

Playing Fair: New FTC Chair Pledges Increased Enforcement to Protect User Data

by [G.S. Hans](#) [1]
March 11, 2013

Last week, Edith Ramirez, the newly named chair of the Federal Trade Commission, participated in her first public appearance as chairwoman at the International Association of Privacy Professionals conference. Her comments there bode well for the future of domestic privacy protection, especially when paired with the FTC's recent settlement with HTC concerning the mobile device maker's unfair and deceptive trade practices.

In her remarks to IAPP, Ramirez highlighted the importance of the FTC's unfairness authority under Section 5 of the FTC Act. We at CDT have [previously advocated for the agency to broaden its interpretation of the unfairness power](#) [2]. Ramirez also reiterated [her support for use of the unfairness power in enforcement actions, within reason.](#) [3] "I feel we've used [the unfairness authority] very reasonably," Ramirez said, emphasizing that such authority doesn't give the agency a blank check. We agree that the unfairness power is important, and that it must be used carefully.

Ramirez also stated that, when evaluating the kinds of harms that consumers might suffer as a result of unfair practices, [those harms need not be monetary or financial in nature, but cannot be speculative.](#) [4] We agree that focusing on monetary harm is too narrow, especially in privacy cases where harms may be reputational or may result in unauthorized or inadvertent disclosures of sensitive information. But unfairness regulation likewise cannot rest on theoretical harms, lest the FTC's regulation seem ad hoc and unpredictable. One of the most important aspects of an FTC enforcement action is the deterrent effect – if other companies cannot determine what lessons to learn from a consent decree, the agency's regulatory strategy becomes scattershot and unhelpful.

The HTC case provides a great example of how the unfairness authority, when carefully applied, can encourage commercial practices that protect user privacy via appropriate security measures. The FTC alleged that HTC had not taken reasonable steps to secure the software it created for its tablets and smartphones, which placed sensitive consumer data at risk. HTC preloaded customized software onto devices before selling them, and therefore consumers had no ability to avoid installing HTC's software on their devices. Unfortunately, the company failed to follow basic steps in the creation of the software. According to the complaint, HTC did not adequately audit its software, train its engineers regarding privacy and security issues, or develop a program to incorporate internal or external feedback regarding security vulnerabilities into new versions of its software.

As a result, the HTC software was vulnerable to third-party applications accessing comprehensive data logs detailing user's geolocation, browsing history, text messages, and applications. The FTC alleged that HTC's statements to consumers regarding its privacy and security practices meant that the oversights the company made constituted a deceptive trade practice, and that its inadequate security measures were an unfair trade practice, given that there was no countervailing benefit to consumers from having an insecure phone. The FTC has often used unfairness authority to regulate data security cases, as in [the Upromise case from last year](#) [5], and companies are on clear notice that poor security practices can be prosecuted under the Commission's unfairness authority.¹

We agree that HTC's actions in this case were per se unfair under the FTC Act, and that this case was a strong candidate for an enforcement action. [Just as last month's mobile privacy report and enforcement against Path demonstrated to companies the importance of privacy by design](#) [6], the HTC enforcement action and the statements of Chairwoman Ramirez emphasize how vital strong security programs are to all technology companies. We hope they heed the message.

1. ¹. One company, Wyndham Hotels, is challenging the FTC's authority to regulate poor data security practices under its unfairness power. The FTC had sought a consent decree with

Wyndham for its lack of adequate security measures to protect customer data, but the company declined to settle. The FTC filed a complaint in federal court against Wyndham, which claims that the FTC cannot rely upon its unfairness authority given the absence of a written security policy communicated to consumers. The outcome of the Wyndham litigation could affect the future of data security actions brought under the unfairness prong of the FTC Act.

-
- [mobile security](#)
- [mobile privacy](#)
- [FTC Act](#)

The copyright © 2013 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

<https://cdt.org/blogs/gs-hans/playing-fair-new-ftc-chair-pledges-increased-enforcement-protect-user-data>

Links:

[1] <https://cdt.org/personnel/gs-hans>

[2] <https://www.cdt.org/blogs/gs-hans/0910laptop-spying-case-indicates-more-aggressive-ftc-stance-privacy>

[3] <http://thehill.com/blogs/hillicon-valley/technology/287089-new-ftc-chief-vows-to-continue-push-for-online-privacy>

[4] https://www.privacyassociation.org/publications/2013_03_08_new_ftc_chair_ramirez_points_to_coppa_mobile_space_bcr_apec

[5] <http://www.ftc.gov/os/caselist/1023116/120403upromisecmpt.pdf>

[6] <https://www.cdt.org/blogs/gs-hans/0702ftc-and-mobile-privacy-be-careful-collecting-user-data-or-face-consequences>