

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

In the Matter of)
Facilitating the Deployment of)
Text-to-911 and Other Next) PS Docket No. 11-153
Generation 911 Applications) PS Docket No. 10-255
Framework for Next)
Generation 911 Deployment)

**Reply Comments of the Samuelson-Glushko
Technology Law & Policy Clinic (TLPC)**

via electronic filing
November 17, 2014

Trip Nistico
Spencer Rubin
Vickie Stubbs
Student Attorneys
Prof. Blake E. Reid
Director
Samuelson-Glushko
Technology Law & Policy Clinic (TLPC)
Robert & Laura Hill Clinical Suite
404 UCB, Boulder, CO 80309-0404
blake.reid@colorado.edu
303.492.0548

Summary

Text-to-911 (“TT911”) is a vital service, and it is necessary to include enhanced location information with texts to 911 so that emergency responders can better save lives. However, it is critical to weigh the public safety benefits of disclosing enhanced location information with the potential for serious privacy and cybersecurity problems that can happen during the collection of location information.

For that reason, we believe that the Commission should consider notice, authorization, and use limitations when making rules for enhanced location information collection. We propose that the Commission use the Fair Information Practice Principles (FIPPs) as a framework for addressing privacy concerns. FIPPs are widely accepted standards through which public and private entities ensure that they themselves respect and protect the privacy of individuals from whom they collect information.¹

In particular, the Commission should require mobile device operating system developers and text message application developers to provide consumers with detailed and transparent notice of how their enhanced location information will be shared when they text 911. We also urge the Commission to consider adopting rules that will allow people to opt-out of automatically sharing their location with 911.

Furthermore, the Commission should require that enhanced location information be embedded in or attached to text messages—an approach that provides the best balance between location accuracy and cybersecurity. Finally, the Commission should seek to limit the use of enhanced location information that is collected when people text 911 so that it is only used within the context of the emergency to which it pertains.

¹ See *Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, The White House, 1 (Feb. 23, 2012) (“*White House FIPPs*”) (attached as Appendix), <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

Table of Contents

Summary	i
Discussion.....	1
I. The Commission should ensure that people receive notice that their enhanced location information will be shared when they text 911.....	4
A. The Commission’s approach to notice will frame people’s expectations for whether and how enhanced location information will be shared with texts to 911.....	5
B. The greatest number of people will receive notice of enhanced location information sharing if mobile devices and text-messaging applications provide this notice.....	5
C. The Commission should launch an educational campaign to ensure that people are aware their enhanced location information will be transmitted when texting 911.....	7
II. To balance safety and privacy interests, the Commission should require that mobile devices and text-messaging applications enable enhanced location sharing for texts to 911 by default while allowing users to opt out.....	8
III. The Commission should ensure that mobile device manufacturers and operating system developers do not build in backdoor access capabilities to enhanced location information.....	11
IV. Enhanced location information should only be used to locate people in an emergency.....	15
Appendix: White House FIPPs	18

Discussion

The student attorneys at the Samuelson-Glushko Technology & Policy Law Clinic (TLPC) at Colorado Law advocate for the public interest in important public policy and legal matters with technological dimensions.² We urge the Commission to balance public safety concerns against potential privacy and cybersecurity problems during the collection of enhanced location information during TT911 sessions.

In the *Third TT911 FNPRM*, the Commission seeks comment on how retrieving the enhanced location of an individual who has sent a text message to 911 will affect that individual's privacy and security.³ Specifically, the Commission asks what kinds of standards work needs to occur “to enable overriding of privacy settings for emergency texts to 911” and what “security risks” should be addressed when a device's enhanced location settings are overridden.⁴

We applaud the Commission's work towards implementing TT911 rules, and we strongly support the Commission's proposal to implement enhanced location sharing for 911 texts. We believe that the public safety benefits of being able to text 911 are substantial, particularly for people with speech or hearing disabilities and others in dangerous situations for whom making a voice call to 911 is impracticable or even life-threatening.

As with any new form of location tracking, however, enhanced location sharing for TT911 will have substantial privacy implications that the Commission should carefully consider—implications underscored by other commenters. In particular, we agree with the National Emergency Number Association (NENA) that the Commission should “focus on ensuring

² These comments reflect the views of the TLPC and not those of any other organizations or individuals.

³ *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment*, Second Report and Order and Third Further Notice of Proposed Rulemaking, PS Docket Nos. 10-255 and 11-153, 29 FCC Rcd. 9846, 9889-90, ¶¶ 100, 103 (Aug. 13, 2014) (“*Third TT911 FNPRM*”), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-118A1_Rcd.pdf.

⁴ *Id.*

consumer privacy” and that there is a “delicate balance” between safety and privacy when enhanced location is used to improve emergency response times.⁵ We also agree with CTIA—The Wireless Association that the Commission should not promulgate any additional rules mandating enhanced location for 911 “[w]ithout resolving . . . important privacy and cybersecurity issues.”⁶

However, we disagree with CTIA that addressing privacy and cybersecurity considerations should dissuade the Commission from adopting an enhanced location requirement at this time.⁷ Protecting privacy, cybersecurity, and public safety is not only critical, but also possible to achieve now. The Commission has all it needs to enact rules that will both improve emergency response times and respect the privacy and cybersecurity interests of people who text 911. Accordingly, the Commission should move ahead with its proposed enhanced location rules while simultaneously enacting clear privacy and cybersecurity protections.

To balance public safety, privacy, and cybersecurity we recommend that the Commission follow the guidelines of the Fair Information Practice Principles (“FIPPs”).⁸ FIPPs are internationally recognized as necessary practices for protecting privacy information about individuals and providing a framework for regulations that address data protection matters.⁹ In 1973, the Secretary of Health, Education, and Welfare’s Advisory Committee on Automated Personal Data Systems created FIPPs to afford “individual[s] a right to participate in deciding what . . . disclosure and use will be made of [their] identifiable information.”¹⁰ Both Congress

⁵ See *Comments of NENA*, 8 (Oct. 16, 2014), <http://apps.fcc.gov/ecfs/document/view?id=60000973944>.

⁶ See *Comments of CTIA*, 12 (Oct. 16, 2014), <http://apps.fcc.gov/ecfs/document/view?id=60000973930>.

⁷ See *id.*

⁸ See *White House FIPPs*.

⁹ Robert Gellman, *Fair Information Practices: A Basic History*, 1 (2.12 ed. Aug. 3, 2014), <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

¹⁰ U.S. Dept. of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems*, 41 (1973), available at <http://www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf>.

and other domestic and foreign governmental entities have enacted laws and regulations implementing various versions of FIPPs to better tailor the privacy framework to the nature of the system in question and the type of information that needs to be protected.¹¹

The version of FIPPs endorsed by the White House in 2012 is ideal for protecting the enhanced location information collected during communications with 911.¹² The White House has deemed its version of FIPPs a standard that “provides a baseline of clear protection for consumers” for “the interactive and highly interconnected environment” in which people’s private data information may be collected.¹³

The FIPPs, at their core, require entities that collect and store people’s personal information to carefully safeguard that data. Under FIPPs, an entity ensures that it will:

- Be “transparent” with—*i.e.*, give notice to—individuals prior to collecting their personal data;¹⁴
- Give “control” to individuals over the collection of their personal data;¹⁵
- Collect personal data in a secure and responsible manner;¹⁶
- Use personal data only within the “context” of the original collection and intended use.¹⁷

Using this framework, we urge the Commission to require that:

¹¹ *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a, as amended (mandating that federal agencies follow FIPPs-like requirements); Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, at 14-15, OECD Doc. C(2013)79 (July 11, 2013), *available at* http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (describing eight FIPPs that are recommended for adoption by member nations).

¹² *See White House FIPPs* at 1.

¹³ *See id.*

¹⁴ *See id.*

¹⁵ *See id.*

¹⁶ *See id.*

¹⁷ *See id.*

- Mobile devices and text-messaging applications give people adequate notice that text-messaging applications will share enhanced location information when texting 911;
- Mobile devices and text-messaging applications give people the ability to opt out of automatically sharing enhanced location information when texting 911;
- Text-messaging applications embed or attach enhanced location information into 911 text messages when people send them, rather than permitting PSAPs to request the information at will; and
- Mobile carriers and text-messaging service providers dispose of any location information that they have obtained once the emergency is over.

I. The Commission should ensure that people receive notice that their enhanced location information will be shared when they text 911.

American citizens will have a strong interest in knowing that TT911 capability exists and how it works—and in particular, how texting 911 might involve unexpected sharing of location information. Indeed, the imposition of FIPPs necessitates that any entity that collects or shares personal data—such as location information—should give people the right to easily understandable and accessible information about collection and sharing.¹⁸

Because TT911 sits at the intersection of conflicting expectations about location disclosure regimes for non-emergency texting and for calling 911, the notice regime for TT911 will significantly impact consumers' expectations around TT911 technology in the long-term. Mobile device operating system developers and text-messaging application developers may be in the best position to alert people of the location-sharing attributes of TT911 functionality. However, we also urge the Commission to consider launching an educational campaign explaining how people's enhanced location information will be shared automatically when they send an emergency text message.

¹⁸ *Id.*

Finally, if the Commission does not implement any other FIPPs standards, it should require notice as a bare minimum. Notice is paramount because people may not necessarily know or understand that enhanced location information will be appended to texts to 911.

A. The Commission’s approach to notice will frame people’s expectations for whether and how enhanced location information will be shared with texts to 911.

When people place voice calls to 911, they are likely to have a clear expectation that their location will only be transmitted during the duration of the call. However, when people text 911, they may not have any expectation of how their location will be tracked—and may expect that it will not. Indeed, the Commission has warned the public that, even if they live in an area where TT911 is available, the 911 call taker *will not* automatically receive their location.¹⁹

Accordingly, it is essential that people receive notification of the new enhanced location tracking capability of TT911. This notification should reassure them that location information appended to texts to 911 will only be collected and used in the context of the emergency.

People will continue to place their trust in 911 if they can send a text message and have a clear expectation of how their enhanced location information will be shared. The Commission should adopt a rule to ensure that mobile devices and text-messaging applications give people notice that their enhanced location information will be shared with mobile carriers and PSAPs when they text 911.

B. The greatest number of people will receive notice of enhanced location information sharing if mobile devices and text-messaging applications provide this notice.

The Commission should adopt an approach to notice that requires mobile devices and text-messaging applications to notify its users of TT911 enhanced location tracking measures using methods that are consistent with operating system- and application-specific user interface

¹⁹ Federal Communications Commission, *Quick Facts & FAQs: Text-to-911*, 2, <http://transition.fcc.gov/cgb/consumerfacts/text-to-911-faq.pdf> (last visited Nov. 16, 2014).

patterns. While we do not believe that the Commission should afford developers flexibility in providing notice, we offer several illustrative examples of notice provisions.

Because the default text-messaging platform for a mobile device is often tied to a device's operating system, mobile devices could provide notice to users that their location will be automatically shared when they send an emergency text message. Mobile devices would provide this notice by presenting the user with a dialogue or other notification following the update of the device's operating system that makes automatic location possible when texting 911.²⁰

As soon as a device completes the operating system update, it could notify its user that her enhanced location information will automatically be transmitted to 911 when she sends a text message to 911—and that privacy settings applicable to non-emergency texts might be overridden in order to do so. Developers could also provide this same notice during the initial set-up of new devices in order to ensure that people migrating from legacy mobile devices to newer smartphones receive the same notice. Because mobile device operating system developers routinely include similar notifications in the operating system installation process—for example, to alert users of other new system features—the financial and technical burden of doing so for TT911 should be relatively low.

While there are many options for how mobile devices and text-messaging applications can provide people with notice of TT911 enhanced location capability, we urge the Commission to ensure that these entities do not simply append this information to their terms of service. Recent studies demonstrate that few people read the terms of service when signing up for new online services, making it unlikely that terms of service will succeed in providing widespread notice of TT911's new automatic location sharing capabilities.²¹

²⁰ The notice should also make clear that users may not be able to text 911 in all locations.

²¹ For example, one study showed that 7% of Britons read the online terms and conditions when signing up for products and services. See Rebecca Smithers, *Terms and conditions: not reading the small print can mean big problems*, The Guardian (May 11, 2011), <http://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems>.

Finally, modern smartphone operating systems generally afford users the ability to disable location sharing generally and on a per-application basis.²² Accordingly, text-messaging applications should provide notice to people that enhanced location will still be shared with mobile carriers and PSAPs when texting 911 even if people turn “off” their location sharing default settings for those applications.

C. The Commission should launch an educational campaign to ensure that people are aware their enhanced location information will be transmitted when texting 911.

In addition to requiring in-application notice, the Commission should also consider launching a simple education campaign discussing the ability to send emergency text messages and how new automatic location capabilities for TT911 will work. The Commission could conduct this campaign similar to its campaign on the limitations of TT911.²³

This campaign could be funded by the government or through the carriers themselves. We do not believe that funding should be a major issue because the campaign could be carried out online, as many of the Commission’s campaigns have been in the past.²⁴ Furthermore, information on automatic location capabilities for TT911 could simply be appended to existing Commission TT911 guides.

However, the Commission should not forgo imposing any notice requirements on mobile devices and text-messaging applications because it has made the information available through an education campaign of this type. We believe that these approaches are complementary. On one hand, requiring various text-messaging platforms to provide notice would ensure that the

²² See, e.g., Apple, *Understanding privacy and Location Services on iPhone, iPad, and iPod touch with iOS 8*, <http://support.apple.com/en-us/HT6338> (last visited Nov. 17, 2014); *Location in Google Settings*, Google, <https://support.google.com/accounts/answer/3118687?hl=en> (last visited Nov. 17, 2014).

²³ *Quick Facts & FAQs: Text-to-911* at 1.

²⁴ For example, the Commission recently launched an educational campaign online to assist people in spotting unauthorized charges on their wireless bill. See *Consumer Guide: Cramming – Unauthorized Charges on Your Phone Bill*, Federal Communications Commission, <http://transition.fcc.gov/cgb/consumerfacts/cramming.pdf> (last visited Nov. 12, 2014).

greatest number of people are made aware that this capability exists. On the other hand, the Commission could provide more detailed information on the capabilities and limitations of TT911 location features. We envision that mobile devices and text-messaging applications would provide notice that the capability exists in a quick and unobtrusive way, and that those people that sought further information could then find it using a quick web search.

II. To balance safety and privacy interests, the Commission should require that mobile devices and text-messaging applications enable enhanced location sharing for texts to 911 by default while allowing users to opt out.

While giving people notice of enhanced location sharing capabilities is an acceptable baseline privacy protection, the Commission should also address how people authorize the transmission of their enhanced location information. The imposition of FIPPs requires that any entity that collects or uses personal data should give people the “right to exercise control over” the “collect[ion]” of that data.²⁵ Strict application of this principle to the sharing of enhanced location information would require the Commission to bar mobile devices and text-messaging applications from sharing enhanced location information with mobile carriers and PSAPs without express authorization from consumers. However, we believe that the exigent emergency circumstances surrounding a TT911 session necessitate a different regime: sharing location with texts by default while allowing users to opt out.

In an emergency, we believe most people will want their enhanced location information automatically transmitted as soon as possible in order to save lives and quickly receive help. It would be redundant, inefficient, and potentially dangerous for a mobile device or texting application to continually seek authorization from people to share their enhanced location, which could delay a response to the scene of the emergency. Common sense dictates that the Commission should not always seek authorization from people before automatically sharing their enhanced location information with 911.

²⁵ *White House FIPPs* at 1.

There are special circumstances, however, in which people will not want to share their enhanced location information with 911. For example, a person may want to report an emergency that she witnessed in a completely different location from her own, but not want to be identified by having law enforcement show up at her current location. Many PSAPs will allow voice callers to remain anonymous upon request, and many PSAPs even have detailed standard practices by which to handle anonymous callers.²⁶ Anonymous 911 calls also appear to play a significant role in the reporting of narcotics or gang-related activity.²⁷

This type of protection given to 911 callers should also be extended to 911 texters. There are already “numerous examples” of metropolitan areas that have deployed SMS via 4, 5, or 6-digit short codes in order to receive anonymous emergency text messages.²⁸ The Association of Public-Safety Communications Officials (APCO) has applauded this practice, noting that the “anonymity afforded [to] the users” has resulted in these PSAPs “receiving information on incidents that may otherwise go unreported.”²⁹

The Commission should strike a balance between promoting safe and efficient emergency responses and respecting people’s privacy. The Commission can do so by requiring that mobile devices and text-messaging applications share location by default, accommodating the majority of people who would accept the automatic transmission of their enhanced location information, while still allowing people who do not want to share their location to opt out.

²⁶ See, e.g., *Tips on Calling 911*, Chicago Police, <https://portal.chicagopolice.org/portal/page/portal/ClearPath/Communities/Safety%20Tips/Tips%20for%20Calling%20911%20and%20311> (last visited Nov. 16, 2014); *911 for Emergency Services*, District of Columbia Office of Unified Communications, <http://ouc.dc.gov/page/911-emergency-services> (last visited Nov. 16, 2014).

²⁷ See, e.g., *Chicago 911 System Info*, Metro Chicago Fire, <http://www.metrochicagofire.com/911.htm> (last visited Nov. 12, 2014).

²⁸ *Text Messages in a PSAP Environment*, APCO International, at 18 (Sept. 30, 2012), <https://www.apcointl.org/doc/911-resources/white-papers/374-text-messages-in-a-psap-environment/file.html>.

²⁹ *Id.*

Thus, we recommend that the Commission require an ‘opt-out’ default regime in which mobile devices and text-messaging applications automatically share enhanced location information with mobile carriers and PSAPs unless a person has turned sharing “off.” Mobile devices and text-messaging applications would not need people’s authorization to share their enhanced location information in the vast majority of circumstances, but would afford people the choice to deauthorize sharing under circumstances where they wish to text 911 anonymously.

Operating system developers and text message application developers should not encounter significant technological challenges in implementing an opt-out mechanism. While we do not recommend a particular user interface, we describe one possibility for the sake of demonstrating the mechanism’s technological feasibility. A mobile device could present people with a screen during the initial setup of a device’s operating system that informs people that their enhanced location will be automatically shared when they send a text message to 911. The screen could then direct people to the operating system’s location menu where they can change this setting. After install, people would only be able to opt-out by entering their settings menu. From the settings menu, people should be able to turn off enhanced location sharing for TT911 just as they would for any user-downloaded application.

Two other regimes for user control over location sharing are possible: ‘always-on’ and ‘opt-in.’ Because these regimes disserve privacy and public safety, respectively, the Commission should not permit them.

Under an always-on regime, mobile devices and text-messaging applications would always share enhanced location with 911 without affording users the option to turn it off. While automatic enhanced location sharing will make emergency responses safer and more efficient, an always-on default would never let people exercise control over the collection of their data under FIPPs nor would it allow them to anonymously text 911.³⁰ An always-on regime would provide little improvement in safety over an opt-out regime and would not afford users the ability to

³⁰ See *White House FIPPs* at 1.

exercise control over their location information. Accordingly, the Commission should reject an always-on regime.

Under an opt-in default regime, mobile devices and text-messaging applications would not share location information with 911 by default, but would allow people to turn location sharing “on.” While this type of default setting demonstrates a high level of respect for user control in accordance with FIPPs and would allow people to anonymously text 911, it would do so at unacceptable expense to public safety.³¹ Because most people will want to share their enhanced location with mobile carriers and PSAPs in an emergency, an opt-in default setting would ignore this preference and potentially placing people in danger by requiring additional action to enable location tracking, thereby undermining the efficacy of TT911. Accordingly, the Commission should reject an opt-in default regime.

III. The Commission should ensure that mobile device manufacturers and operating system developers do not build in backdoor access capabilities to enhanced location information.

FIPPs require that a person be given the right to secure and responsible handling of personal data.³² In order to best protect the security of mobile device users, the Commission should avoid creating any rules that would encourage mobile device manufacturers or operating system developers to give backdoor access for a PSAP to obtain enhanced location information—which could be exploited by hackers, foreign governments, or even stalkers without the consent of the mobile device user.

In general, a ‘backdoor’ is a feature that application programmers create in order for a particular user—*e.g.*, a law enforcement officer—to bypass an application’s security settings.³³ For example, Apple had long programmed a backdoor into their operating system so that law

³¹ *See id.*

³² *See id.*

³³ *Definition of Backdoor*, About Technology, http://netsecurity.about.com/cs/generalsecurity/g/def_backdoor.htm (last visited Nov. 16, 2014).

enforcement could bypass the password protection of Apple devices in order to access people's secure data.³⁴

However, software development companies have moved away from including backdoors in their software because it poses such a great security risk.³⁵ In particular, it is difficult to build a backdoor that permits entry only by a designated entity and not by bad actors seeking to break into the backdoor.

The Commission has proposed requiring “an ‘emergency mode’ for texts to 911, similar to the functionality that would be enabled if the user were to place a voice call to 911.”³⁶ We fear that such an emergency mode for non-voice call communications could present a serious security risk. This approach implies that PSAPs might be able to query a person's location periodically after they text 911, similar to the way in which PSAPs “rebid” for the 911 voice callers' locations at thirty-second intervals until sufficient location data is obtained.³⁷ The June Communications Security, Reliability, and Interoperability Council (CSRIC) Report detailed at least one approach for texting that would create a functionality that is “similar to an E9-1-1 voice call rebid.”³⁸

³⁴ See Craig Timberg, *Apple will no longer unlock most iPhones, iPads for police, even with search warrants*, Washington Post (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.

³⁵ See Joseph Bonneau, *Guessing passwords with Apple's full-device encryption*, Freedom to Tinker (Oct. 8, 2014), <https://freedom-to-tinker.com/blog/jbonneau/guessing-passwords-with-apples-full-device-encryption>.

³⁶ *Third TT911 FNPRM*, 29 FCC Rcd. at 9889, ¶¶ 100, n.270 (“In this discussion, we are focused on the development of standards necessary to enable an ‘emergency mode’ for text to 911, similar to the functionality that would be enabled if the user were to place a voice call to 911.”)

³⁷ APCO International, *Wireless 9-1-1 Deployment and Management Effective Practices Guide*, 38, <https://www.apcointl.org/doc/911-resources/apco-standards/188-wireless-9-1-1-deployment-and-management-effective-practices-guide/file.html> (“*APCO Effective Practices Guide*”).

³⁸ CSRIC, *Final Report – Investigation into Location Improvement for Interim SMS (Text) to 9-1-1*, 19 (June 2014), http://transition.fcc.gov/pshs/advisory/csr4/CSRIC_IV_WG-1_Task-1_Final_061814.pdf (“*CSRIC Final Report*”).

We acknowledge that the rebidding process is crucial for voice calls because sufficiently accurate location data “does not arrive with [an] initial wireless E9-1-1 call,” and that, similarly, sufficiently accurate location data may not be able to be obtained in the time it normally takes to send a text message.³⁹ However, the Commission should reject this approach in the context of TT911 because (1) it would create a backdoor that could be exploited by bad actors, and (2) embedding location information directly into the body of or otherwise appending location information to emergency text messages would create a much lower security risk.

We believe that a rebidding process for PSAPs to query a person’s location after receiving an emergency text message, where PSAPs will be able to remotely trigger devices to obtain enhanced location information, will create a problematic security backdoor. This functionality will require programmers to build a major security override into software that could be exploited by anyone that is able to spoof their identity to fool the device’s operating system into accepting that they are a PSAP with the necessary security credentials to trigger the override.

Even if the emergency mode that the Commission has proposed can only be initiated after a mobile device user has sent a text message to 911, this will still present an unnecessarily high security risk. Because emergency text messages can be sent from third-party interconnected text-messaging applications as well as native text-messaging applications, this emergency mode functionality will need to be able to be initiated by a countless number of different applications.

In other words, while the emergency mode will be controlled by the mobile device’s operating system, third-party applications will still need to have some level of control over this feature so that it can be initiated when a person sends a text to 911 from a third-party application. Because so many disparate entities will need access to the override feature, the operating system will not be able to tightly control access to this feature in the same way that it can control the emergency mode initiated by a voice call to 911, as wireless voice calls to 911 placed from third-party applications do not automatically transmit the user’s location

³⁹ *Id.*

information.⁴⁰ This location-tracking loophole will create an attractive target for hackers and developers of malicious applications.

In addition to simply allowing people to utilize the backdoor feature itself without permission, security backdoors also create a host of ancillary security issues.⁴¹ Cryptography expert Matthew Blaze has explained that the problem with security backdoors is “not just that somebody is going to use the same back door that law enforcement uses . . . [i]t’s that introducing the back door is very likely to either introduce or exacerbate a flaw in the software.”⁴² For example, enterprising hackers with malicious intent could feasibly exploit the process by which PSAPs would be able to query the location of a mobile device to spoof the location of the device so that PSAPs would receive misleading enhanced location information.

The Commission could avoid these problems by requiring operating system developers and text-messaging application developers to embed location information directly into text messages to 911. Instead of creating a security backdoor for PSAPs to query the enhanced location information of mobile users, this approach would create a ‘frontdoor’ that only sends location information once a person ‘opens the door’ by sending a text to 911. This approach will eliminate any need for remote access to the device’s location services. Furthermore, this approach would be a strictly software-based approach that would avoid the need for costly network upgrades.⁴³

Embedding location directly in emergency text messages could also provide enhanced location information that is as accurate as the information obtained in the course of voice calls to

⁴⁰ See *VoIP and 911 Service*, Federal Communications Commission (Oct. 8, 2014), <http://www.fcc.gov/guides/voip-and-911-service>.

⁴¹ See Chris Morran, *Giving Police Backdoor Access to Smartphones is an Invitation to be Hacked*, Consumerist (October 3, 2014), <http://consumerist.com/2014/10/03/giving-police-backdoor-access-to-smartphones-is-an-invitation-to-be-hacked/> (quoting University of Pennsylvania cryptology expert Matthew Blaze).

⁴² *Id.*

⁴³ See *CSRIC Final Report* at 19-20.

911 for the vast majority of texts-to-911. Although accurate location information may not always be available when the initial text message is sent, the Commission could avoid this problem by also requiring applications to send an automatic follow-up message with additional location information.

Specifically, the Commission could require that applications:

- Send ‘best available’ information with or in the initial text message, and;
- Send sufficiently accurate enhanced location information to the PSAP in an automatic follow-up text message either when it becomes available or 30 seconds after the initial message is sent.

As APCO noted in its *Effective Practices Guide for PSAPs* for voice calls to 911, “additional Rebids [beyond 30 seconds] have not been shown to add significant value.”⁴⁴ Therefore, embedded location likely can provide sufficiently accurate information without presenting the security risk of an emergency mode approach that would allow PSAPs to query a mobile device’s location at will.

IV. Enhanced location information should only be used to locate people in an emergency.

Once a person has shared her enhanced location information with mobile carriers, PSAPs, and text-messaging service providers during a TT911 session, those entities should not make it available for marketing or financial gain. Companies benefit greatly from selling user data while consumers feel that their privacy has been eroded. For example, Facebook is implementing a new tool for marketing purposes called “geofencing” in which a user’s location information is transmitted for purposes of “Location Aware Ads” to be sent to the user. The user must opt out of location information sharing in order not to receive these ads.⁴⁵

⁴⁴ *APCO Effective Practices Guide* at 38.

⁴⁵ Jack Marshall, *Facebook Launches Location-Based Ads*, Wall St. Journal (Oct. 8, 2014), <http://blogs.wsj.com/cmo/2014/10/08/facebook-launches-location-based-ads>.

Because consumer data is already being collected on a large scale, the Commission should avoid exacerbating this problem by creating a lucrative opportunity for mobile carriers, PSAPs, and text-messaging service providers to sell enhanced location information. Specifically, the Commission should prohibit commercial entities from selling enhanced location information obtained from TT911 sessions because people should not have to consent to share their location information with marketing firms in order to be located quickly in an emergency.

By using enhanced location information for profit, mobile carriers, PSAPs, and text-messaging service providers would violate the FIPP that limits the context of sharing location information with 911 if that information were disclosed for purposes beyond the scope of the emergency.⁴⁶ Furthermore, it is even more important now for the Commission to place firm controls around enhanced location information access, and retention given recent revelations of government agencies monitoring individual's information for nonconsensual uses.⁴⁷

* * *

We applaud the progress already made in the TT911 docket, and support the Commission's efforts to promulgate rules that allow enhanced location information sharing in TT911 sessions. The Commission should not delay in implementing this process, as it will make emergency responses to text messages more expedient, which will in turn save lives. However, the Commission should carefully consider the privacy implications of new location tracking capabilities, like enhanced location sharing. We look forward to discussing the contours of our proposal with the Commission.

⁴⁶ See *White House FIPPs* at 1.

⁴⁷ Trevor Timm, *NSA's Vast Surveillance Powers Extend Far Beyond Counterterrorism, Despite Misleading Government Claims*, Electronic Frontier Foundation (Nov. 11, 2013), <https://www.eff.org/deeplinks/2013/11/nsas-surveillance-powers-extend-far-beyond-terrorism-despite-governments>.

Respectfully submitted,

/s/

Trip Nistico

Spencer Rubin

Vickie Stubbs

Student Attorneys

Blake E. Reid

Director

tlpc@colorado.edu

303.492.0548

Appendix: White House FIPPs⁴⁸

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 that person provides the data.
4. **Security:** Consumers have a right to secure and 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 measures in place to assure they adhere to [these principles].

⁴⁸ *White House FIPPs* at 1, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.