



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

July 13, 2012

Via Electronic Filing

Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

**Re: Comment - Privacy and Security of Information Stored on
Mobile Communications Devices CC Docket No. 96-115/DA 12-918**

Dear Ms. Dortch:

Federal Trade Commission (FTC) staff appreciates this opportunity to respond to the above-referenced Federal Communications Commission (FCC) Public Notice. Through this Public Notice you seek comment on “the privacy and data-security practices of mobile wireless service providers with respect to customer information stored on their users’ mobile communication devices.” Additionally, you ask about existing “privacy and security requirements” for such data and the role of third parties in collecting and storing the data.

We note that the issues you raise in your request for comment concern a variety of different entities within the mobile ecosystem, including operating system providers, application developers, advertising networks, handset manufacturers, and telecommunications carriers. We commend the FCC for seeking comment on these issues, and offer our views based on our long-standing jurisdiction over the activities of all of these entities, other than the common carrier activities of telecommunications carriers. We would be pleased to work with the FCC as it considers the important issues raised in the notice.

In keeping with its extensive history of examining privacy implications of emerging technologies, in recent years, the FTC has devoted additional resources to protecting consumers’ privacy in the mobile ecosystem.¹ It has created a mobile technology unit; developed a mobile

¹ The FTC has protected consumers’ privacy through law enforcement, policy, and education initiatives. Over the past several decades, we have brought 92 cases enforcing the Fair Credit Reporting Act (“FCRA”); 40 data security cases; 19 cases enforcing the Children’s Online Privacy Protection Act (“COPPA”); over 100 spam and spyware cases; dozens of cases enforcing the Do Not Call Rule; and dozens of cases involving consumer privacy. We have also

lab containing a variety of smartphones, software, and equipment that permit investigators to collect and preserve evidence and conduct research; and engaged in a host of policy, enforcement, and education activities. Our goal has been to ensure that information consumers provide through mobile devices is protected and that consumers have the confidence to take advantage of the many benefits of the mobile marketplace.

Based on our expertise in this area, we believe that strong privacy and data security protections for consumers are critical in the mobile ecosystem. In this letter, we offer our views on several of the questions raised.

First, the FCC Public Notice asks about whether current practices in the mobile ecosystem raise concerns with respect to privacy and security. The Commission has testified twice on this issue and has expressed strong concerns about the lack of basic privacy protections on many new and emerging mobile products and services.² The Commission also examined this question extensively during a series of three public roundtables on consumer privacy, a preliminary staff report issued in December 2010, and a final report entitled *Protecting Consumer Privacy in an Era of Rapid Change* (“Privacy Report”), issued this March.³ The Privacy Report contains several discussions of practices that raise privacy and security concerns in the mobile arena. For example, it notes that the unique features of a mobile phone – which is highly personal, almost always on, and travels with the consumer – have facilitated unprecedented levels of data collection. It also noted the potential for mobile devices to collect and retain location information, that could be used to build detailed profiles of consumer movements over time and could be used in ways not anticipated by consumers. To address these concerns, the Commission called on companies to (1) limit collection to data they need for a

hosted many workshops; released several reports on privacy issues; testified before Congress on numerous occasions; provided comments on privacy legislation; and issued consumer and business education materials on privacy issues.

² *Consumer Privacy and Protection in the Mobile Marketplace: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (2011) (statement of David C. Vladeck); *Protecting Mobile Privacy: Your SmartPhones, Tablets, Cell Phones and Your Privacy: Before the Subcomm. for Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2011) (statement of Jessica Rich).

³ The Commission began this broad initiative in light of the vast array of new and evolving technologies and business models – such as social media, smart phones, and cloud computing – that rely on the collection and use of consumer data. The Privacy Report calls on businesses that collect and use consumer data, in both the online and offline contexts, to: (i) adopt the concept of privacy by design, (ii) simplify consumer choice, and (iii) increase the transparency of commercial data practices. The Privacy Report also continues to push industry to develop a Do Not Track mechanism and it supports enactment of federal baseline privacy legislation. See FTC, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, FTC Report (Mar. 2012), available at <http://ftc.gov/os/2012/03/120326privacyreport.pdf>. But see *id.* App. C (Dissenting Statement of Commissioner J. Thomas Rosch).

requested service or transaction (e.g., a wallpaper app or an app that tracks stock quotes does not need to collect location information);⁴ (2) establish standards that address data collection, transfer, use, and disposal, particularly for location data; and (3) provide consumers with more prominent notice and choices where location data is collected and shared with third parties.

Second, on a related note, the FCC Public Notice asks whether consumers are given meaningful notice and choice in this area. We believe that providers of mobile products and services must do a much better job of providing consumers with basic information about what information they are collecting, how it is used, and what third parties gain access to it. Recently, FTC staff released a report on mobile apps for children.⁵ This report found that in virtually all cases, neither app stores nor app developers provide disclosures that inform parents what data the apps collect from children, how the apps share the data they collect, or with whom they share the data. The report recommended that all members of the children's app ecosystem – including the stores, developers, and third parties providing services – should play an active role in providing key information to parents. The report also encouraged app developers to provide information about data practices simply and succinctly.

In addition, the Commission recently hosted two workshops that examined specific aspects of the mobile ecosystem. In April of 2012, the FTC held a workshop to explore developments in the mobile payments industry, which included an examination of the privacy and data security concerns that may arise from the growing adoption of such technology.⁶ In May, the FTC hosted a workshop that examined mobile privacy disclosures.⁷ Panelists examined how short, effective, and accessible privacy disclosures could be made on mobile devices, discussing research on how consumers interact with existing disclosures, the use of icons to depict privacy practices, and the use of layered disclosures, among other things. Based upon the record, FTC staff expects to issue guidance to inform industry, consumers, and policy makers that would address technological advancements and marketing developments that have emerged since the FTC first issued its online advertising disclosure guidelines known as “Dot

⁴ As noted in the Privacy Report, companies may also collect and use data for limited purposes that extend beyond simply product or service delivery. For example, use of data for product improvements such as website redesign or safety improvements would likely be considered consistent with the context of the consumer's interaction. See FTC, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, FTC Report at 40 (Mar. 2012), available at <http://ftc.gov/os/2012/03/120326privacyreport.pdf> (Rosch, dissenting).

⁵ FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), available at http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtml.

⁶ FTC, *Paper, Plastic . . . or Mobile? An FTC Workshop on Mobile Payments* (Apr. 26, 2012), available at <http://www.ftc.gov/bcp/workshops/mobilepayments/>.

⁷ FTC, *In Short – Advertising & Privacy Disclosures in a Digital World* (May 30, 2012), available at <http://www.ftc.gov/bcp/workshops/inshort/index.shtml>.

Com Disclosures.”⁸

Third, the FCC Public Notice requests comments about the concept of privacy by design. In addition to the extensive discussion of this issue in its Privacy Report, the FTC’s enforcement efforts have underscored the importance of privacy by design. For example, the FTC has recently challenged the privacy and security practices of several leading technology companies, many of which operate in the mobile space. In its cases against Facebook, Google, and Myspace, the FTC alleged that each of the companies misrepresented its privacy practices to consumers. In each case, the company’s failure to implement privacy by design contributed to the alleged misrepresentations. As a remedy, the FTC negotiated orders with the companies that contained strong injunctive relief, including a requirement that the companies establish comprehensive privacy and information security programs that are subject to review by independent third-party auditors.⁹ These order provisions can serve as guidance for other companies seeking to implement privacy by design. And in the case of Google, the existing order provides protections for consumers using the Android operating system.

Fourth, the FCC Public Notice raises several questions about appropriate data security in the mobile environment. Here, the FTC’s enforcement actions can serve as a guide. The FTC has brought 40 data security cases, alleging that companies engaged in data security failures by, among other things, storing sensitive data in clear text, failing to maintain strong passwords, failing to use updated anti-virus and anti-spyware software, failing to implement appropriate firewalls and the like. These enforcement actions can provide guidance to all actors in the mobile ecosystem. Additionally, technological advances in the mobile area, such as the use of end-to-end encryption and dynamic data authentication, may lead to best practices that offer the potential for increased data security in certain contexts, such as mobile payments.¹⁰

Fifth, the FCC Public Notice asks whether consumers should bear responsibility for the

⁸ FTC, *Dot Com Disclosures: Information About Online Advertising* (May 2000), available at <http://www.ftc.gov/os/2000/05/0005dotcomstaffreport.pdf>.

⁹ *In the Matter of Myspace, LLC*, FTC File No. 102 3058 (May 8, 2012) (proposed consent order), available at <http://ftc.gov/os/caselist/1023058/index.shtm> (requiring company to implement privacy program subject to independent third-party assessment); *In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), available at <http://www.ftc.gov/os/caselist/0923184/index.shtm> (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/1023136/index.shtm> (requiring company to implement privacy program subject to independent third-party audit); see also *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/0923093/index.shtm> (requiring company to implement information security program subject to independent third-party audit).

¹⁰ See FTC Workshop, *Paper, Plastic . . . or Mobile? An FTC Workshop on Mobile Payments* (Apr. 26, 2012), session 3 transcript pp. 10-12.

privacy and security of their data. Many of the recommendations in the Commission's Privacy Report were aimed at encouraging companies to implement privacy-protective practices so that the burden for protecting privacy would not weigh so heavily on consumers. Currently, consumers face a substantial burden in reading and understanding lengthy and complex privacy policies and exercising the limited choices offered to them. At the same time, consumers must have the tools they need to avoid unwittingly disclosing their personal information through their mobile devices. We have addressed this issue by providing consumers with extensive educational materials on mobile privacy, including tips on securing wi-fi communications, using public wi-fi hot spots, understanding mobile apps, and understanding cookies.

Finally, the Commission's enforcement actions and business education have emphasized to companies operating in the mobile space that existing laws protecting privacy, data security, and other consumer protections apply to them. For example, in an action against the developer of mobile apps, including children's games for the iPhone and iPod touch, the FTC alleged that a company illegally collected and disclosed personal information from children under age 13 without the required parental consent.¹¹ In addition to imposing a \$50,000 penalty on the app developer, the consent order resolving the allegations requires the developer to delete improperly collected information. The order not only guided the individual company's future conduct, but also serves to condition the marketplace by providing important guidance to other industry members.

In another example, the FTC sent letters to the marketers of six mobile apps that provide background screening services.¹² The FTC warned the apps marketers that, if they have reason to believe the background reports they provide are being used for employment screening, housing, credit, or other similar purposes, they must comply with the Fair Credit Reporting Act ("FCRA"). The FCRA protects the privacy of sensitive consumer report information and ensures that the information is accurate and not used for impermissible purposes. The Commission's letters encourage the companies to review their apps and their policies and procedures to confirm they comply with the FCRA.

The FTC publishes extensive educational materials directed to businesses regarding how they can comply with existing laws and regulations, including in the mobile context, on its Business Center web site and blog.¹³ Topics that the Business Center has covered include how businesses can comply with the CAN-SPAM Act, COPPA, and Do Not Call.¹³

¹¹ *U.S. v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Ca. Sept. 8, 2011) (consent decree), available at <http://www.ftc.gov/os/caselist/1023251/index.shtm>.

¹² See Press Release, FTC, *FTC Warns Marketers that Mobile Apps May Violate Fair Credit Reporting Act* (Feb. 7, 2012), available at <http://www.ftc.gov/opa/2012/02/mobileapps.shtm>.

¹³ See FTC Business Center, available at <http://business.ftc.gov/>.

¹³ See, e.g., FTC, *The CAN-SPAM Act: A Compliance Guide for Business* (Sept. 2009), available at <http://business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business>;

In closing, we hope that this information has been of assistance to the FCC as it considers privacy and security issues with respect to the storage of consumer data on mobile devices. The FTC will continue to devote substantial resources to this area, and we look forward to working with the FCC to ensure that we avoid duplicative actions in areas where our jurisdictions may be overlapping.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Vladeck', with a long horizontal flourish extending to the right.

David C. Vladeck