New US privacy bill would regulate mobile data collection

The Mobile Device Privacy Act

On 12 September, Representative Ed Markey (D-Mass.) released the 'Mobile Device Privacy Act,'[1] which would require the Federal Trade Commission (FTC) to adopt regulations addressing monitoring software installed on mobile devices. The new obligations would impact wireless service providers, equipment manufacturers, device retailers, operating system providers, website operators, and other online service providers, underscoring the number of industry segments involved and the complexity of addressing privacy concerns in today's mobile wireless ecosystem.

The bill stems from media reports last year regarding Carrier IQ's monitoring software, which was installed on millions of mobile devices. The reports alleged that Carrier IQ's software was tracking keystrokes without user knowledge or permission, spurring a series of lawsuits. "Consumers should be in control of their personal information, including if and when their mobile devices are transmitting data to third parties," said Markey. "This legislation will provide greater transparency into the transmission of consumers' personal information and empower consumers to say no to such transmission."[2]

Under the draft Mobile Device Privacy Act, the FTC would have one year to issue regulations requiring carriers and device retailers to disclose at the point of sale, in a 'clear and conspicuous' manner: (1) The fact that monitoring software is installed; (2) The type of information that the software is capable of collecting and transmitting; (3) The identity of the parties with which the information will be shared; (4) How the information will be used; (5) The procedures by which a consumer who has consented to the collection and transmission of information by monitoring software may exercise the opportunity to prohibit further collection and transmission; and (6) Further information the FTC may 'consider appropriate'.

If the monitoring software is installed after the consumer purchases the device or service, the entity installing the software or providing the software download must make the disclosure. The disclosures must also be displayed (in a clear and conspicuous manner) on the website of the party required to make the disclosures. The Mobile Device Privacy Act authorises the FTC to provide an exemption to the required disclosures if the FTC determines that the use of the monitoring software for a particular purpose is 'consistent with the reasonable expectations of consumers.' Industry groups and privacy advocates are likely to spar over the scope of this exemption.

One noteworthy element of the bill is the definition of 'monitoring software' that spurs a host of new regulations: the term 'monitoring software' means software that has the capability to monitor the usage of a mobile device or the location of the user and to transmit the information collected to another device or system, whether or not such capability is the primary function of the software or the purpose for which the software is marketed. This broad definition would encompass a wide array of mobile apps and services, so much so some industry advocates have expressed concern. For example, Mark MacCarthy, Vice President for Public Policy at the Software & Information Industry Association, commented that the bill 'would impose rigid privacy rules on the mobile industry that can only lead to stagnation and a loss of innovate dynamism.'[3]

The Mobile Device Privacy Act would also require parties to obtain express consent from consumers before the monitoring software begins collecting and transmitting data. In addition, they must provide consumers that have consented with the opportunity at any time to prohibit further collection and transmission of information by such software. The bill would also impose new information security requirements on recipients of the monitoring data. The FTC would have one year to adopt regulations requiring: (1) A security policy addressing the collection, use, sale, other dissemination, and maintenance of the monitoring data; (2) The identification of a point of contact responsible for the management of the security of the information; (3) A process for identifying and assessing 'reasonably foreseeable vulnerabilities' in any system containing monitoring data, which must include regular breach monitoring; (4) A process for preventive and corrective action to mitigate any vulnerabilities identified by the system; (5) A process for disposing monitoring data in a way that makes it 'permanently unreadable or undecipherable'; and (6) A standard method for the destruction of paper documents and other non-electronic data containing such information.

The FTC's regulations require the policies and procedures to be displayed in a clear and conspicuous manner on the recipients' websites. Parties that enter into agreements to share the monitoring data would have to file those agreements with the FTC or the Federal Communications Commission (FCC).

The Markey bill would also establish joint FTC and FCC oversight, with the FCC having enforcement authority over commercial mobile service providers, commercial mobile data service providers, and mobile device manufacturers and the FTC having authority over other parties. The bill also provides for state attorney general suits and a private right of action.

Although the US Presidential election in November makes near-term legislative action unlikely, the bill continues to spark debate between industry groups and consumer advocates over the need for and scope of new data privacy and security legislation.

Mark W. Brennan Associate
Hogan Lovells US LLP
mark.brennan@hoganlovells.com

1. http://markey.house.gov/document/2012/mobile-device-privacy-act-2012
2. http://markey.house.gov/press-release/markey-releases-mobile-device-privacy-act
3. http://www.siia.net/blog/index.php/2012/09/mobile-privacy-time-for-collaboration-not-legislation/