JUSTICE NEWS

Statement of Deputy Assistant Attorney General for the Criminal Division Jason Weinstein Before the House Subcommittee on Crime, Terrorism and Homeland Security

Washington, D.C. ~ Tuesday, January 25, 2011

Good afternoon, Subcommittee Chairman Sensenbrenner, Committee Chairman Smith, Ranking Member Scott, and Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the Department of Justice. We welcome this opportunity to provide our views about data retention by companies that provide the public with Internet and cell phone services. I am particularly pleased to be able to speak with you about data retention, because data retention is fundamental to the Department's work in investigating and prosecuting almost every type of crime.

In offering this testimony, our goal is explain the nature of the public safety interest in data retention by providers. We do not attempt to discuss appropriate solutions, evaluate cross-cutting considerations, or evaluate the proper balance between data retention and other concerns. We look forward to continuing the dialog on these important issues with Congress, industry, and other interested organizations.

The harm from a lack of retention

Our modern system of communications is run by private companies that provide communications services. These providers include the companies that sell us cell phone service, the companies that bring Internet connectivity to our homes, and the companies that run online services, such as e-mail. These providers often keep records about who is using their services, and how. They keep these non-content records for business purposes; the records can be useful for billing, to resolve customer disputes, and for business analytics. Some records are kept for weeks or months; others are stored very briefly before being purged. In many cases, these records are the only available evidence that allows us to investigate who committed crimes on the Internet. They may be the only way to learn, for example, that a certain Internet address was used by a particular human being to engage in or facilitate a criminal offense.

All of us rely on the government to protect our lives and safety by thwarting threats to national security and the integrity of our computer networks and punishing and deterring dangerous criminals. That protection often requires the government to obtain a range of information about those who would do us harm.

In discharging its duty to the American people, the Department increasingly finds that Internet and cell phone companies' records are crucial evidence in cases involving a wide array of crimes, including child exploitation, violent crime, fraud, terrorism, public corruption, drug trafficking, online piracy, computer hacking and other privacy crimes. What's more, these records are important not only in federal investigations, but also in investigations by state and local law enforcement officers.

Through compulsory process obtained by law enforcement officials satisfying the requirements of law, the government can obtain access to such non-content data, which is essential to pursue investigations and secure convictions that thwart cyber intrusions, protect children from sexual exploitation and neutralize terrorist threats – but only if the data is still in existence by the time law enforcement gets there.

There is no doubt among public safety officials that the gaps between providers' retention policies

and law enforcement agencies' needs can be extremely harmful to the agencies' investigations. In 2006, forty-nine Attorneys General wrote to Congress to express "grave concern" about "the problem of insufficient data retention policies by Internet Service Providers." They wrote that child exploitation investigations "often tragically dead-end at the door of Internet Service Providers (ISPs) that have deleted information critical to determining a suspect's name and physical location." The International Association of Chiefs of Police adopted a formal resolution stating that "the failure of the Internet access provider industry to retain subscriber information and source or destination information for any uniform, predictable, reasonable period has resulted in the absence of data, which has become a significant hindrance and even an obstacle in certain investigations." In 2008 testimony before this Committee, FBI Director Robert Mueller reported that "from the perspective of an investigator, having that backlog of records would be tremendously important," and that where information is retained for only short periods of time, "you may lose the information you need to be able to bring the person to justice." Former Attorney General Gonzales similarly testified about "investigations where the evidence is no longer available because there's no requirement to retain the data."

In a 2006 hearing before another committee in this House, an agent of the Wyoming Division of Criminal Investigation gave a heart-wrenching example of the harm that a lack of data retention can cause. He described how an undercover operation discovered a movie, depicting the rape of a two-year-old child that was being traded on a peer-to-peer file sharing network. Investigators were able to determine that the movie had first been traded four months earlier. So, investigators promptly sent a subpoena to the ISP that had first transmitted the video, asking for the name and address of the customer who had sent the video. The ISP reported that it didn't have the records. Despite considerable effort, the child was not rescued and the criminals involved were not apprehended.

In some ways, the problem of investigations being stymied by a lack of data retention is growing worse. One mid-size cell phone company does not retain any records, and others are moving in that direction. A cable Internet provider does not keep track of the Internet protocol addresses it assigns to customers, at all. Another keeps them for only seven days—often, citizens don't even bring an Internet crime to law enforcement's attention that quickly. These practices thwart law enforcement's ability to protect the public. When investigators need records to investigate a drug dealer's communications, or to investigate a harassing phone call, records are simply unavailable.

These decisions by providers to delete records are rarely done out of a lack of desire to cooperate with law enforcement; rather, they are usually done out of an understandable desire to cut costs. Some providers also seem to delete records out of a concern for customer privacy.

Yet, as a result of short or even non-existent retention periods, criminal investigations are being frustrated. In one ongoing case being investigated by the Criminal Division's Child Exploitation and Obscenity Section working with the Federal Bureau of Investigation and Immigration and Customs Enforcement, we are seeking to identify members of online groups using social networking sites to upload and trade images of the sexual abuse of children. One U.S. target of this investigation uploaded child sexual abuse images hundreds of times to several different groups of like-minded offenders – including one group that had thousands of members. Investigators sent legal process to Internet service providers seeking to identify the distributors based on IP addresses that were six months old or less. Of the 172 requests, they received 33 separate responses noting that the requested information was no longer retained by the company because it was out of their data retention period. In other words, 19 percent of these requests resulted in no information about these offenders being provided due to lack of data retention. Indeed, lack of data retention has to date prevented us from identifying the investigation's chief U.S. target.

In October 2008, a federal arrest warrant was issued for a fugitive drug dealer. Law enforcement officers later identified a social networking account used by an associate of the drug dealer. Logins to the

social networking account were traced back to IP addresses assigned by a particular cellular provider, revealing that the social networking account was being accessed through that cellular provider's network. A subpoena was sought for data identifying the particular cellular phone number to which the IP addresses were assigned, but the cellular provider was unable to isolate the device by the IP addresses identified, because the data was not there. The inability to identify the specific cellular phone being used to access the social networking account stymied the effort to get the drug dealer off the street.

In many cases, investigations simply end once investigators recognize that, pursuant to provider policy, the necessary records have almost certainly been deleted. This occurs, for example, when a victim of a hacking crime discovers an attack too late, or when evidence of criminal conduct involving the Internet comes to light only after lengthy and complex forensic examination. Unlike burglaries, murders, and arsons, online crimes can be difficult to detect, and even more difficult to investigate. A business that has been hacked may not realize that its customers' identifying information has been stolen until months after the theft. Moreover, investigating online crimes can require obtaining many different records from many different providers in order to pierce the veil of anonymity provided by the Internet. The reason why the government may need access to records months or years after they were made is not because the government is slow or lazy in investigating those crimes, but because gathering the evidence in compliance with federal law – including meeting the statutory thresholds to obtain orders and warrants – takes time.

The current preservation regime

These unfortunate incidents arose under a legal regime that does not require providers to retain non-content data for any period of time, but instead relies upon investigators, on a case-by-case basis, to request that providers preserve data.

Federal law permits the government only to request that providers preserve particular records relevant to a particular case while investigators work on getting the proper court order, subpoena, or search warrant to obtain those records.

This approach has had its limitations. The investigator must realize he needs the records before the provider deletes them, but providers are free to delete records after a short period of time, or to destroy them immediately. If, as has sometimes been the case, a provider deletes the relevant records after just a few seconds or a few days, a preservation request can come too late. For example, suppose agents investigating a terrorist seize a computer and analyze it for evidence of who communicated with the target. If the terrorist has communicated over the Internet with co-conspirators, but those communications are older than the ISPs' retention periods, then investigators lose the ability to use information about the source and destination of those communications to trace the identity of other terrorists. With respect to those communications, provider practices thwart the government's legal authority to preserve evidence.

The current preservation regime also suffers from inconsistent responses from providers. In some cases, providers have been affirmatively uncooperative. In these instances, providers have failed to provide law enforcement agencies with reliable contact information, have ignored preservation requests, and have undermined the confidentiality of investigations by informing customers about preservation requests.

Many of the larger providers have established policies about how long they retain this data. For obvious reasons, I will not testify about how long those periods are for specific providers. I will say that, in general, those periods are rarely longer than a few months, and in some cases are considerably shorter.

Privacy and costs

EXHIBIT A

Data retention implicates several concerns. These include not just the needs of public safety, but also privacy interests and the burden on providers. Imposing greater retention requirements would raise legitimate concerns about privacy, and these concerns should be considered. However, the absence of strong data retention requirements introduces different privacy risks, as the government may be less effective at targeting malicious activities that threaten citizens' private data. Moreover, any privacy concerns about data retention should be balanced against the needs of law enforcement to keep the public safe. In considering those factors, it is important to be clear what data retention is *not* about.

Data retention is not primarily about collecting additional data that is not already collected. Most responsible providers are already collecting the data that is most relevant to criminal and national security-related investigations. In many cases, they have to collect it in order to provide service to begin with. In other cases, they collect it for the company's security, or to research how their service is being used. They simply do not retain that data for periods that are sufficient to meet the needs of public safety.

To be sure, the presence of large databases, by itself, poses privacy concerns. Those databases exist today, but data retention requirements could make them more common. Privacy concerns about those databases might be addressed by tailoring the information that is retained and clarifying the time period for which it is retained. Although we do not have a position on what information should be retained or for how long, the Department would welcome such a discussion.

A discussion about data retention is also not about whether the government should have the ability to obtain retained data. Retained data is held by the provider, not the government. Federal law controls when providers can disclose information related to communications, and it requires investigators to obtain legal process, such as a subpoena or court order and in some cases with a search warrant, in order to compel providers to disclose it.

As members of the Committee may be aware, there is an ongoing discussion about whether those laws strike a proper balance between privacy protection and public safety. I do not address that discussion in these remarks. Yet, whatever one's position in that discussion might be, data retention concerns a different question: Whether, in cases where law enforcement needs to obtain certain types of non-content data to protect public safety, and satisfies the legal standard for obtaining that data, the data will be available for that discrete purpose at all.

Short or non-existent data retention periods mean the data will not be available. Denying law enforcement that evidence prevents law enforcement from identifying those who victimize others online, whether by the production and trade of sexually abusive images of children, or by other online crimes, such as stealing private personal information.

It also can disserve the cause of privacy. Americans today face a wide range of threats to their privacy interests. In particular, foreign actors, including cyber criminals, routinely and unlawfully access data in the United States pertaining to individuals that most people would regard as highly personal and private. Data retention can help mitigate those threats by enabling effective prosecution of those crimes. Cyber criminals, often anonymously, hack into computer networks of retailers and financial institutions, stealing millions of credit and debit card numbers and other personal information. In addition, many Americans' computers are, unbeknownst to them, part of a "botnet" – a collection of compromised computers under the remote command and control of a criminal or foreign adversary. Criminals and other malicious actors can extensively monitor these computers, capturing every keystroke, mouse click, password, credit card number, and e-mail. Unfortunately, because many Americans are using such infected computers, they are suffering from an extensive, pervasive, and entirely unlawful invasion of privacy at the hands of these actors. Making extensive use of data retained by providers, the Department has successfully investigated and prosecuted criminals who use these techniques to invade the public's privacy.

EXHIBIT A

Unlike the Department of Justice – which must comply with the Constitution and laws of the United States and is accountable to Congress and other oversight bodies – malicious cyber actors do not respect our laws or our privacy. The government has an obligation to prevent, disrupt, deter, and defeat such intrusions. The protection of privacy requires that we keep information from those who do not respect it — from criminals and others who would abuse that information and cause harm. Investigating and stopping this type of criminal activity is a high priority for the Department, and investigations of this type require that law enforcement be able to utilize lawful process to obtain data about the activities of identity thieves and other online criminals. Privacy interests can be undercut when data is not retained for a reasonable period of time, thereby preventing law enforcement officers from obtaining the information they need to catch and prosecute those criminals. Short or non-existent data retention periods harm those efforts.

Providers incur some costs in retaining that data, and although storage costs have been dropping exponentially, it is possible that longer retention periods would impose higher costs. However, when data retention is purely a business decision, it seems likely that the public safety interest in data retention is not being given sufficient weight. There is a role for Congress in striking a more appropriate balance.

Thus, I welcome a discussion about the balance among public safety, providers' needs, and privacy interests. Legitimate debates about privacy protection should not be resolved solely through the "delete" key.

Conclusion

I very much appreciate the opportunity to discuss with you the important role of data retention in helping law enforcement fight crime, improve public safety, and defend the national security while protecting privacy. We look forward to continuing to work with Congress as it considers whether legal changes are needed in this area. I also wish to emphasize that the Administration is in the process of developing comprehensive views on both cybersecurity legislation and potential amendments to the Electronic Communications Privacy Act. Nothing in my testimony should be interpreted to pre-judge the outcome of those discussions.

This concludes my remarks. I would be pleased to answer questions from you and other members of the Committee.

EXHIBIT A