The Bronx Defenders

Redefining public defense.

**Memorandum in Support – The New York Electronic Communications Privacy Act**

IN SUPPORT OF: A.09235 (Dinowitz)

*SUBJECT: Relates to creating the New York electronic communications privacy act; relates to the search and seizure of electronic devices and electronic communications.*

New developments in digital technology have resulted in the rapid expansion of law enforcement's ability to surreptitiously conduct surveillance and collect intimate information from our citizenry. Meanwhile, legal protections of our devices and data have been slow to develop, leaving electronic surveillance and information gathering largely unregulated and tipping the scales of justice and power away from the public. The Bronx Defenders support the NYECPA because it restores the balance by creating necessary safeguards and ensuring judicial oversight of modern policing.

In the last fifteen years surveillance technology use by law enforcement has exploded. As public defenders, we have witnessed the rise of this powerful new surveillance firsthand. Police now compel cellular providers to reveal the physical location of phone subscribers in real time and retrospectively. So called "IMSI catchers" or "Stingrays" imitate cellular towers to pinpoint the location of users, intercept content, and collect data on all mobile phone subscribers in their radius. Digital forensic software allows police to extract the contents of password protected smart phones and tablets with the push of a button. Emails, texts, and digital communications are intercepted as they travel through the air and from electronic storage. Social Media accounts can be quickly accessed to reveal a lifetime of social networks, personal beliefs, and communications. While these technologies used to be restricted to the military and Federal government, they are now regular tools of local law enforcement. In short, civilian police forces can now access our entire digital lives with relative ease to identify our friends, political associations, personal exchanges, and whereabouts.

This explosion of law enforcement surveillance capabilities is paralleled by woefully underdeveloped judicial and statutory law. Claims of Fourth Amendment protection against unlawful surveillance are often denied based on judicial decisions issued before the creation of the internet, cellular phones, email, social media, and big data.[1] Although several high courts have expressed concern with this outdated jurisprudence, and indicated a need for change, these decisions remain binding law.[2] Meanwhile, statutory law has similarly failed to keep pace. The Federal Stored Communications Act, which regulates electronic information held by third parties internet service providers, was written in 1986 before the invention of the World Wide Web and

[1] *See e.g. United States v. Miller*, 425 U.S. 435 (1976); *Smith v Maryland*, 442 U.S. 735 (1979).
[2] *See e.g. U.S. v. Jones*, 132 S.Ct. 945, 957 (2012)(Sotomayor concurring); *People v. Weaver*, 12 N.Y.3d 433, 442 (NY 2009).

modern digital communication. New York's Articles 700 & 705, which regulate government surveillance of electronic communications were drafted in the 1970's and have remained relatively untouched since.

The divergence of technology and law has resulted in unparalleled secrecy and lack of judicial oversight. Recently the New York City Police Department released records demonstrating that "IMSI catchers" or "Stingrays" were used in the Bronx over 200 times from 2008 to 2015. However, use of this military grade technology has never been litigated in the courts of our jurisdiction or subject to robust judicial scrutiny because its use is routinely kept from the accused. This failure to disclose the use of location tracking technology is not isolated to "IMSI catchers." In one recent case a Bronx Judge noted the "very disturbing" fact that prosecutors did not reveal that police had previously obtained real time location tracking information without judicial oversight when requesting a subsequent court order for the same information.[3] However, the court held that while the government's actions violated statutory law, no remedy was available. Cases like these exemplify the dangerous unwieldy nature of applying 20th century law to 21st century surveillance technology. This type of location tracking represents only a small part of the growing use of relatively unregulated use of surveillance technology. The Bronx Defenders has also witnessed an increased use of search warrants for digital devices and social media accounts that are both unlimited scope and completely lacking in particularity. Indeed some courts have noted that modern digital "search warrants are the closest things to general warrants we have confronted in this history of the Republic.'"[4]

The NYECPA addresses the immediate need for procedural safeguards and judicial oversight of surveillance technology by requiring the use of warrants for law enforcement seeking to obtain electronic communications, location information, and personal information from individuals or third party service providers. It also imposes limitations on the use of general warrants by strengthening the particularity requirement. Finally, it ensures robust public dialogue by requiring disclosure of the use of common forms of surveillance technology against our citizenry.

[3] *See People v. Campos*, 50 Misc. 3d 1216(A) (Sup. Ct. B.X. Co. 2015).
[4] *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1175 (Vt. 2012) (quoting P. Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. in Brief 1, 11 (2011)).