

The FTC and Mobile Privacy: Be Careful in Collecting User Data, or Face the Consequences

by [G.S. Hans](#) [1]
February 7, 2013

The FTC's announcement late last week of [a settlement with a mobile app developer](#) [2] and [the Commission's simultaneous release of a mobile privacy report](#) [3] highlighted the agency's focus on protecting consumer privacy in the popular mobile space. Moreover, the Commission's actions provided a pointed reminder to app developers that they must consider privacy at the earliest stages and in all phases of creating their innovative products.

The settlement was with Path, a social networking company, arising out of alleged violations of the Children's Online Privacy Protection Act (COPPA) and the FTC Act. With respect to COPPA, the company had not actually targeted children, but it collected birthdates in the enrollment process and that, the FTC concluded, was enough to give the company knowledge that it was collecting data from children under 13. The company found the problem on its own and modified its software to kick out anyone who entered a birthdate indicating an age less than 13, but its initial design placed it in violation of COPPA, which carries civil penalties that the FTC invoked – a warning to all about how strict the FTC is about kids' privacy. (We have concerns, by the way, that [recent revisions to the FTC's COPPA Rule](#) [4] could affect too many firms that are not targeting children.) To its credit, [Path apologized for its actions](#) [5] and urged other developers to consider privacy issues from the outset when designing new apps. We echo this call for privacy by design.

Also highlighting the importance of privacy by design was the Commission's use of the FTC Act. At issue was the app's collection of user contacts. In the iOS version, Path presented users with three options to connect with friends by (1) using the phone's Address Book, (2) connecting to Facebook to access a user's Friends list, or (3) inviting friends to join by email or SMS. However, even if the user chose none of these options, the app still automatically scanned the user's Address Book and recorded all the data therein. This, the Commission concluded, was deceptive under the FTC Act.

Importantly, this is [not the first time](#) [6] that an iOS app has inadvertently collected contact data from a user's Address Book. Indeed, one study from 2012 found that [nearly 19% of iOS 5 apps collected Address Book data without the knowledge or consent of users](#) [7]. Fortunately, iOS 6 rectified this particular issue ([as well as many other security vulnerabilities](#) [8]). What is significant about the FTC's action is that it tells developers they cannot simply accept every feature in an OS's interface that automatically pulls data from the user's device. Instead, developers must think very carefully about each item of data they collect, even if they do not use the data.

Amplifying this point, the FTC provided guidance that could help companies avoid privacy problems, with the release of its [Mobile Privacy Disclosures report](#) [9] and [new business education materials for mobile developers](#) [10]. The privacy report provides suggestions for both mobile platform providers (such as Apple, Google, Microsoft, and BlackBerry) and app developers on how to best protect consumer privacy. We think these recommendations – such as including just-in-time notices, providing clear privacy policies, and obtaining affirmative express consent for certain categories of data collection and dissemination as appropriate – would, if implemented, provide strong privacy protections for the growing mobile market.

The FTC also states in the report that adherence to codes produced by a multistakeholder process on mobile app transparency being convened by the National Telecommunications and Information Administration may be viewed favorably in enforcement actions against app developers. The NTIA process has been difficult, but we still hope that it will produce a code of conduct that creates robust protections for consumers.

In the interim, companies should be diligent in incorporating privacy protections into mobile apps from the beginning – not as an afterthought. While privacy by design can be a challenge for

developers focused on developing innovative products, especially given the ease in which data can be collected and shared on mobile platforms, the FTC's recent actions demonstrate that developers must think about privacy in every stage of the development process, or face costly, time-consuming enforcement actions. By releasing its privacy report and best practices, and pursuing companies that improperly collect personal information, however inadvertently, the FTC has provided more than enough guidance for developers to determine how to protect their users' data and provide sufficient notice-and-consent models for consumers.

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

The content on this site is for informational purposes only. 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/0702ftc-and-mobile-privacy-be-careful-collecting-user-data-or-face-consequences>

Links:

- [1] <https://cdt.org/personnel/gs-hans>
- [2] <http://www.ftc.gov/opa/2013/02/path.shtm>
- [3] <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>
- [4] <https://www.cdt.org/blogs/emma-llanso/2012coppa-rule-brings-regs-date-who-must-comply>
- [5] <http://blog.path.com/post/42023928427/path-and-the-ftc>
- [6] <http://articles.latimes.com/2012/feb/14/business/la-fi-tn-twitter-contacts-20120214>
- [7] <http://www.cultofmac.com/179733/19-of-ios-apps-access-your-address-book-without-your-permission-until-ios-6-report/>
- [8] <https://www.cdt.org/blogs/0110apple-ios-6-and-privacy-0>
- [9] <http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf>
- [10] <http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security>