



Developers of New Apps Need to Consider Privacy Issues

Feb 22, 2012

There's been much talk of Google's upcoming streamlined privacy policy. Now come new demands for cleaner, user-friendly data collection and usage disclosures in the mobile app world. Two recent events highlight changes that online advertisers and app developers need to prepare for: (1) [a letter from Congressmen Henry Waxman and G.K. Butterfield](#) to Apple regarding the security of user address books and contacts stored on iOS devices and (2) [an FTC report regarding privacy disclosures](#) for mobile apps directed at children.

The Congressmen's letter is in response to the recent Path address book fiasco in which Path acknowledged – and apologized for – its collection of consumer address book information without notifying users. News surrounding Path's activities led to Congressional concerns over the extent to which consumer data, especially contact information, is being collected and stored for future harvesting, all without the consumer's knowledge or permission. The Waxman-Butterfield letter quotes the Guardian: "there's a quiet understanding among many iOS app developers that it is acceptable to send a user's entire address book, without their permission, to remote servers and then store it for future reference. It's common practice, and many companies likely have your address book stored in their database."

The congressmen called for Apple to address how its app policies and practices protect consumer privacy. Apple was swift to respond, and within the day vowed to release a software update to prevent data collection that would violate the company's privacy policies.

On the heels of the Waxman-Butterfield letter (but in the works well beforehand) comes a report by the FTC: "[Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing.](#)" The report title pretty much says it all. The FTC surveyed some 960 kid-based apps sold through Apple and Android to determine, from the various app's promotion pages and websites, the extent to which the developers disclose what [child] consumer data is collected and how it is used. The FTC reported that it was disappointed with the results – that disclosures were scant or nonexistent.

Tying its authority over mobile apps with its authority to enforce children's privacy protections online through the Children's Online Privacy Protection Act (COPPA), the FTC warned that it will be reviewing more mobile apps directed at children over the next six months, but this time, it will be enforcing – not just surveying – COPPA



compliance. COPPA requires operators of online services directed to children under age 13 to provide notice and obtain parental consent before collecting items of “personal information” from children.

Several times in the FTC report the agency suggested the need for clear, concise, consistent and timely information on data collection and usage. That means disclosures of how the app (or third party advertisers) will/may use the consumer data should be upfront and precede download so that parents can determine whether or not to allow their children to use the app. Disclosures should include any connections to other social media.

The FTC report also identified (several times) the types of data that could be collected – from contact information, to location information, to call data, as well as in-app data. App developers and third party advertisers should take into account the importance of full disclosure.

Perhaps most importantly, the FTC report and the Waxman-Butterfield letter demonstrate that the government views Apple and Android (and other app stores) not just as the marketplace for app sales, but also as the gatekeepers. The FTC report pointed to Apple and Android as providing the architecture for disclosures and suggested that app stores could incorporate icons to make disclosures more easily identifiable. The Congressmen’s letter all but accuses Apple for its app’s failings.

We have been seeing increasing backdoor regulation by the government through major online presences in a couple of places, including [here](#) and [here](#). Since government regulators acknowledge the difficulties in keeping up with developments in new technologies, it’s fair to assume they will look to major online presences to have a hand in helping keep them up to speed and keeping advertisers and developers under wraps.

tags: [Cyber law](#), [Internet privacy](#), [Marketing to children](#)

*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!