The fundamental shift of digital activity into the mobile space has caused a meteoric rise in the number of American citizens using their mobile devices to access the Internet, engage in mobile commerce (mCommerce) and download a seemingly unlimited number of available mobile applications. Mobile devices are now the primary way for Americans to access the Internet, rather than through a laptop or desktop computer. In light of this rapidly evolving mobile ecosystem [1] as well as of several cases related to mobile privacy issues and increasing consumer concern about privacy on mobile devices, the U.S. Federal Trade Commission (FTC) has moved to establish guidelines for stakeholders in the mobile arena [2].

In a new Staff Report released in on February 1, 2013, the Federal Trade Commission (FTC), the government’s primary consumer protection agency, outlines several recommendations for mobile industry players on how to avoid FTC scrutiny and enforcement action. According to FTC Chairman Jon Leibowitz, this approach is necessary due to the large amount of commerce going mobile, as well as to the “wild west” nature of many of the rules and practices in the mobile space. Today’s smartphones allow multiple entities – wireless service providers, mobile operating system (OS) developers, handset manufacturers, mobile app companies, analytics vendors and advertisers – the opportunity to gain access to personal information at a level unheard of in the desktop environment.

However, it is important to note that, although the Commission approved the report, it is not binding. The report simply reflects the FTC’s strong focus on the issues and represents voluntary best practices for consumer privacy in mobile applications. In this article we review the contents of the
FTC report, stakeholder perspectives and suggested direction for further action from a consumer-advocacy perspective.

Mobile Privacy Legislative Review

Recent Federal Actions. Closely following the FTC’s 2012 recommendations regarding online privacy from the “Do Not Track” initiative, the FTC’s Staff Report is its strongest statement yet on mobile privacy issues and represents a move toward establishing rules and practices in line with those for the Internet. The report includes specific calls to improve mobile privacy disclosures by four primary mobile players: (1) mobile platform operating system (OS) providers, (2) mobile application developers, (3) mobile advertising networks and analytics companies and (4) others, including application developer trade associations, academia, usability experts and privacy researchers [2].

For mobile platform providers, the FTC suggests they build in privacy alerts and management tools for mobile users and implement enforceable standards for their mobile application developers. Specific recommendations include providing just-in-time privacy disclosures and exploring development of a one-stop "privacy dashboard," so consumers can review the data types accessed by applications they have downloaded. Further recommendations include developing icons to more clearly depict the real-time transmission of various user data and offering a do-not-track (DNT) mechanism. The report states that a mobile DNT mechanism, which a majority of the Commission endorses, would allow consumers to choose to prevent tracking by ad networks or other third parties as they navigate among apps on their phones.

For mobile application developers, the FTC recommends that they first provide a privacy policy for applications and ensure it is easily accessible through app stores. Second, developers should provide just-in-time disclosures gaining user consent before collecting and sharing sensitive information such as financial, health, geo-location or children’s data. Third, before integrating into an app any third-party code – from advertisers or analytics vendors for example – developers should determine what user information the third party will be collecting and communicate their findings to consumers. Finally, developers are encouraged to participate in mobile privacy best practices training and education.

For mobile advertising networks and other third parties, the FTC suggests that they improve communication with app developers, enabling them to provide full and truthful disclosures to consumers. Additionally, these groups should work with platforms to develop and ensure effective implementation of mobile DNT mechanisms.

Mobile Privacy Legislative Review

Mobile Privacy Legislative Review

Recent State Actions. Before the FTC’s latest Staff Report, California Attorney General Kamala Harris and the California Department of Justice issued the first set of state recommendations on mobile privacy. The report states that mobile application developers should “minimize privacy surprises” for their customers by minimizing or avoiding the collection and retention of consumer data not related to an app’s basic functionality. Additionally, consumers should be provided access to any personally identifiable data collected. Given the state’s huge consumer market, the California Attorney General’s mobile privacy recommendations essentially set the standard for technology companies nationwide and were likely the basis for the federal recommendations [3, 4].
Additional Federal Actions. Besides the FTC’s action, the U.S. Department of Commerce’s National Telecommunications and Information Administration (NTIA) is engaged in its own activities related to the issues of mobile privacy. On February 21, 2013, NTIA officials held one of a series of multi-stakeholder meetings on mobile privacy. This ongoing effort is expected to result in development of a consumer data “privacy code of conduct” concerning mobile application and interactive services transparency [5].

Mobile Privacy Stakeholder Perspectives

A number of stakeholders maintain a strong interest in the issue of mobile privacy. Key stakeholders include the federal and state governments, mobile platform OS providers, mobile application developers, mobile advertising networks and consumer advocacy groups and consumers.

Federal and State Governments. Government at both the state and federal levels has been concerned with mobile privacy issues for a number of years. In particular, the federal government’s experience regarding several pivotal cases has contributed to its concern and driven the FTC to begin development of the latest recommendations. For example, the seriousness with which the FTC is focused on mobile privacy is evidenced in its recent case against Path, Inc., the operator of a two-year-old social networking mobile application. Path was fined $800,000 for collecting children’s personal information via their mobile application without parental consents [6, 7]. In another case, the FTC charged handset manufacturer HTC with customizing the software on its smartphones to allow third-party applications to install software that could steal personal information, surreptitiously send text messages or enable the device’s microphone to record the user’s phone calls. The company must fix the issues or face penalties up to $16,000 [8]. In a case preceding those against Path and HTC, the FTC targeted Frostwire, a peer-to-peer software developer. Frostwire settled with the FTC, who charged that its software would likely cause users to unknowingly share sensitive personal files, including pictures, from their Android smartphones [9, 10]. Too often the mobile industry has demonstrated to the FTC and others that some degree of industry oversight is necessary in order to protect consumers. The question government agencies are grappling with is: How much oversight?

Mobile Platform OS Providers. The primary stakeholders able to promote mobile privacy and data protection are the mobile platform OS providers such as Amazon, Apple, Google, HP, Microsoft and RIM and their app stores, since mobile platform providers largely determine the mobile-user experience and users’ awareness of data privacy. Additionally, these providers have critical leverage over mobile application developers when they review apps for acceptance on their platforms and in their marketplaces. Because of this leverage, the FTC’s recommendations heavily target these stakeholders and have caused a substantial degree of stakeholder concern. Their main point of worry revolves around the issue of supervision of mobile app developers. Mobile platform providers are worried about their potential liability if they have not adequately evaluated the privacy protections of a mobile app in their store. Additionally, providers are concerned about any federal move toward increased regulation, which could have the effect of stifling innovation and ruining cutting-edge companies by exposing their innovations to competitors under some open-government, pre-market, privacy-approval process [11]. This stakeholder group strongly prefers industry-led, self-regulatory approaches to mobile privacy, believing they would be more efficient and effective.

Mobile Application Developers. Representatives from mobile-application-developer trade groups such as the Association for Competitive Technology and NetChoice have expressed their general support for the FTC’s recommendations. However, they are concerned about what they view as unintended consequences, such as app stores not screening for privacy at all (to avoid altogether the issue of whether they have done so adequately). Additionally, developers, like the platform providers, are concerned about the
costs involved in meeting compliance and worry that lawmakers will transform what they claim are helpful recommendations into “stifling regulations” [12].

**Mobile Advertising Networks.** Mobile privacy recommendations, such as those put forth in California, state that mobile advertising is not part of the basic functionality of a mobile app. As a result, mobile advertising industry members are confused and concerned about the level of scrutiny and enforcement they might be subject to, particularly as many mobile apps are ad-supported software. The mobile ecosystem is dependent upon ad revenue and mobile advertising networks are concerned that their role in the space is not clearly understood.

**Consumers and Consumer Advocacy Groups.** Although consumers gain a wealth of benefits from their mobile devices, they are increasingly concerned with the privacy issues surrounding these devices. It is well known that mobile apps collect large amounts of personal data without notifying consumers. From a privacy perspective mobile devices are unique because they are personal to the consumer (adult or child) using them. Devices are used for a number of activities like accessing the Internet and social networks, sending emails and text messages, taking and sharing photographs and making phone calls. Additionally, the small size of the device’s screen leaves little room for privacy disclosures. And mobile devices are typically always with the user and turned on, leaving an open door for data collection of all kinds. Consumers are, therefore, in a vulnerable position with respect to their mobile privacy [13]. Consumer advocacy groups, such as Moms with Apps and others, are working on behalf of consumers to press mobile industry players to implement the FTC recommendations and promoting the use of privacy icons [14]. At the least, consumer groups are strongly in favor of the FTC’s actions and would support stronger measures as needed.

### A Consumer Advocacy Perspective

The FTC Staff Report illustrates a set of guidelines for behavior and action from players in the mobile ecosystem. As such, the commission has taken some very important first steps regarding the issue of mobile privacy. Additionally, the NTIA’s ongoing work toward a mobile privacy code of conduct is also a promising development. However, these agencies must go further and seek to transform their recommendations into more binding measures through the legislative process.

The current FTC report urges the various mobile industry players to provide proper mobile privacy disclosures to consumers with the implication that, if self-regulation fails, it may take other steps. Any further legislative and regulatory mandates are yet to be defined; however, they should be initiated soon due to the potentially lengthy legislative process. Federal agencies should begin laying the groundwork right away for mobile privacy legislation. Agencies such as the FTC and NTIA, created for the express purpose of protecting consumers and serving the public good, have a mandated responsibility to investigate and monitor the activities of entities that possess certain know-how for obtaining consumers’ personally identifiable information from their mobile applications and services. Although mobile industry players claim they are capable of self-monitoring, arguably their overwhelming concern is for their own survival.

Although mobile industry players claim they are capable of self-monitoring, arguably their overwhelming concern is for their own survival. Ultimately, they will default to activities that maximize their profits – even at the expense of consumer trust and privacy – if firm legislation is not in place to guarantee delivery of strong penalties for violations.
Resources Mentioned in the Article


