IfrahLaw
FTC Beat
FTC and State AG News for E-commerce

Since When Did the FTC Start Regulating Cyber Security?

May 11, 2011

There's no question that the Federal Trade Commission has the authority to prevent deceptive and unfair trade practices, such as false or misleading claims directed at consumers. Somehow, however, that authority has morphed into a much broader reach than one would have expected on the basis of common sense. We've written extensively about such jurisdictional overreaching by the FTC in the health food industry (see, for instance, this article). One of the latest examples of the FTC's expansion of its powers is its recent settlement agreement with Twitter.

The FTC and Twitter entered into a settlement agreement in March to resolve claims that the company deceived consumers regarding its privacy protection practices. The FTC's action was a result of two security breaches at Twitter in 2009 that permitted hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information and tweets. The security breaches and underlying security practices at Twitter, according to the FTC, were in contravention of Twitter's published privacy policy.

The variance between Twitter's stated policy and its practice was the "hook" for the FTC, which alleged that Twitter thus deceived its users regarding its privacy protection measures. To address this alleged deception, the settlement agreement between the FTC and Twitter requires that Twitter not make any misrepresentations about its security measures and its protection of non-public user data. This portion of the settlement makes sense and appears to be within Commission jurisdiction, but the settlement terms are far more extensive. One troubling aspect is that the agreement outlines security measures for Twitter to follow and institutes external monitoring requirements.

So how does the FTC go from preventing deceptive trade practices to regulating cyber security? And where is the statutory authority for this power? The Commission appears to be engaging in an increasingly common practice of creating new standards and expanding its reach – outside its authority, outside the traditional rulemaking process – by developing those standards through settlement agreements with companies under investigation. These companies are likely to agree to a variety of terms in order to get the government off their back. From their perspective, it often makes sense to end a dispute with the FTC rather than to challenge its power.

So Twitter may have determined that it was in its interest to agree to the FTC's cyber security requirements. It may already have instituted adequate measures to comply with

the terms of the agreement. But the FTC may next "shop" the terms of the Twitter settlement agreement to other companies it is considering investigating. The terms of the agreement will gradually become industry policy, and the FTC will go after companies that don't adhere to that policy (which was never formally instituted).

This process of informal power expansion has been undertaken by the FTC in the health food industry and is being challenged by POM Wonderful LLC in federal district court. It remains to be seen whether the Commission will be reined in by the courts. In the interim, companies with a significant online customer base should be aware that the FTC is inching its way into regulating data privacy and data security.

FTC Beat is authored by the Ifrah Law Firm, a Washington DC-based law firm specializing in the defense of government investigations and litigation. Our client base spans many regulated industries, particularly e-business, e-commerce, government contracts, gaming and healthcare.

The commentary and cases included in this blog are contributed by Jeff Ifrah and firm associates Rachel Hirsch, Jeff Hamlin, Steven Eichorn and Sarah Coffey. We look forward to hearing your thoughts and comments!