack of any consumer harm is the staff's election not to pursue an action based on its Section 5 power to regulate "unfair" acts or practices, which requires a showing of substantial consumer injury.

The consent order would bar Nomi, for a period of twenty years, from *misrepresenting* the options through which consumers can control the collection or use of their data and from *misrepresenting* the extent to which notice will be provided to consumers. It would not require that such options or notification actually be made available to consumers. The narrow scope of the relief provisions follows from the majority's view that the alleged injury to consumers was not the absence of in-store notification and the unavailability of an in-store opt-out, *per se*, but was instead Nomi's "allegedly false and material statement of the opt-out choices available to consumers" in its former online privacy policy. Accordingly, the consent order conspicuously lacks a provision common to many consent decrees that the FTC has entered in data privacy cases, *i.e.*, a provision requiring the adoption of a comprehensive privacy program, compliance with which is to be certified through biennial assessments over the life of the order.

The ironic upshot of the majority decision is that Nomi could have avoided the FTC enforcement action altogether by *not* posting a privacy policy, *not* describing its practices to consumers, and *not* offering an opt-out mechanism at all—points made by Commissioner Wright in his dissent. Even the three-person majority emphasizes that the proposed consent order "does not require that Nomi provide in-store notice when a store uses its services or offer an in-store opt-out." Given the potential logistical difficulties of providing in-store notification and opt-out options, or even imagining what they would look like, the next company may think twice before offering such options or making statements that can be construed as implying such options are available. Indeed, *all* companies may think twice before posting a privacy policy that they are not otherwise required to post. For, as Commissioner Wright argued in his dissent, the majority decision "sends a dangerous message to firms weighing the costs and benefits of voluntarily providing information and choice to consumers."

For more information regarding the consent order between Nomi and the FTC or to discuss data security practices generally, please feel free to contact Jim DeGraw, Seth Harrington, David McIntosh, Doug Meal, Mark Szpak, Michelle Visser, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.