TESTIMONY

of

Kurt F. Schmid

Executive Director,

Chicago High Intensity Drug Trafficking Area (HIDTA)

on

ECPA Reform and the Revolution in Cloud Computing

Before the

Subcommittee on the Constitution, Civil Rights and Civil Liberties

Thursday, September 23, 2010

Mr. Chairman and Members of the Subcommittee on the Constitution, Civil Rights and Civil Liberties, my name is Kurt F. Schmid and I am the Executive Director of the Chicago High Intensity Drug Trafficking Area (HIDTA) Program in Chicago, IL. The HIDTA Program enhances and coordinates drug control efforts among local, State and Federal law enforcement agencies. The Program provides participating agencies with technology, equipment, coordination and other resources to combat drug trafficking and its harmful consequences in critical regions of the country[1].

I appear as an individual not representing any particular law enforcement agency or entity, but as a law enforcement official with over 40 years of experience, many of those 40 years dealing with ever-evolving communication and computer technologies and the attendant challenges to *preserve* law enforcement's lawfully-authorized electronic surveillance capability while maintaining the privacy rights of individuals and sustaining Industry's ability to keep pace in a fiercely competitive market(s).

The Face of Crime

Many aspects of the traditional criminal landscape have changed significantly as a direct result of new technology. *While law enforcement embraces new and innovative technologies and their positive impact on our society,* we must also be vigilant in how the criminal exploits them to harm others.

Modern communication tools integrated with Internet services has propelled individuals and businesses well into the 21st century. Correspondingly, many criminals have exploited new technologies in ways not previously anticipated. As an example, more traditional crimes like prostitution, street-corner drug trafficking activity, laundering and moving illicit proceeds, just to name a few, have taken on an entirely new dimension using networked technologies, and offers the criminal a "cloak of invisibility" from traditional public or law enforcement observation and detection.

[1] Office of National Drug Control Policy, HIDTA Program Policy and Budget Guidance, 2009

Further exploitation by criminals has created entirely new, more effective ways to operate criminal enterprises. Examples include using social networking applications as an instant communication tool to conduct gang operations, a recruiting tool that can enlist and indoctrinate criminal cohorts from around the world, or a training platform to teach effective ways to avoid detection. Crimes like identity theft, human trafficking, child exploitation, moving large amounts of ill-gotten capital, among others, have taken on a global aspect.

Diminishing risk of physical harm and more difficult detection also has many criminals migrating to the most elaborate of communication applications. Tendencies to communicate via text messaging and/or e-mail, especially by the upcoming generation (criminal element), has caused a sea change in how law enforcement conducts lawful intercepts and/or accesses (stored) digital evidence. As more users migrate from desktops and laptops to the now ubiquitous and powerful 'smartphones' to conduct their computing and communication functions, traditional data retention guidelines under ECPA do not apply. This data retention gap has manifested itself as the end of a trail of electronic evidence in major criminal investigations.

Cloud Computing

Cloud computing may be the next significant evolution of the Internet in the flexibility and robust nature of services the cloud(s) will offer its users. While the nature and power of these services and the platform upon which they come are unprecedented, preserving law enforcement's ability to lawfully access information related to criminal activity that happen to reside in the cloud(s) or other yet unknown media is not. New and emerging technologies should not, by their unique and secure nature alone, determine law enforcement's lawfully-authorized access to digital information residing in or transiting a particular medium.

Law Enforcement's Requirements & Perspective

Simply stated, law enforcement must preserve its ability to conduct lawfully-authorized electronic surveillance and must have

reasonably expeditious access to stored information that may constitute evidence of a crime committed or about to be committed regardless of the technology platform on which it resides or is transferred. Service providers must retain these records for a reasonable time set forth by statute or regulation. Without these Constitutionally-tested authorities, the safety of the public is put at significant risk. Balancing privacy with public safety in these challenging times, more than ever, requires collaboration and cooperation among law enforcement, privacy advocates and industry.

Lessons Learned

The law enforcement community has repeatedly learned that the criminal quickly adapts new technologies to his repertoire of tools not only to enhance his illicit activities, but also to create a (temporary) safe haven in which to operate. Law enforcement, generally lagging the technological capability and/or the legal precedent to intercept/access the communication/data, must deal with these difficult situations for sometimes long periods before solutions are found. Opportunities to sit at the table with industry, privacy advocates and lawmakers prior to major technology rollouts are crucial to preventing sometimes *years of unintended consequences.*

The rollout and subsequent activity facilitated by Congress enacting the Communications Assistance for Law Enforcement Act (CALEA) in 1994 defined statutory obligations telecom carriers had to implement to help law enforcement preserve its ability to conduct lawful electronic surveillance. This action was taken by Congress to preserve public safety. As challenging as it has been, CALEA also created the opportunity for law enforcement to sit at the table with industry and develop standards by which law enforcement's requirements can be addressed, thus helping preserve public safety. Absent CALEA, law enforcement's ability to conduct lawful intercepts would have been significantly diminished or even eliminated.

A similar approach addressing cloud computing and other emerging technologies seems reasonable and necessary in

reforming ECPA. Law enforcement's preference to preserving its ability to access relevant electronic/digital data to detect, prevent and solve crime is to sit at the table with lawmakers, privacy groups, industry and others to articulate its requirements and concerns. Such a process will more likely result in effective legislation that balances privacy and public safety and sustains a reasonably equitable and level playing field for Industry. If no action is taken to reform ECPA, other less desirable outcomes, namely awaiting a Court's decision sometimes promulgated by officials not sufficiently steeped in relevant technological, law enforcement operational and/or privacy issues may determine how we deal with these complex issues. This type of undesirable outcome can lead to long periods of having to comply with flawed case law.

Summary

Law enforcement is constantly striving to preserve, *not expand* its lawfully-authorized electronic surveillance and digital data access authority. A very important component of that preservation involves retaining, *not relinquishing,* established thresholds when subpoenas and search warrants are appropriate. Subpoenas assist law enforcement to focus on investigative targets, frequently serving as a tool to eliminate innocent persons from being investigated while serving to develop additional leads and evidence on the offender in question. Our nation's citizens demand that law enforcement "connect the dots" to detect, prevent or retrospectively investigate crime; subpoena authority assists law enforcement to *collect* the relevant dots; the process necessary prior to connecting them.

We live in a rapidly changing and dangerous world. Any erosion of law enforcement's lawful access to digital information while criminals are continually empowering themselves with technologies of unprecedented capabilities creates a perilous and paradoxical dilemma.

State and local law enforcement agencies, unlike Government agencies with abundant resources, are particularly susceptible to and challenged by criminals exploiting emerging communication technologies. A tragic but all too common example of this

susceptibility is a violent crime such as a homicide committed in a local jurisdiction – a cellular phone is often the key to solving the crime. Quick access to data related to that phone often determines whether or not the offender is captured before he commits other egregious criminal acts. Lawful access to digital communication media and sufficient retention of those data by service providers are critical to State and local law enforcement's daily investigative efforts and must be preserved.

Applying the ECPA to some of today's technologies has ranged from difficult to impractical. Any reform of the ECPA should address new and emerging technologies without unduly hampering or constraining law enforcement in its mission to protect the public.