ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

July 13, 2012

INITIAL COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

To

THE FEDERAL COMMUNICATIONS COMMISION

Privacy and Security of Information Stored on Mobile Communications Devices

CC Docket No. 96–115; DA 12–818 (77 Fed. Reg. 35336)

By notice published on June 13, 2012, the Federal Communications Commission ("FCC") seeks comments on "privacy and data security practices of mobile wireless services providers with respect to customer information stored on their users' mobile communications devices."[1] The Electronic Frontier Foundation ("EFF") agrees that there is a need to refresh the record since the FCC last visited these issues in 2007.

Modern cell phones raise grave and well-known privacy and security issues. A recent UC-Berkeley study of Americans' use of mobile phones and privacy

> "found widespread understanding that sensitive personal information such as text messages, contact lists, and voicemail is stored on phones, and that substantial percentages of respondents with smartphones used them to engage in activities that might generate sensitive information, including visiting websites, using social networks, and using location services.... These activities can reveal communications with circles of contacts, health-related or other personal research queries, and a wide variety of intellectual and political interests, to name just a few revealing types of information."[2]

---

[1] https://www.federalregister.gov/articles/2012/06/13/2012-14496/privacy-and-security-of-information-stored-on-mobile-communications-devices

[2] Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, *Mobile Phones and Privacy*, at 1, 5 (July 11, 2012), available at http://ssrn.com/abstract=2103405

454 Shotwell Street • San Francisco, CA 94110 USA
v +1 415 436 9333 f +1 415 436 9993 i www.eff.org e information@eff.org

Carriers, meanwhile, increasingly collect such data more than ever before. Tools including network-side proxies and consumer device-side monitoring software like Carrier IQ enable carriers to collect large amounts of data about consumers' activity in efficient and organized forms.

Carriers today also appear more interested in using such data for general marketing purposes. Last August, AT&T allowed customers to opt into data use for marketing purposes;[3] Verizon did so on an opt-out basis. As one commenter put it, "Verizon Wireless finally got around to sending a polite email to customers informing them that everything they do on their phones is now used to target them with ads. Policy changes implemented last month allow it to employ browsing history, search terms, location, app and feature usage, and demographic information it buys from other companies to power targeting."[4]

In response to these concerns, EFF proposed a set of baseline mobile "best practices" principles in the format of a Bill of Rights[5] that closely follows the rights enumerated in the White House whitepaper "Consumer Data Privacy in a Networked World."[6] The FCC should consider these consumer rights in evaluating the carriers' obligations.

1. **Individual control**: Users have a right to exercise control over the personal data that applications collect about them and how the applications use it. The right to individual control also includes the ability to remove consent and withdraw that data from service provider servers. The White House whitepaper puts it well: "Companies should provide means of with drawing consent that are on equal footing with ways they obtain consent. For example, if consumers grant consent through a single action on their computers, they should be able to withdraw consent in a similar fashion."

---

[3] http://news.cnet.com/8301-1035_3-20097369-94/at-t-punches-up-targeted-ad-business/.
[4] http://techcrunch.com/2011/11/16/verizon-opt-out/.
[5] https://www.eff.org/deeplinks/2012/03/best-practices-respect-mobile-user-bill-rights.
[6] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

2. **Focused data collection**: EFF had earlier set forth standard best practices for online service providers.[7] Cellular carriers should be even more careful about concerns unique to mobile devices. Especially sensitive areas include location data, and the contents and metadata from phone calls and text messages. Cellular carriers should only collect the minimum amount required to provide the service, with an eye towards ways to achieve the functionality while anonymizing personal information. The concept of "privacy by design" is critical here, given that cellular communications are strongly associated with device identifiers.

3. **Transparency**: Users need to know what data their carrier is accessing, how long the data is kept, and with whom it will be shared. Users should be able to access human-readable privacy and security policies, both before and after installation. Transparency is particularly critical in instances where the user does not directly interact with the application (as with, for example, Carrier IQ).

4. **Respect for context**: Data should only be used or shared in a manner consistent with the context in which the information was provided. When a cellular carrier wants to make a secondary use of the data, it must obtain explicit opt-in permission from the user.

5. **Security**: Cellular carriers are responsible for the security of the personal data they collect and store. That wireless communications are physically accessible "through the air" for readily than wired communications means, for example, that transmissions should be encrypted wherever possible, and that data moving between a phone and a server should always be encrypted at the transport layer.

6. **Accountability**: Ultimately, all actors in the mobile industry are responsible for the behavior of the hardware and software they create and deploy. Users have a right to accountability.

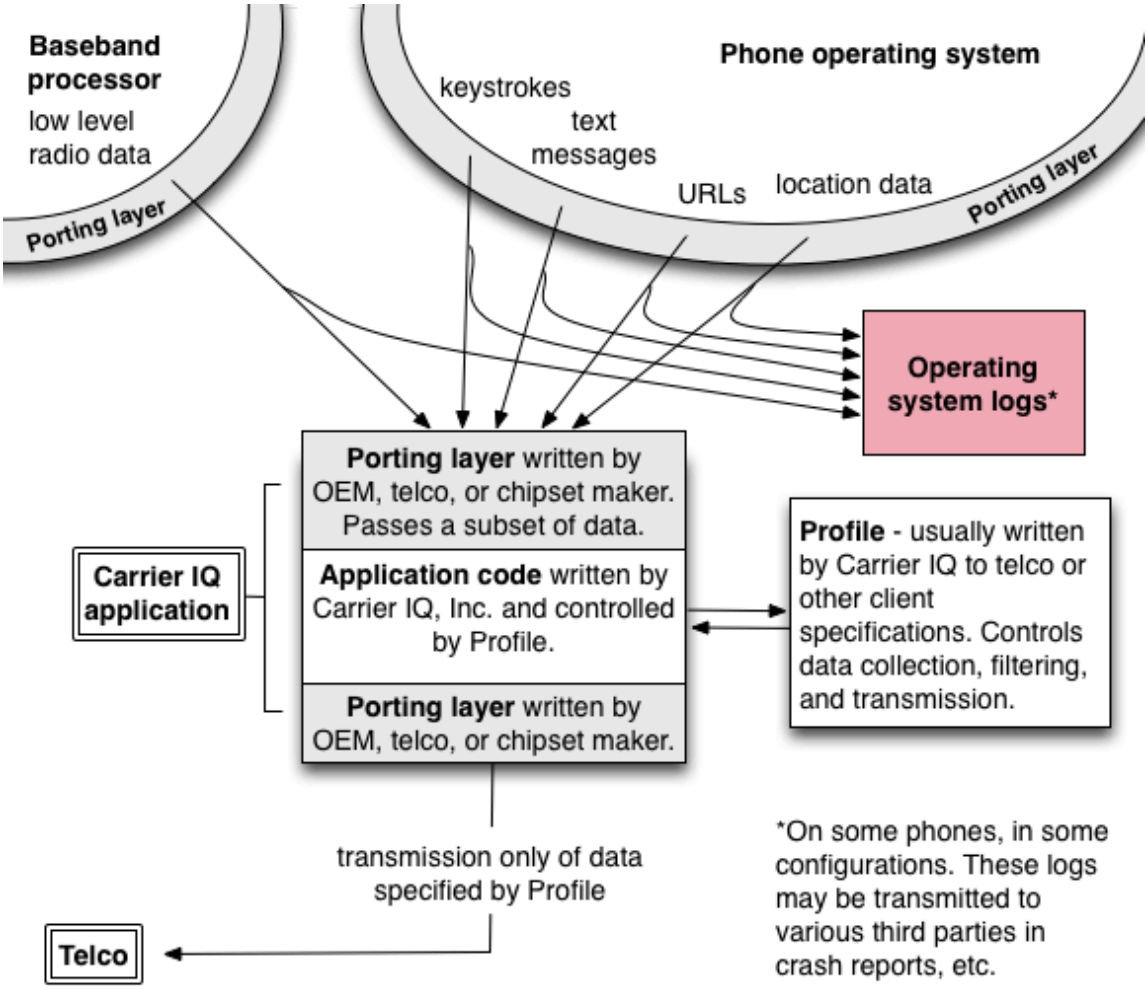
Evolving Carrier Practices

In response to the 2007 Further Notice, carriers told the Commission that consumers control the information residing on their devices. This assertion is not true today. The use of software like Carrier IQ demonstrates that carriers collect more data than before: in documenting the Carrier IQ episode, EFF produced a graphic[8] demonstrating what information the program was collecting, and where it was being sent. On many phones, Carrier IQ was embedded within the OS or baseband firmware, and users were given no clues that it existed. In

---

[7] https://www.eff.org/wp/osp.
[8] https://www.eff.org/deeplinks/2011/12/carrier-iq-architecture.

many deployments, the Carrier IQ stack had access not only to location and radio data, but information about programs running on the phone and URLs entered by the user.



Carrier IQ Architecture
As interpreted by Electronic Frontier Foundation
December 12, 2011 • https://www.eff.org/deeplinks/2011/12/carrier-iq-architecture

Moreover, carriers now collect and store more information about users in records tied to device identifiers. This practice raises new issues: in a 2010 breach of AT&T security, for example, the email addresses of iPad owners were unintentionally exposed.[9]

Notice and Choice

The Commission asks, "Are consumers given meaningful notice and choice with respect to service providers' collection of usage-related information on their devices?" The answer is no. Carrier IQ was deployed in such a way that the average user would not know that it existed, and information about the use of Carrier IQ was ultimately revealed through independent security researcher analysis. Even if this type of software is well known in the industry and the research community, the general public knew little about it. It's not clear that this issue and its bearing on consumer privacy would have otherwise come to light — and consumers certainly haven't been given adequate choice about them.

Even when the issue is not technical, transparency has been lacking. Last September, the release of a Justice Department memo in response to Freedom of Information Act ("FOIA") requests from ACLU and others led to greater public knowledge about how long several major carriers retain data such as cell tower history (for location), customer IP addresses, call logs, text messages and web surfing habits.[10]

More generally, notice and choice alone are not enough under EFF's mobile privacy principles. The UC-Berkeley study suggests that "transparency about how mobile data is

---

[9] http://online.wsj.com/article/SB10001424052748704312104575299111189853840.html.
[10] http://www.wired.com/threatlevel/2011/09/cellular-customer-data/.

collected and used, along with robust user controls and procedural and technical privacy safeguards, may be necessary to avoid backlash against programs that rely on mobile data."[11]

Current Practices

The Commission also asks whether the current carrier practices serve the needs of both providers and consumers. In some areas, the answer is a clear no. For example, location and communication records collected and retained by the carriers are increasingly being handed over to law enforcement agencies — as a recent report shows, federal, state, and local agencies made a minimum of 1.3 million requests to carriers for cell phone data in the last year alone.[12] The Justice Department FOIA-released memo "Retention Periods of Major Cellular Service Providers" tells us that AT&T retains location data about its customers for at least three years, while Sprint retains it for around 18 to 24 months.[13]

By contrast, the UC-Berkeley study found that Americans generally dislike the idea that carriers retain location data: 46% responded that carriers should not retain such data at all, while 28% answered that location data should be kept for less than a year. Obviously, Americans believe that this data should be private, and thus carrier retention policies do not meet the ordinary consumer's needs.

We know relatively little about the carriers' needs and hope that the carriers will provide more information in their comments. That T-Mobile retains cell tower history data for four to

---

[11] *Mobile Phones and Privacy*, at 3.
[12] https://www.eff.org/deeplinks/2012/07/law-enforcement-agencies-demanded-cell-phone-user-info-much-more-13-million-times.
[13] http://www.wired.com/threatlevel/2011/09/cellular-customer-data/.

six months, while AT&T retains such data for three or more years, suggests that there is little genuine carrier need for cell tower history at all.

Similarly, in response to the media coverage of Carrier IQ, Sprint was one of several companies that distanced itself from the software and committed to its removal.[14] Again, if Sprint can operate without the Carrier IQ information, it's unclear why it (or any other similarly situated carrier) needed to collect the data in the first place. If carriers continue such expanded data collection, they must provide meaningful justifications. Furthermore, it's still not clear to consumers what data is being collected by which entities, and what those entities' practices with respect to that data are.

With regard to the question of whether current practices raise concerns about privacy and data security, EFF believes that the answer is a resounding yes. The public response to information about Carrier IQ is one telling example, but there are numerous others. These problems relate not just to data collection, but to the security of data on the device itself, which can be compromised by current carrier practices of delaying or even blocking security updates. EFF reported on this problem in 2011,[15] noting that "[a]lthough Apple, Google, and Microsoft should develop security fixes faster, they are fundamentally limited by carrier intransigence."

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

Parker Higgins

Lee Tien

---

[14] http://news.cnet.com/8301-30686_3-57360436-266/sprint-updates-phones-to-eliminate-carrier-iq/.

[15] https://www.eff.org/deeplinks/2011/03/carrier-intransigence-harms-internet-security.