Before the
U.S. House of Representatives, Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties

HEARING ON
ECPA REFORM AND THE REVOLUTION IN CLOUD COMPUTING

September 23, 2010

Written Statement of Thomas B. Hurbanek
Senior Investigator
New York State Police Computer Crime Unit

Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Subcommittee, my name is Thomas Hurbanek, and I am a Senior Investigator with the New York State Police Computer Crime Unit, a statewide detail of specially trained investigators and civilian staff that provides investigative and forensic support to State, Local, and Federal law enforcement agencies. Thank you for the opportunity to testify about ECPA reform and the revolution in Cloud Computing.

Today, I would like to highlight the challenges that Cloud Computing presents to State and Local law enforcement officers who are attempting to investigate and prevent crimes in order to protect the citizens and businesses within their jurisdiction. The Electronic Communications Privacy Act can provide a confusing set of rules regarding law enforcement access to business records, communications, and stored data, yet any reforms must be carefully weighed to preserve the existing balance between individual privacy and the ability of law enforcement to conduct investigations and protect the public. Legislation that targets a specific technology, such as cell phones, could also impact other technologies involving Internet connected devices.

We can look at Cloud computing from two perspectives. First there is the delivery of computing services to end users over the Internet. Second is the migration of business computing infrastructure to shared resources, accessed over the Internet, which can be provided within the enterprise or provisioned from third party providers.

If we look at the historical development of the computing and communications resources available to consumers in just my lifetime, the starting point is a household with one hard line telephone connection provided by a large United States based telephone company. Broadcast television was delivered free through the airwaves with no user interaction, thus providing no investigative usefulness. Mail was delivered to a home address or Post Office box by the United States Postal Service. Business was often conducted face-to-face or over the telephone and business records were in paper form. The sources of information available to a law enforcement investigator were limited, but all shared a powerful nexus to a local address or individual.

This situation advanced with the availability of personal computers, which allowed for the creation and storage of digital documents in the home and office, cellular telephones, which allowed users to combine mobility with communications, and the Internet, which allowed for the connection of these devices, and ultimately led to the convergence of technologies we are faced with today.

The connected consumer of today can be accessing and storing information over the Internet using many devices, home and work computers, one or more smartphones or other devices connected to multiple wireless providers, GPS units, game consoles, e-readers, and even vehicles. The consumer can be communicating with thousands of people using social networking sites, multiple e-mail, messaging and Internet telephone accounts, and identities available from hundreds of possible providers, while also transacting business with thousands of companies from around the world. Documents and

packages related to these transactions are delivered from a variety of global and regional shipping companies.

Criminals have adopted every piece of this technology and used it to improve their ability to commit crimes, or to victimize individuals and businesses worldwide with no regard for borders, laws and jurisdiction. This can make investigations involving the Internet daunting for the majority of police officers and extremely challenging even for highly trained investigators with access to advanced tools and equipment.

One example is the theft of online banking credentials where highly organized groups are using very sophisticated attacks to compromise legitimate Internet sites, infect the computing devices we rely on, obtain legitimate access credentials, and steal millions of dollars from consumers, small to medium sized businesses, local governments and school districts. These thefts can be devastating to the victim and direct countless energy and resources away from productive activity. Banking regulators estimate that more money is being stolen in online thefts than through traditional bank robberies.

In the State of New York there are nearly 20 million people. Citizens and businesses expect that when they call the New York State Police or one of over 500 local police agencies because they are a victim of crime, that their case can be investigated. The investigations cover every possible crime. A person is kidnapped, a child is missing or being exploited, a homicide suspect is at large, an identity is stolen, a bank account is compromised, a company website is shut down by denial of service, or a sophisticated attacker steals corporate secrets or attacks our critical infrastructure. When the perpetrator of this crime is not readily known, law enforcement must develop sources of information to begin the process of identifying suspects. When the crime involves the use of devices connected to the Internet, one of the primary sources of information are business records maintained by private sector entities, from a one person, home based business, to a multinational corporation.

In New York State, law enforcement does not have administrative subpoena power. Requests for subpoenas must first be reviewed by the District Attorney and then presented to a Grand Jury. Each County has its own procedure and criteria for requesting and obtaining subpoenas, and in some jurisdictions they can be difficult to obtain, especially for investigations involving non-felony offenses. This can lead to a situation which forces police officers to triage the number of requests for subpoenas resulting in crimes that go uninvestigated or under investigated.

Time is our enemy in Internet investigations, records and communications may not be retained, or information may intentionally or accidently be deleted or corrupted. Technology has created many new sources of information that may be accessed by law enforcement, equalized by the very number of private sector entities that must be contacted to build information during an investigation.

The advances of Cloud Computing present even more challenges for law enforcement. I would like to highlight the impact of a few technologies:

- Encryption – Companies are using advanced encryption technology to secure data that is transmitted across the Internet. This may create situations where law enforcement does not have the technological means to access communications, regardless of the legal authority to do so. The recent concerns in many countries about the encryption implemented on Blackberry devices demonstrates this problem.

- Virtualization – We are rapidly moving to an environment where software applications run on virtual computers and servers that can instantly be deleted and restarted with a fresh environment, removing traces of data that law enforcement has been able to access during the forensic examination of a seized computer. These virtual environments can be operated outside of the United States.

- Data Storage – With the evolution of Cloud Computing services, the storage locations for data are moving from our personal and business computers to locations on the Internet accessed by multiple devices. Locations in the United States will often be out of the jurisdiction of State and Local law enforcement. Data will also be stored outside of this country and not only in jurisdictions that have a friendly relationship with the United States. This is already creating challenges for large enterprises with business data stored in multiple countries with differing privacy rules.

- Apps – Applications in the Cloud can be accessed from anywhere, and data can be imported from one storage location, processed, and returned to the original location. An example would be photos taken with a smartphone from one manufacturer, uploaded to a storage service maintained by an online service, processed with software by a different online service, and forwarded using one or more communication services.

The combination of Cloud Computing technologies described here could create an environment where entire segments of business activity could be conducted outside of the reach of law enforcement. The effect of capabilities employed on television and in the movies may cause a misconception of the ability of law enforcement to access information on the Internet. At the New York State Police, we cannot sit at our computer and access the extensive data about individuals and their transactions with companies on the Internet. There is no database that lets me choose an individual and identify all of the e-mail, messaging, and social networking accounts that they use. I cannot access the subscriber information for all Internet based telephone accounts like we have done in the past with telephone subscriber directories.

I would like to close with an example from a recent case in New York State. While investigating a business and executing a search at the business location, it was discovered that there were no financial records about the business stored on site. All records were stored and processed on offshore servers which were accessed from the business, and the accountants for the business accessed a limited number of records from

a different location to prepare tax returns. This is just one example of how the technological advances and jurisdictional issues created by Cloud Computing may already be negating the fact that there are new sources of transactional records being maintained by companies operating on the Internet, especially in the case of State and Local law enforcement.

Thank-you again for the opportunity for the New York State Police to provide testimony before the Subcommittee.