Bill Requires Permission for Mobile Monitoring Software

February 8, 2012

Against the backdrop of controversy surrounding the use of monitoring software pre-installed on mobile phones, Rep. Edward Markey (D-MA) recently released a draft bill [1] requiring clear disclosure and express consent before monitoring software is used.

CDT has long advocated [2] for a comprehensive privacy law that would obviate the need for narrow legislative responses to newly-arising privacy issues. That said, this bill recognizes important privacy issues and we commend Markey for his efforts. Individuals have the right to know of, and in many cases say no to, monitoring software on their mobile phones.

We encourage further discussion around key provisions of the bill. This is a complicated issue: mobile phones implicate different players with different interests and obligations. For example, a wireless carrier's collection of certain data concerning the operation of its network might be considered a "commonly accepted practice" when clearly disclosed and subjected to reasonable use limitations. Furthermore, app stores should not be burdened with disclosure and choice obligations that properly fall to individual application developers.

Context: The Carrier IQ Controversy

The bill comes shortly after widespread reporting that monitoring software, developed by the company Carrier IQ, was deployed onto more than one hundred million handsets by carriers and phone manufacturers. The Carrier IQ software tapped into a large and potentially revealing swath [3] of diagnostic information from the mobile phone's operating system. For example, it could monitor what apps were used, whether an SMS was successfully sent, whether the screen is on or off, and the phone's location. However, the software did not log [4] individual keystrokes or the contents of SMS messages, email, photographs, audio or video. Phone carriers utilized the software primarily for diagnosis of hardware and network issues, collecting limited sets of data [5].

It is important to note that this kind of monitoring software is not an inherent evil. For example, in the desktop computer context, most of us are familiar with the dialogue box that announces a program has crashed, asking to submit an error report (which includes details about your computer and how it was being used around the time of the crash). Other ongoing monitoring and reporting tools, like Mozilla's Test Pilot platform, are clearly opt-in and give users extensive controls [6]. The deployment of Carrier IQ's software is different primarily because it was not offered with the same level of transparency and choice to the owner of the mobile phone.

Summary of the Bill

Markey's bill requires several kinds of companies to clearly disclose details about monitoring software and obtain express consent before putting such software to use. The entities obligated to observe these requirements are those that (1) sell mobile phones, (2) provide commercial mobile services, (3) manufacture phones, or (4) operate a "website or other online service from which a consumer downloads monitoring software." The bill also requires the user to consent to the software's operation before it can begin collecting and transmitting information.

"Monitoring software" is rather broadly defined as "software that has the capability automatically to monitor the usage of a mobile telephone or the location of the user and to transmit the information collected to another device [] whether or not the capability is the primary function of the software[.]"

The bill also sets forth obligations for any party *receiving* transmissions from monitoring software on a mobile phone. First, they must establish broadly-defined policies and procedures regarding information security practices. We believe these requirements are already implied under the FTC's enforcement actions under Section 5 [7], but it's nice to see them reinforced here. Second, if an

entity is receiving a transmission directly from the monitoring software and has an agreement concerning that information with a party *other* than the person who owns the phone (e.g., contracts with a carrier), that agreement must be filed with both the FTC and the FCC. This relatively narrow pre-notification requirement may not be unreasonable in this context. However, it's worth noting that the European Commission has signaled a move away from such pre-notification requirements in its recently proposed revision to the Data Protection Directive [8], citing undue administrative expense and lack of usefulness to regulators.

More Detail Needed

Since this bill involves a diverse set of entities—carriers, phone manufacturers, and online services—further discussion is needed. Indeed, each party deserves a separate analysis.

For example, carriers have a special interest in data concerning the performance of their wireless networks (e.g., where and when calls are dropped). When collections of this sort of connectivity data are properly disclosed and used for operational purposes, they might be considered "commonly accepted practices" as described in the recent FTC privacy report [9] and not subject to user choice. However, we have greater concerns about the collection of more revealing data like individual app usage, URLs, and the content of communications, regardless of purpose. Collection of these data is far less likely to be viewed as "commonly accepted," and carriers should here offer their users choice. (Whether that choice is opt-out or opt-in depends on an array of other details: the sensitivity and scope of the information collected, how long that data is stored in identifiable form, how that data is used, etc.)

Furthermore, "app stores" and other repositories for apps authored by third parties should not be burdened with the obligation to disclose information beyond the scope of their services. For example, an app store is unlikely to know the identity of the person to whom an app will transmit information and how that information will be used. As written, the bill could easily sweep in common sorts of apps that "monitor the usage of a mobile telephone" in order to offer coupons, manage power management, or trigger appointments and alarms. If this was the case, app stores would incur obligations under the bill. While we encourage mobile platforms and app stores to provide consumers with as much information as possible (e.g., clearly presenting the permissions requested by apps), responsibility ultimately rests with app developers in this context. We've elaborated upon this point in our app developer's best practices document. [10]

Finally, as written, the bill might be read so to require redundant disclosures (e.g., perhaps requiring both a handset operator and carrier to disclose and obtain consent). This is undesirable for companies and might be confusing to users. In most cases, it would be fair for the party collecting and using data to comply with any notice and consent obligations.

We commend Markey for taking initiative on this bill and look forward to further discussion.

Source URL:
https://www.cdt.org/blogs/aaron-brauer-rieke/82bill-requires-permission-mobile-monitoring-software

Links:
[1] http://markey.house.gov/press-release/markey-releases-discussion-draft-mobile-device-privacy-act-wake-carrier-iq-software
[2] https://www.cdt.org/policy/recommendations-comprehensive-privacy-protection-framework
[3] http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/
[4] http://www.carrieriq.com/CIQ_Press_Statement_DEC_1_11.pdf
[5] http://arstechnica.com/tech-policy/news/2011/12/carrier-iq-hit-with-privacy-lawsuits-as-more-security-researchers-weigh-in.ars

[6] https://testpilot.mozillalabs.com/privacy.php
[7] http://business.ftc.gov/legal-resources/29/35
[8] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
[9] http://www.ftc.gov/opa/2010/12/privacyreport.shtm
[10] https://www.cdt.org/report/best-practices-mobile-applications-developers-v-beta