INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

TESTIMONY

Statement of

Chief John M. Douglass

Chair, Mid-Sized Cities Section
International Association of Chiefs of Police

Before the

Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security

United States House of Representatives

January 25, 2011

515 N. WASHINGTON STREET
ALEXANDRIA, VA 22314
703-836-6767
WWW.THEIACP.ORG

Good Morning Mr. Chairman and Members of the Subcommittee,

My name is John Douglass and I serve as the Chief of Police in Overland Park, Kansas, a suburb of Kansas City. I am here today on behalf of the International Association of Chiefs of Police representing over 20,000 law enforcement executives in over 100 countries throughout the world. I am pleased to be here this morning to discuss the challenges currently confronting the U.S. law enforcement community and our need for further clarity on data retention issues.

In the United States, there are more than 18,000 law enforcement agencies and well over 800,000 officers who patrol our state highways and the streets of our communities each and every day. A great number of those officers also survey the Internet, phone and data logs and other electronic communication as they investigate crimes. Each day, federal, state, local and tribal law enforcement agencies are investigating cyber crime cases ranging from bank intrusions to fraud, intellectual property, terrorism and economic espionage, and, unfortunately "innocent images," or child pornography crimes.

Data preservation is a key component in any investigation. When criminals access the Internet through an ISP (or Internet Service Provider), send text messages, emails and other data, it creates important records and other information. In every case where criminal or civil action is envisioned, there is a clear need to preserve third party logs and business records related to connections which specifically demonstrate that a suspect's service provider is connecting with a victim's service provider or through another infrastructure en route.

When law enforcement suspects that a crime has been committed, we request a subpoena, court order, and search warrant etc. to obtain critical evidence from a service provider such as, customer records, connection information and stored data.

Take, for example, a case from Southern California which would not have been solved without the cell phone data from Verizon Wireless:

On July 26, 2006 22 year old Tori Vienneau and her 10 month infant son, Dean were murdered in their 2 bedroom apartment in San Diego. Tori was found strangled in her living room and baby Dean was found strangled and hung from his crib in one of the adjoining bedrooms. This horrifying crime scene triggered an exhaustive 18 month investigation.

The case was ultimately solved exclusively by the circumstantial evidence, including cell text message content and cell tower data from Verizon Wireless. The defendant denied any involvement in the killings and provided an intricate and extensive alibi.

Investigators focused their attention on Dennis Potts almost immediately because he was rumored to have had dinner plans with Tori on the night of her murder. Mr. Potts denied these rumors of dinner plans and the victim's cell phone was examined for any text messages between the two of them supporting/refuting such rumors. In a most interesting twist, all incoming and outgoing text messages prior to 6:30 pm on the night of the killings had been deleted. The victim's cell phone provider was contacted, but the text message content was not stored by the cell provider and therefore could not be recovered that way. Over the ensuing months, the victim's phone was subjected to extensive forensic analysis in the hopes of recovering some of these messages.

The defendant's cell phone carrier (Verizon Wireless) was also contacted and investigators were told incoming text message content (victim to defendant texts only) was preserved only for 3-5 days. In a stroke of good luck, this incoming data still existed and was preserved. It later proved to be pivotal in proving the defendant's guilt. The text message content proved not only that the defendant lied to investigators and that the two did, in fact, have plans to meet that evening, but also that the defendant was checking to see if the victim and her son were alone in the apartment.

Verizon also provided the cell tower data for the defendant's phone. This data, coupled with some additional testing, showed that the defendant's alibi was false and he was not

where he said he was. Furthermore, at the time of the killings, his cell phone "pinged" off of a cell tower only 500 yards from the victim's apartment. This became the single most important piece of evidence linking the defendant to the killings and to is ultimate conviction in September, 2009.

Clearly, preserving digital evidence is crucial in any modern-day criminal investigation.

While law enforcement does have success obtaining evidence through the appropriate legal process—because we are extremely aware of spoliation concerns—we are not always successful.

Many times we face obstacles in our investigations—from the differing locations of victims vs. perpetrators to the time when we request the information. Additionally, there are cases where we are not able to work quickly enough—mostly because a "lead" is discovered after the logs have expired or we are unaware of the specific service provider's protocols concerning data retention time periods.

For example, while most service providers save data for 30 days, there is no national standard and not all providers follow the 30 day rule. We are aware of specific ISPs who only save data for 15 days. 30 days is cutting it close many times depending upon when a victim reports a crime or when we discover a crime has been committed. So, as you can imagine, data preserved for a small window of time anything less than that can translate into a headache for law enforcement.

Also troublesome is that, when we are dealing with crimes committed online, often we have difficulty locating the ISP, as their servers can be located anywhere in the world. These days, online criminals operate internationally and electronic evidence can be virtually untraceable. Additionally, because laws differ internationally, obtaining information from foreign ISPs can often be difficult due to another country's retention practices.

Here are a few examples of cases where we have needed information from several different service providers located in many countries:

In a recent case, an international suspect hacked into United States based systems through systems in the United Kingdom. In this instance, data logs were located at the suspect's location in Europe, in the server's location in the UK, as well as victim locations in the US. Because all of these logs are essential to prosecution, search warrants were immediately issued for all parties in order to secure evidence which could spoil long before the arrest of a suspect.

In another case, an IP—or Internet Protocol— was stolen from a fortune 500 corporation and attempted to be sold to competitors—the suspect was in the Middle East and the victim company was in the US. Data logs and business records for connections, email accounts, online payment processors, etc. are all critical evidence. In this case, subtle nuances were important—when a web mail account was created versus the IP accessing the account are normally only established through log and related data has a lifecycle for retention and can easily spoil.

In both of these cases, we were lucky—had there been insufficient data retention to allow normal law enforcement efforts to legally obtain logs, the cases would not have been possible to successfully investigate or prosecute.

In closing, federal, state, tribal and local law enforcement are doing all that we can to protect our communities from increasing crime rates and the specter of terrorism—both online and in our streets, but we cannot do it alone. We need the full support and assistance of the federal government and clear guidance and regulations on data retention to aid us in successfully investigating and prosecuting the most dangerous of criminals.

Thank you.