FTC "Browser Sniffing" Case Could Mandate Disclosure of Unexpected Privacy Practices

by G.S. Hans [1]
December 11, 2012

Last week the FTC announced [2] its proposed settlement with Epic Marketplace, an online advertising company that had been accessing users' browser history in order to deliver tailored advertising. The FTC found that Epic's failure to disclose this practice in its privacy policies violated Section 5 of the FTC Act, which prohibits deceptive or unfair consumer acts and practices. In this case, the FTC was aggressive in its enforcement – identifying a bad consumer practice, locating a material omission in a privacy policy, and demonstrating the agency's watchful eye over online behavior advertising. Historically, the FTC's deceptive practices enforcement had focused on affirmative misstatements (for example, in the Upromise case) [3], so the Epic case marks a continued trend [4] of finding a lack of transparency itself to be inherently deceptive. However, focusing entirely on transparency within a privacy policy is still an unnecessarily narrow interpretation of Section 5's requirements In some instances – like browser sniffing – we think the agency could pursue the actual practice as fundamentally deceptive (or unfair) under the FTC Act.

According to the FTC complaint [5], Epic was engaged in online behavioral advertising by tracking consumers' online activities. The goal was to deliver targeted advertising specific to each user's interests, based on their browser use. In its privacy policy, Epic claimed that it was merely tracking user visits to sites within Epic's network. In practice, however, Epic obtained users' browsing histories from their browsers in order to deliver advertisements. By using code to scan style sheets and determine whether users had visited the sites before, Epic was able to sniff browsing histories [6] and discover that users were interested in sensitive financial and medical topics such as debt relief, personal bankruptcy, incontinence, and fertility. Epic's tracking practices did not confine themselves to sites within Epic's network, but gathered data from other sites as well – despite what the company had said in its privacy policy.

The FTC has long focused [7] on regulating online behavioral advertising, and this case shows how behavioral advertising can easily become overly intrusive and imperil consumer privacy. Under Section 5 of the FTC Act, the agency has the authority to pursue companies that commit unfair or deceptive acts or practices. CDT has previously advocated [6] for FTC enforcement against browser sniffing as a per se deceptive practice. Browser history sniffing works by exploiting the functionality of HTML that allows sites to display links you've previously visited as purple instead of blue — any link your site is going to render can get checked against the browser's history to see if you've been there before or not. History sniffers abuse this functionality, by querying browser history for tens of thousands of URLs that the site has no intention of rendering for the user. Such a blatant misuse of a browser's capabilities certainly seems to be an inherently deceptive means to access a user's website history contrary to reasonable expectations.

But the FTC didn't use this interpretation in the Epic case; instead, in its complaint it relied upon Epic's misrepresentations (and lack of representations) as the deceptive practice, rather than the act of browser sniffing as inherently deceptive (or unfair). This in itself is important. Now, companies engaging in particularly invasive or unexpected behavioral advertising techniques likely have an affirmative obligation to disclose those practices in a privacy policy. For example, the FTC may now require ad networks engaging in browser fingerprinting [8] or HTML5 local storage to track users across different sites to disclose this practice to users.

However, the FTC's deception claim relied upon the omission of a description of this practice to users who were evaluating Epic's opt-out procedure. In reality, presumably few internet users ever read and evaluated the opt-out notice, so relying upon that as the basis for a claim does not strike at the heart of troublesome practices. Perhaps this analysis is not entirely fair. After all, the FTC's gradual transition from requiring a deceptive statement to requiring affirmative notice of certain privacy practices is a welcome and important development. But it's worth considering what would have

happened if Epic accurately described its sniffing in a rarely seen privacy policy, or not offered an opt-out at all. Would the FTC have been willing to pursue the company? The FTC did not need to address that question in this settlement, but we think that given the invasiveness of browser sniffing to users such practices clearly violate Section 5.

The FTC continues to identify [9] new fact patterns to apply its unfairness and deception enforcement powers more broadly, which is a promising step. We hope that the agency will use the Epic case as a jumping off point for browser sniffing, rather than treating it as the limits of its enforcement powers.

- online privacy
- FTC Act
- browser history sniffing

Source URL:
https://www.cdt.org/blogs/gs-hans/1112ftc-browser-sniffing-case-could-mandate-disclosure-unexpected-privacy-practices

Links:
[1] https://www.cdt.org/personnel/gs-hans
[2] http://www.ftc.gov/opa/2012/12/epic.shtm
[3] http://www.ftc.gov/opa/2012/01/upromise.shtm
[4] http://www.ftc.gov/opa/2009/06/sears.shtm
[5] http://www.ftc.gov/os/caselist/1123182/121205epiccmpt.pdf
[6] https://www.cdt.org/blogs/justin-brookman/browser-history-sniffing-news
[7] http://www.ftc.gov/os/2007/12/P859900stmt.pdf
[8] https://panopticlick.eff.org/about.php
[9] https://www.cdt.org/blogs/gs-hans/0910laptop-spying-case-indicates-more-aggressive-ftc-stance-privacy