

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Implementation of the Telecommunications) CC Docket No. 96-115
Act of 1996: Telecommunications Carriers')
Use of Customer Proprietary Network)
Information and Other Customer Information)

**REPLY COMMENTS OF THE
MASSACHUSETTS OFFICE OF THE ATTORNEY GENERAL**

Martha Coakley
Attorney General
Commonwealth of Massachusetts
One Ashburton Place
Boston, MA 02108

July 30, 2012

Table of Contents

I. INTRODUCTION	1
II. BACKGROUND	2
III. COMMENT.....	3
A. Consumers face substantial harms when private information is revealed without their consent.	3
B. The President’s Consumer Privacy Bill of Rights provides a framework for the FCC’s mobile data privacy rules.	5
C. Consumer consent must be context-specific.	6
D. Consumers must have meaningful notice with respect to their personal information.	6
E. Consumers must have meaningful choice with respect to their personal information.	7
F. The Commission should not rely on voluntary measures to protect consumers’ personal information.	8
G. The Commission should be informed by Massachusetts’ privacy requirements for mobile service providers.	9
IV. CONCLUSION.....	15

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Implementation of the Telecommunications) CC Docket No. 96-115
Act of 1996: Telecommunications Carriers')
Use of Customer Proprietary Network)
Information and Other Customer Information)

**REPLY COMMENTS OF THE
MASSACHUSETTS OFFICE OF THE ATTORNEY GENERAL**

I. INTRODUCTION

Martha Coakley, Attorney General of the Commonwealth of Massachusetts (“Attorney General”) hereby submits reply comments in response to the Public Notice (“Notice”) released by the Federal Communications Commission (“FCC” or “Commission”) on May 25, 2012, requesting comments on privacy and security issues related to information that is stored on consumers’ mobile communications devices.¹ These reply comments respond to some, but not all, of the initial comments filed on July 13, 2012 in response to the Notice.²

¹ *Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, CC Docket No. 96-115, Public Notice, DA 12-818, May 25, 2012.

² Comments were filed in CC Docket No. 96-115 on July 13, 2012 by the following parties: Electronic Privacy Information Center (“EPIC”) and Consumer Watchdog; Federal Trade Commission (“FCC”); Center for Digital Democracy (“CDD”); Comments of Greek Orthodox Archdiocese of America, United Church of Christ Office of OC, Inc., and United States Conference of Catholic Bishops (“U.S. Conference of Catholic Bishops et al.”); CTIA – The Wireless Association (“CTIA”); AT&T, Inc. (“AT&T”); The Future of Privacy Forum (“FPF”); Telecommunications Industry Association (“TIA”); TechAmerica; Sprint Nextel Corporation (“Sprint”); New America Foundation’s Open Technology Institute, Benton Foundation, Center for Media Justice, Chicago Media Action, Free Press, Institute for Self-Reliance, Media Alliance, Peoples Production House, Public Knowledge, and the Peoples Channel & Durham Community Media (“Open Technology Institute et al.”); Internet Commerce Coalition; Interactive Advertising Bureau; Information Technology and Innovation Foundation; Electronic Frontier Foundation (“EFF”); Consumer Electronics Association; Common Sense Media; Center for Democracy & Technology; Alliance for

No commenter disputes that privacy is essential to consumers and to their trust of the various service providers in the “wireless ecosystem.” Since the FCC last solicited comment on these issues, technology (and what service providers can do with that technology) has changed dramatically.³ As detailed by the Federal Trade Commission (“FTC”) in their filed comments, the potential for mobile service providers to collect detailed information about consumers has grown and there is generally a “lack of basic privacy protections on many new and emerging mobile products and services.”⁴ The Attorney General agrees with many other commenters that robust privacy and data security protections are essential.⁵

The FCC should require transparency and consumer choice regarding all data collection and sharing. Carriers must handle consumer data in a secure manner and provide consumers with assistance in deleting personal information from their devices.

II. BACKGROUND

In the FCC’s Notice, the Wireless Telecommunications Bureau and Office of General Counsel jointly seek comments regarding information stored on consumers’ mobile communications devices and on whether current privacy and security rules should, or already do, apply to the information.⁶ In 2007, the FCC revised and updated

Telecommunications Industry Solutions (“ATIS”); Verizon Wireless; and Alarm Industry Communications Committee.

³ See Notice, at n. 7.

⁴ FTC at 2. In particular, the FTC expresses concern with location-specific data. *Id.* at 3.

⁵ See, e.g., FTC, at 2; EPIC, at 2; U.S. Conference of Catholic Bishops *et al.*; CDD, at 13-14; Open Technology Institute *et al.*, at 1.

⁶ Notice, at 1.

its rules with respect to customers' private information and sought comment on issues related to mobile devices.⁷ However, the primary focus then was on the ability of consumers to ensure that their private information was completely erased when equipment was refurbished.⁸ As discussed in the Notice, technology and business practices have "evolved dramatically" in the wireless market in the intervening years.⁹ Strong data privacy and security measures are necessary to ensure transparency and consumer control over what information is collected about their purchasing, internet browsing, location and travels, and the content of their communications, and with whom such information is shared.

III. COMMENT

A. Consumers face substantial harms when private information is revealed without their consent.

The unintended disclosure¹⁰ of a consumer's personal and private information can cause economic, physical, and other harms. As the FTC noted in its March 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change* ("FTC Privacy Report"),¹¹ consumers are subject to harm from unanticipated uses of data, including "the unexpected revelation of previously private information, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g.,

⁷ *Id.*, at 2.

⁸ *Id.*

⁹ *Id.*, at 1.

¹⁰ Unintended disclosure includes both on the part of commercial entities and on the part of consumers who do not understand that their personal information is being shared.

¹¹ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, March 2012 ("FTC Privacy Report").

purchase history, employment history) to unauthorized third parties.”¹² As the FTC stated in its comments¹³ and described in its 2012 Privacy Report, “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,” with the potential that location information “could be used to build detailed profiles of consumer movements over time and could be used in ways not anticipated by consumers.”¹⁴

Strong data privacy and security measures are necessary to ensure transparency and consumer control over what information is collected about their purchasing, internet browsing, location and travels, and the content of their communications, and with whom such information is shared. These measures are required to protect consumers, but also, as the White House has recognized: “Strong consumer data privacy protections are essential to maintaining consumers’ trust in the technologies and companies that drive the digital economy.”¹⁵ As detailed by Open Technology Institute et al., the mobile service providers have been “historically unreliable in their disclosure of how and for what purpose they collect [consumers’] data.”¹⁶ Consumers have a right to know how that data is collected and to make decisions about what information they are willing to disclose.

¹² Id., at 8.

¹³ FTC, at 2-3.

¹⁴ FTC Privacy Report, at 33.

¹⁵ White House, *Consumer Privacy In A Networked World: A Framework for Protecting Privacy and Promoting Innovation In The Global Digital Economy*, February 2012 (“White House Consumer Privacy Report”), at 1 (available at: <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>). See, also, Common Sense Media, at 4.

¹⁶ Open Technology Institute et al., at 6-7.

B. The President’s Consumer Privacy Bill of Rights provides a framework for the FCC’s mobile data privacy rules.

The Attorney General echoes the recommendation of other commenters that the FCC utilize the Consumer Privacy Bill of Rights,¹⁷ recently endorsed by President Obama, as a framework for its rules.¹⁸ The White House report, *Consumer Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in a Global Economy*, enumerates the following principles in its Consumer Privacy Bill of Rights:

1. *Individual Control*: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
2. *Transparency*: Consumers have a right to easily understandable and accessible information about privacy and security practices.
3. *Respect for Context*: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
4. *Security*: Consumers have a right to secure responsible handling of personal data.
5. *Access and Accuracy*: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
6. *Focused Collection*: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
7. *Accountability*: Consumers have a right to have personal data handled by companies with appropriate measure in place to assure they adhere to the Consumer Privacy Bill of Rights.¹⁹

¹⁷ White House, *Consumer Privacy In A Networked World: A Framework for Protecting Privacy and Promoting Innovation In The Global Digital Economy*, Feb. 2012 (“White House Consumer Privacy Report”), available at: <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>. The Consumer Privacy Bill of Rights is provided as Appendix A to the report.

¹⁸ See, e.g., EPIC at 2; EFF at 2-3.

¹⁹ White House Consumer Privacy Report, at App. A (Consumer Privacy Bill of Rights).

C. Consumer consent must be context-specific.

The “Context” principle contained in the White House’s Consumer Bill of Rights is an essential component of consumer protection. As noted by EPIC and the White House Consumer Privacy Report,²⁰ consumers have little control over how third parties treat their data, and it is incumbent upon carriers to disclose all purposes for which the data is being collected. Even if a carrier asserts that a primary purpose for collecting certain data is network management and improving service quality, if the carrier then sells the data to a merchant or data broker, that fact must be disclosed, and consumers must consent to that specific use of the data. It is incumbent upon the mobile service provider to seek prior permission (based on accurate and adequate notice) from the consumer if the data is being used in a different manner or different scope for which the consumer originally approved.

D. Consumers must have meaningful notice with respect to their personal information.

The Attorney General acknowledges that there may be legitimate business purposes for which mobile service providers collect personally identifiable information. However, there is simply no excuse for any lack of transparency as to those collection practices. At a minimum, consumers must know the types of information that the service provider collects, when it collects it, the purposes for the collection, uses of the data, how frequently the data is collected or updated, whether and when the data is deleted, what data is shared with third parties, and for what purposes. Disclosures should be clear, conspicuous, and easy to understand, and posted prominently on websites as well as on

²⁰ EPIC, at 11; White House Consumer Privacy Report, at 13.

paper or electronic bills. The Attorney General concurs with the FTC that mobile service providers “must do a 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.”²¹

Many commenters agree that disclosure requirements are essential²² and currently inadequate,²³ however, disclosure should be considered a bare minimum element of any mobile data privacy rules that the Commission ultimately adopts. The Attorney General supports EPIC’s recommendation that carriers provide specific notice to consumers identifying the entities that have gained access to their personal information.²⁴ It is not sufficient to tell consumers that their information may be shared with “third parties.”

E. Consumers must have meaningful choice with respect to their personal information.

As noted above, mere disclosure of mobile data practices is insufficient to protect consumers. The FCC should adopt “opt in requirements” that enable consumers to affirmatively give permission for the collection of personal information as well as sharing of that information with third parties *whatever the stated reason*.²⁵ In the current environment, consumers do not have “meaningful choice”²⁶ with respect to that collection

²¹ FTC at 3.

²² See, e.g., U.S. Conference of Catholic Bishops *et al.*, at 4; EPIC, at 12-13;

²³ See, e.g., Open Technology Institute *et al.*, at 8.

²⁴ EPIC at 13.

²⁵ Many commenters support “opt in” requirements. See, e.g., Open Technology Institute *et al.*, at 8; EPIC, at 9; Common Sense Media, at 2; U.S. Conference of Catholic Bishops, at 4.

²⁶ Notice at 4.

of personal and usage-related information.²⁷ The FCC must go beyond providing consumers tips on how to navigate privacy policies and how to opt out of data collection (when possible), and require some responsibility on the part of the mobile service providers.²⁸ Under no circumstance should wireless providers share consumer information with third parties without “express consent” from consumers.²⁹

F. The Commission should not rely on voluntary measures to protect consumers’ personal information.

The U.S. Conference of Catholic Bishops et al. observe that “currently practices serve the needs of providers much more than the needs of consumers.”³⁰ Indeed, the Commission should reject recommendations by the industry to rely on voluntary measures.³¹ Without proper disclosure and meaningful choice, mobile service providers simply do not have the economic incentive to respect the privacy of consumer data, and protect it from security vulnerabilities. In fact, mobile service providers have an incentive to cut corners with respect to protecting data and privacy, and to sell data to third parties.³² The Attorney General echoes the sentiment expressed by the Center for Digital Democracy that codes of conduct and other voluntary measures “have all failed to

²⁷ U.S. Conference of Catholic Bishops et al., at 4; EPIC, at 9; Open Technology Institute *et al.*, at 1.

²⁸ *See, e.g.* FPF at 9 (recommending a web page with tips for protecting information that is stored on mobile devices).

²⁹ EPIC at 10.

³⁰ U.S. Conference of Catholic Bishops at 5.

³¹ TIA at 8; AT&T at 23; CTIA at 5; Verizon Wireless at 2.

³² *See, e.g.*, IAB, at 1 arguing that mobile marketing is a “tremendous value” to both the economy and consumers; Open Technology Institute *et al.* at 5-6 (“The Internet advertising market in the U.S. is worth an estimated \$300 billion, and the data collection available to carriers through applications like Carrier IQ would provide them with a treasure trove of consumer data to sell targeted ad space and in-depth market research on their customers.”).

ensure that consumers are protected” as evidenced by recent expansions in mobile marketing and data collection.³³

Industry commenters are correct that there are many different entities involved in the mobile applications market.³⁴ However, this does not absolve mobile service providers of any responsibility. The CPNI regulations are neither too complex nor are they “heavy-handed structural and economic regulation”³⁵ that should be thrown out. Any new requirements regarding mobile data privacy need not be “rigid”³⁶ The Commission should reject AT&T’s argument that the adoption of requirements regarding disclosure and consumer choice for mobile data collection and sharing for mobile service providers will “skew competition” and will result in regulatory disparity.³⁷ Mobile service providers have a unique relationship with consumers and provide the link between the device and the public switched telephone network or the Internet.³⁸ The expectation of privacy is likely greater in this situation. In addition, mobile service providers should include a warning in their privacy disclosures that third party applications may have their own privacy policies or none at all.

G. The Commission should be informed by the Massachusetts Attorney General’s experience in enforcing Massachusetts’ Data Security Laws and Regulations.

The FCC asks whether current practices of mobile wireless service providers with

³³ CDD at 11-13.

³⁴ *See, e.g.*, FPF at 6.

³⁵ FPF at 7.

³⁶ AT&T at 5.

³⁷ *Id.* at 3.

³⁸ *See, e.g.* CDD at 2-3 (“mobile devices, no longer a luxury or merely an option, have become a fundamental part of the communications and marketing landscapes . . . these devices are unique, with specially designed user interfaces that raise significant consumer protection and privacy issues.”).

respect to information stored on their customers' mobile communication devices raise consumer privacy and data security concerns and/or "create actual data-security vulnerabilities, and whether "privacy and data security should be greater considerations in the design of software for mobile devices[.]” The Attorney General is charged with enforcing the Massachusetts Data Disposal Law (M.G.L. c. 93I), and the Massachusetts' Data Security Regulations (201 CMR 17.00 *et seq.*), which together set forth minimum standards meant to safeguard the security of data (including electronic data) consisting of or containing personal information of Massachusetts residents. The Attorney General's enforcement experience of Massachusetts data security laws shows that there are unique data-security risks and vulnerabilities associated with mobile communication devices that can be reduced or ameliorated through implementation and enforcement of minimum data security standards. The Commission should be informed by the Massachusetts experience, and establish rules that require mobile service providers to assess the risks associated with their goods and services to their users' data - whether stored by the user on his or her device, and/or accessed, used, processed, maintained, stored, or sold by the mobile service provider – and incorporate and implement privacy and security safeguards and controls that protect that data from unauthorized use, access, or disclosure.

1. Mobile communication devices are subject to unique security vulnerabilities.

As observed by the FTC in its 2012 Privacy Report (at 33), “[t]he 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.” The Attorney General adds that these same characteristics raise numerous security concerns. For example, portable communication devices are particularly susceptible to loss or theft, and

the data thereon susceptible to unauthorized access or use.³⁹ The devices are often enabled and used to send highly personal data via wi-fi or data networks, and such data is thus vulnerable to unauthorized interception. Malware or viruses can infect the devices via e-mail attachments or downloaded mobile applications. To the extent a mobile service provider accesses data from a user's device and incorporates it onto their own computer systems, security vulnerabilities within those systems (such as the failure to update anti-virus and anti-spyware software, poor password management, lack of data encryption, and inadequate firewall protections) lead to additional risks of unauthorized use and disclosure of user data.⁴⁰

2. The Commission should adopt rules establishing minimum security safeguards of data stored on or accessed from mobile communication devices.

Massachusetts' approach to data security provides a useful model for how to address these security vulnerabilities and risks. Massachusetts' "Standards for the Protection of Personal Information of Residents of the Commonwealth" (201 CMR 17.00 *et seq.*), enforced by the Attorney General, applies to any entity that owns, licenses or "receives, stores, maintains, processes, or otherwise has access to personal information"

³⁹ See *In re Maloney Properties, Inc.*, Civil Action No. SUCV2012-1127 (Mass. Sup. Ct., Mar. 21, 2012) (Employee left laptop containing unencrypted PI of 621 Massachusetts residents unsupervised in automobile overnight. The laptop was stolen and never recovered); *In re Belmont Savings Bank*, Civil Action No. SUCV2011-02774 (Mass. Sup. Ct. July 28, 2011) (unencrypted backup computer tape containing personal information of 13,380 Mass. residents was left on a desk overnight and inadvertently discarded by the evening cleaning crew).

⁴⁰ See *Commonwealth of Massachusetts v. Briar Group, LLC*, Civil Action No. SUCV2011-01185 (Mass. Sup. Ct., Mar. 28, 2011) (malcode installed on company's point-of-sale computers due to poor password management and insufficient security over remote access utilities and WiFi networks allowed hackers access to payment card info of tens of thousands of customers stored on central computer system); *In re The TJX Companies, Inc.*, Civil Action No. SUCV2009-2602 (Mass. Sup. Ct., Jun. 23, 2009) (insufficient data security over computer network system resulted in data breach of thousands of consumers' personal data). See also Perloff, Nicole, *Even Big Companies Cannot Protect Their Data*, NY TIMES ONLINE, Jan. 17, 2012 (reporting that recent attacks at major online retailers "point to an unsettling new world in which even the supposed stalwarts of the Internet — Amazon, eBay and even the security giants paid to keep hackers at bay — cannot seem to keep personal information safe").

of Massachusetts residents “in connection with the provision of goods or services or in connection with employment.”⁴¹ Covered entities must develop, implement, and maintain minimum administrative, technical, and physical safeguards protecting “personal information.” “Personal information” consists, with limited exceptions, of a resident’s first and last name, together with that resident’s Social Security number, driver’s license number or state-issued identification card number, or financial account number (including credit or debit card number).⁴²

The regulations enumerate numerous, specific safeguards that must be implemented and maintained with respect to personal information.⁴³ Certain of those safeguards apply with particular force to mobile communications devices. For example, a covered entity that stores or transmits personal information must ensure that such personal information is encrypted if it is to travel over public networks, transmitted wirelessly or stored on portable devices.⁴⁴ Results from a 2011 Data Breach Notifications Report issued by the Massachusetts Office of Consumer Affairs and Business Regulation highlight the effectiveness of encryption as a data security safeguard for portable devices: if all portable devices had been encrypted from 2007 to 2011, the number of residents whose personal information was compromised would be lowered by 47 percent, or 1,490,308 Massachusetts residents.⁴⁵

⁴¹ 201 CMR 17.02.

⁴² Mass. Gen. L. c. 93H, § 1.

⁴³ *See generally*, 201 CMR 17.03 and 17.04.

⁴⁴ 201 CMR 17.04(3), (5).

⁴⁵ 2011 Data Breach Report, at 4.

The regulations further require minimum safeguards for personal information stored on systems connected to the internet, including reasonably up-to-date firewall protection, operative system security patches, system security agent software with malware protection and virus definitions.⁴⁶ Additionally, where a covered entity contracts with a third party service provider, it must take reasonable steps to ascertain that the provider is capable of maintaining appropriate security measures and require that provider by contract to implement and maintain such appropriate security measures for personal information.⁴⁷

Importantly, while the Massachusetts Data Security regulations impose minimum security standards, they do not endeavor to impose “one-size-fits-all” requirements to be applied uniformly. Such flexibility seems especially appropriate given the diversity of entities that operate within the mobile communication device space. The requirements imposed by the regulations are by their terms scalable to the size, scope and type of business, the amount of stored data, and the need for security and confidentiality of the data.⁴⁸ Additionally, the minimum computer system security standards enumerated in 201 CMR 17.04 are by design intended to be responsive to technological changes. For example, the regulations apply a standard of technical feasibility.⁴⁹ They are further technology neutral with respect to the security requirements for personal information

⁴⁶ 201 CMR 17.04(6), (7).

⁴⁷ 201 CMR 17.03(f).

⁴⁸ 201 CMR 17.03(1) (requiring covered entities to “develop, implement, and maintain a comprehensive, written information security program containing specific administrative, technical and physical safeguards appropriate to the size, scope and type of business of the entity, the amount of resources available to the entity, the amount of data at issue, and the need for security and confidentiality of the data.”).

⁴⁹ 201 CMR 17.04 (requiring entities to establish and maintain “a security system covering its computers, including any wireless system” that includes minimum security elements “*to the extent technically feasible*”) (emphasis added).

stored or transmitted electronically, including encryption.⁵⁰ Such flexibility ensures that the safeguards mandated by the regulations are tailored to the specific characteristics of a given entity, the sensitivity of the personal data at issue, and the particular security risks threatening that data.

The Commission should establish minimum security standards requiring entities operating within the mobile communications industry to develop, implement, and maintain with respect to data stored on or accessed from their users' portable communication devices. Such security standards should incorporate specific protections in light of the unique characteristics of the communication devices and the manner in which they are intended to be used – including for example protections such as data encryption, wireless network security, robust password and user authentication protocols, firewall and virus protections, and policies and procedures designed to restrict unauthorized individuals from access to users' data. The Attorney General urges the Commission to look to the Massachusetts Data Security Regulations as a useful framework for such standards.

3. The Commission should adopt rules to require the deletion of all personal information by carriers before phones are refurbished and resold.

Similar security concerns are raised with respect to the refurbishment and resale of used portable communications devices. Massachusetts Data Disposal Law is meant to protect against data breaches resulting from improper destruction or disposal of personal information of Massachusetts residents.⁵¹ The law requires that any destruction or

⁵⁰ See generally, 201 CMR 17.04

⁵¹ Mass. Gen. Law c. 93I, *et seq.*

disposal of electronic media and other non-paper media that contains personal information of a Massachusetts resident be done in such a manner so that the “personal information cannot practically be read or reconstructed.”⁵²

The Commission should adopt similar standards with respect to the refurbishment and resale of portable mobile devices. Consumers must have assurances that their personal information will not remain on mobile devices if they recycle those devices. Carriers should be required to ensure that all personal information is deleted before phones are refurbished and resold. Moreover, carriers should provide easy to follow instructions for consumers to delete their personal information before they recycle mobile devices or in the case of handset loss. At present they do not.⁵³

IV. CONCLUSION

The Attorney General commends the FCC for recognizing the technological changes that have taken place in the mobile telecommunications market. As stated in the White House’s Consumer Privacy Report: “Privacy protections are critical to maintaining consumer trust in networked technologies.”⁵⁴ Voluntary mechanisms are insufficient to adequately protect consumers’ data privacy. Therefore, the Attorney General urges the FCC to strengthen its rules in a timely manner to protect consumers.

⁵² Mass. Gen. Law c. 93I, § 2(b).

⁵³ AT&T’s Privacy Policy webpage includes a link to the CTIA’s “Go Wireless Go Green” webpage with regard to deleting information from one’s handset. From there, the consumer must navigate the website to find the link for device-specific instructions (which brings the consumer to yet another website: <http://www.securetradein.com/dataeraser/>). After entering the type of device, the consumer must enter their e-mail address and register to receive any additional instructions. If the consumer registers, he or she will receive a link they must “click” to download a pdf file with instructions. The e-mail includes admonitions that the instructions are proprietary and may not be transmitted by e-mail or reproduced in any manner.

⁵⁴ White House Consumer Privacy Report, at i. See, also, FPF, at 8.

The rules should require transparency, context-specific customer notification, and consumer choice through “opt-in” mechanisms rather than “opt-out” requirements.

Further, given the unique security vulnerabilities to data stored or accessed from mobile communication devices, the Commission should establish minimum security standards to ensure that their consumers’ personal data is protected from unauthorized use and disclosure, and ultimately destroyed if the device is refurbished.

Respectfully submitted,

MARTHA COAKLEY,
ATTORNEY GENERAL

/s/Stephanie Kahn

By: Stephanie Kahn, Chief
David W. Monahan, Deputy Chief
Sara Cable, Assistant Attorney General
Consumer Protection Division
Office of the Attorney General
One Ashburton Place, 19th Floor
Boston, MA 02108

/s/Jesse S. Reyes

By: Jesse S. Reyes, Chief
Sandra Merrick, Deputy Chief
Office of Ratepayer Advocacy,
Office of the Attorney General
One Ashburton Place, 18th Floor
Boston, MA 02108

July 30, 2012