Before the
Federal Communications Commission
Washington, DC

In the Matter of:		
Request of NASNA to Address Issues Related to 911 Applications for Smartphones	)))	RM-11780

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

Eilif Vanderkolk
Student Attorney

Blake E. Reid
Director

tlpc@colorado.edu
303.492.0548

via electronic submission
March 6, 2017

The Samuelson-Glushko Technology Law and Policy Clinic (TLPC) respectfully replies to comments on the Oct. 18, 2016 petition submitted by the National Association of State 911 Administrators (NASNA) in the above-referenced proceeding.[1] The petition and comments raise important location data, interface design, and cybersecurity issues that may result from the proliferation of poorly designed devices and applications capable of contacting emergency services.[2]

These issues are also important in the context of the Commission's efforts to address inadvertent dialing and non-service initialized (NSI) devices, which we address in the attached report, *Understanding and Solving the Problems that Non-Service Initialized Devices and Non-Emergency 911 Calls Cause for PSAPs, First Responders, and the Public.* [3] In these comments, we briefly explain the connection between the location data, interface design, and cybersecurity issues raised in this proceeding and the context of inadvertent dialing and NSI devices.

I. Location Data

The potential described by commenters for the transmission of inaccurate location data by poorly designed devices is not only a problem for legitimate users of those devices, but an attribute that could be leveraged by malicious actors to conceal the source of a denial of service attack.

For example, NENA states that "although . . . user confirmation or manipulation of location data could be valuable in certain circumstances (particularly for indoor locations), we share NASNA's concerns that not all application developers will have carefully and thoroughly implemented anti-spoofing safeguards, absent clear guidance on the need to do so."[4] MCP also urges "the FCC to consider rules that would mitigate the likelihood of a spoofed emergency call. This may include requiring 911 Apps to provide a PSAP with both the true location of the device as well as the user-generated location."[5]

The TLPC Report describes the vulnerability of PSAPs to small-scale Denial-of-Service (DOS) attacks.[6] Location information can be used to identify a DOS attack when the attacker is using multiple handsets from the same physical location. Given the ability to manipulate where the calls are apparently originating will make it harder to distinguish malicious attacks from legitimate 911 calls. While we take no position on the viability of anti-location spoofing regulations, the potential implications of location spoofing for DOS attacks is a critical consideration.

[1] Letter of the National Association of State 911 Administrators, Request of NASNA to Address Issues Related to 911 Applications for Smartphones, RM-11780, at 2 (Oct. 18, 2016), https://ecfsapi.fcc.gov/file/1219857319120/RM11780.pdf.

[2] *Id.*

[3] Samuelson-Glushko Technology Law & Policy Clinic, *Understanding and Solving the Problems that Non-Service Initialized Devices and Non-Emergency 911 Calls Cause for PSAPs, First Responders, and the Public*, (Nov. 21, 2016) http://tlpc.colorado.edu/wp-content/uploads/2016/11/2016.11.21-911-Inadvertant-Call-Whitepaper-Final.pdf ("TLPC Report") (also attached).

[4] Comments of the National Emergency Number Association, *Request of NASNA to Address Issues Related to 911 Applications for Smartphones*, RM-11780, at 3 (Feb. 2, 2017) ("NENA Comments").

[5] Comments of Mission Critical Partners, *Request of NASNA to Address Issues Related to 911 Applications for Smartphones*, RM-11780, at 8 (Feb. 2, 2017).

[6] TLPC Report at 11.

II. Interface Design

Commenters also argue that ease of access features can often lead to reduced 911 access by overwhelming PSAPs with inadvertent calls. For example, NENA states that "as the mobile-device industry learned (the hard way) with features like 'hold '9' for 9-1-1,' these well-intentioned features often *reduce* consumer access to 9-1-1 service by consuming scarce network and human capacity that could be used to handle actual emergency calls."[7]

We agree. The TLPC Report found that "efforts by handset manufacturers and users to make dialing 911 faster and easier in the event of an emergency can make devices more prone to dialing 911 accidentally."[8]

Furthermore, commenters have noted that existing 911 application companies are already releasing shortcut-enabled applications. For example, ACT notes that "RapidSOS, a Boston-based app company in the 911 space, provides a platform that enables consumers to connect immediately with emergency services utilizing its 'one touch' application." [9]

We agree with NENA that inadvertent calls resulting from abbreviated dialing interfaces meant to speed access to 911 during an actual emergency risk draining PSAP resources, and it is unclear whether or to what extent these features offer actual advantages to access. The TLPC Report discusses several potential interface design problems, such as the ability to place a 911 call simply by pressing and holding the side button on a watch, caused by well-intentioned developers who wished to make accessing emergency services more efficient.

III. Cybersecurity

Finally, commenters argue that the introduction of 911 applications will create additional cybersecurity risks and drain PSAP resources without offering a significant improvement to emergency service access. For example, APCO notes that 911 applications would not only "introduce a significant cybersecurity risk for PSAPs, it contravenes the universality of 9-1-1 because an app's functionality varies according to whether and to what degree PSAPs use [an associated] web-based interface. Telecommunicators cannot be expected to simultaneously monitor a separate interface for each app." [10] New York City also noted that "apps could be a vector for malicious users to purposefully degrade the 911 system and emergency workers' ability to respond."[11]

We agree. Smartphones, and in particular NSI devices, already have the potential to be a threat to PSAP cybersecurity.[12] Increases in emergency application functionality may increase PSAP

[7] NENA Comments at 4.

[8] TLPC Report at 2.

[9] Comments of ACT | The App Association, *Request of NASNA to Address Issues Related to 911 Applications for Smartphones*, RM-11780, 2 (Feb. 2, 2017).

[10] Comments of the Association of Public-Safety Communications Officials-International, Inc., *Request of NASNA to Address Issues Related to 911 Applications for Smartphones*, RM-11780, 5 (Feb. 2, 2017).

[11] Comments of the City of New York, *Request of NASNA to Address Issues Related to 911 Applications for Smartphones*, RM-11780, 2 (Feb. 1, 2017).

[12] TLPC Report at 10.

vulnerability to cyber-attacks. While 911 applications may improve service in some circumstances, the Commission should consider whether this improvement is worth the cybersecurity tradeoff.

Respectfully submitted,

/s/

Eilif Vanderkolk
Student Attorney

Blake E. Reid
Director

CC: Austin Randazzo, Attorney Advisor, Policy and Licensing Division, Public Safety and Homeland Security Bureau.