

Laptop Spying Case Indicates More Aggressive FTC Stance on Privacy

by [G.S. Hans](#) [1]
October 9, 2012

The Federal Trade Commission announced late last month that [it had settled a landmark case](#) [2] with seven rent-to-own companies and a software design firm for alleged consumer spying via laptop webcams, screenshots, and keystroke monitoring. This settlement is important because it marks the most expansive use by the FTC of its “unfairness” authority to pursue privacy violations. As privacy legislation has stalled in Congress in the short term, this latest action could signal more aggressive FTC action under its existing authority to reign in dubious privacy practices.

According to [the complaint](#) [3], the software company, DesignerWare, provided software to rent-to-own franchises that rented laptops to consumers. The software was designed to allow franchises to shut off computers remotely if the rental contract had been breached – for example, if customers failed to make timely payments or if they stopped communicating with the franchise.

DesignerWare’s programs, however, were capable of much more than just remotely deactivating computers. Via Detective Mode, a special add-on feature, rent-to-own franchises could track a computer’s physical location, create fake software registration windows to gather information, log keystrokes, take screenshots, and even spy on consumers via the laptop’s webcam. In some instances, Detective Mode-enabled webcams took pictures of children, naked people, and people having sex. As a result, the FTC charged DesignerWare and the rent-to-own companies with violations of the FTC Act.

Nearly every other developed country has instituted robust privacy protections that follows the [Fair Information Practice Principles](#) [4] (FIPPs). In the US, by contrast, the FTC can only use the FTC Act of 1914, which established the agency and gave it the power to regulate *unfair* and *deceptive* acts or practices in commerce. In recent years, the FTC has relied upon its “deceptiveness” authority more than “unfairness” in order to pursue privacy violations, as in [the recent MySpace case](#) [5]. In that case, Myspace claimed in its privacy policy that it would not share users' personally identifiable information (PII) without first requiring notice and consent from users. However, the FTC alleged that Myspace gave third-party advertisers access to Friend IDs, which allowed advertisers at a minimum to learn the full names of individual users, which violated the terms of the privacy policy.

Most privacy cases rely on these types of “gotcha” scenarios, where a company mistakenly represents some aspect of their practices and then can be charged with acting deceptively. Structurally problematic website practices are less frequently the subject of FTC Act enforcement cases, in part because they are harder to discover. In addition, institutionalized practices might not necessarily be deceptive, but rather confusing or obscure to users. At first glance, unfairness seems a stronger fit for privacy cases in which users may not be aware of undisclosed practices that collect and use their data. However, the unfairness enforcement power requires a three-part analysis as [set out by the FTC Act](#) [6]. Unfair acts or practices must cause (or be likely to cause) (1) substantial injury to consumers (2) that cannot be reasonably avoidable, (3) and are not offset by benefits to consumers. While public policy considerations can play a role in this analysis, they cannot be the primary justification for an unfairness claim.

However, the unfairness prong has been applied in data security cases. Several high profile actions, including those against [Reed Elsevier](#) [7], [BJ’s Wholesale Club](#) [8], and [Wyndham Hotels](#) [9], have alleged weak or ineffective security systems protecting user data. In these cases, companies were responsible for user PII, including names, credit card numbers, Social Security numbers, addresses, purchase histories, and dates of birth. But these companies failed to enact adequate security methods, including anonymization, encryption, and user verification. As a result of these lax security procedures, consumers were exposed to the possibility of identity theft or other fraudulent activities – a very real injury that could not be offset by any possible benefit.

Privacy practices, unlike security measures, are more difficult to evaluate under the unfairness test. Under the third prong of the unfairness balancing test, companies that engage in bad privacy practices can point to a corresponding consumer benefit, making an unfairness claim unsuitable. If a company has a policy that might expose a consumer to harm, that company can often assert that there are countervailing benefits that point against an unfairness claim. For example, targeting users with ads based on their preferences and personal characteristics might implicate the unfairness prong, but a company could assert that targeted ads are actually beneficial to users, because they provide information about products that are particularly appealing to individual users. Because the unfairness test has a built in escape hatch for defendants, it can be a challenge for the FTC to successfully litigate unfairness claims.

It can also be difficult to determine what kind of harm is sufficient for the unfairness standard. CDT has suggested that [the types of harm that result from privacy violations should be interpreted broadly](#) [10], including data breaches, obstacles to innovation, dangers from government access, and encroachments upon individual liberty. In our prior commentary, [we have argued for the FTC's adoption of FIPPs in its understanding of consumer harm](#) [11] under the unfairness prong.

The Commission has recently indicated that it might expand its conception of what constitutes unfairness in the privacy context. For example, its high profile settlement with [Facebook](#) [12] included unfairness claims in addition to deception claims. But, as the first major case relying upon unfairness concerning the dissemination of consumer PII, the settlement indicates a major step forward in ensuring that the government protects user privacy.

In its [complaint against Designware](#) [3], the Commission made its strongest statement that poor privacy practices are governed by its unfairness authority, indicating that it considers harm to be sufficiently likely as a result of disclosing personal, financial, and confidential information to third parties. In its complaint, the Commission confidently alleged that DesignerWare's software caused substantial harm:

However, the drawbacks of unfairness – its multifaceted balancing test and lack of clarity over what is fair and what isn't – demonstrates why CDT has long argued for a substantive baseline consumer privacy law protecting users and encouraging new innovations. A baseline consumer privacy law would provide clear guidance to companies and define acceptable practices, as well as clearly and forcefully demonstrate to consumers that regulators are committed to protecting user privacy and promoting fair practices. In the interim, however, the FTC's renewed commitment to using unfairness to protect consumers is welcome.

- [FTC Act](#)

Copyright © 2013 by 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://www.cdt.org/blogs/gs-hans/0910laptop-spying-case-indicates-more-aggressive-ftc-stance-privacy>

Links:

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

[2] <http://www.ftc.gov/opa/2012/09/designware.shtm>

[3] <http://www.ftc.gov/os/caselist/1123151/designerware/120925designerwarecmpt.pdf>

[4] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

- [5] <http://ftc.gov/os/caselist/1023058/120911myspacecmpt.pdf>
- [6] <http://www.law.cornell.edu/uscode/text/15/45>
- [7] <http://www.ftc.gov/os/caselist/0523094/080801reedcomplaint.pdf>
- [8] <http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf>
- [9] <http://ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf>
- [10] <https://www.cdt.org/files/pdfs/Privacy-In-Digital-Age.pdf>
- [11] https://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf
- [12] <http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf>