Department of Justice

STATEMENT OF

JAMES A. BAKER
ASSOCIATE DEPUTY ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

SENATE JUDICIARY COMMITTEE

AT A HEARING ENTITLED

**The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age**

PRESENTED

SEPTEMBER 22, 2010

Good afternoon, Chairman Leahy, Ranking Member Sessions, and Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice. We welcome this opportunity to provide you with our perspective about how the Electronic Communications Privacy Act, as amended (ECPA), is used today by investigators and prosecutors throughout the country. Since its enactment nearly 25 years ago, ECPA has become a vital tool for the law enforcement community. It is also important for national security, law enforcement, and cyber security activities, as well as for protecting privacy interests.

As you know, ECPA is part of a set of laws that controls the collection and disclosure of the content of communications, such as phone calls and emails, as well as content that has been stored remotely. Passed in 1986 and repeatedly amended over the years, ECPA also regulates the collection and disclosure of certain non-content information about communications, which is sometimes referred to as "metadata." These laws (1) restrict communication service providers' ability to disclose such information, and (2) outline the rules governing access to that information by both government and private entities.

Department of Justice attorneys specializing in ECPA regularly give advice about all manner of investigations, including terrorism, drug trafficking, violent crime, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. Crucial evidence of all of these types of crimes is in the hands of telecommunications and other providers, and with few exceptions, ECPA places the same limitations on the government's access to those records regardless of what type of matter is under investigation. Judgments and balances made in ECPA inevitably will affect not only law enforcement generally, but also critical national security investigations and cyber security programs, as well as the interests of private sector companies trying to protect critical data.

ECPA's provisions are also important for protecting individual privacy. For example, ECPA places limitations on the government's access to content and metadata pertaining to communications of customers and subscribers. Section 2702 of Title 18, United States Code, generally prohibits Internet and telephone service providers from voluntarily divulging such information to the government, with certain limited exceptions. In addition, section 2703 sharply limits the ability of the government to obtain those records even using a subpoena—which, in other investigative contexts, is the most common method for obtaining records held by a third party, such as financial and medical records. Instead, before most metadata can be compelled, section 2703 requires a court order based upon a specific judicial finding of relevance and materiality. ECPA also places some limitations on the circumstances and degree to which Internet and telephone service providers may disclose content to private parties.

In light of the importance of ECPA's provisions today, and the balance the statute strikes between various important interests, there are several considerations we respectfully urge Congress to keep in mind before undertaking major changes to the statute.

1. Public Safety Must Not Be Compromised.

All of us rely on the government to protect our lives and safety by thwarting national security and cyber threats and punishing and deterring dangerous criminals. Information related

to communications, both content and non-content information, is often critical to the investigations that are necessary to achieve these objectives. Compulsory process served on communications companies can be a key tool in thwarting cyber criminals, protecting children from sexual exploitation, and neutralizing terrorist threats.

The type of information that investigators obtain from service providers includes both the content of communications as well as metadata – non-content information – about those communications. Such metadata often represents the cornerstone of an investigation. Investigators use metadata to learn important facts about a suspect's associates and activities and to weed out individuals who are not involved in unlawful activity so that limited investigative resources may be directed most efficiently. Metadata can show investigators with whom a suspect communicates, at what time, and for how long. Importantly, investigators often use such non-content information as a basis for requesting authorization from a court for more intrusive types of searches and surveillance, such as stored communication content or a wiretap. It is essential that investigators have the ability to obtain metadata about a suspect's activities in a timely and efficient manner based upon a level of factual predication – and pursuant to an authorization – that is commensurate with the fact that most requests for metadata occur at early stages of an investigation. If it is unduly difficult for investigators to obtain metadata, it may hamper the government's ability to respond promptly and effectively to real threats.

Here is one example of how communications metadata can help in an investigation. In April 2010, a Sheriff's Office Uniformed Patrol Lieutenant in Baton Rouge, Louisiana attempted to stop a suspect. The suspect shot the Lieutenant through the neck and fled. An investigation later identified the suspect, and an arrest warrant was obtained for attempted first degree murder of a police officer. In their efforts to locate and arrest the suspect, officers determined that the suspect used several cell phones to communicate with his girlfriend and other associates. Officers used ECPA subpoenas and court orders to the cell phone companies to obtain calling records and location records. This information ultimately allowed officers to confirm the suspect's location.

As a second example, in a DEA investigation in 2008, investigators seized approximately $900,000 from a tractor trailer during a traffic stop in Detroit. After gaining the cooperation of the driver, the DEA identified a number of cellular telephones with "Push-To-Talk" features that were being used to contact organizational leaders in Mexico. Telephone toll record analysis along with additional investigation revealed a pattern of switching cellular telephones to avoid detection and law enforcement interception. This technique effectively prevented the agents from obtaining the authority to conduct wiretap intercepts on these phones. The DEA was still able to use ECPA process to obtain cell site data to identify members of the criminal organization near Detroit. Obtaining this information was critical to this outcome. Without the use of telephone toll record data, cell site information, and pen register data, the DEA would not have been able to identify these dangerous drug traffickers.

ECPA legal process has also proven instrumental in thwarting child predators. In a recent undercover investigation, an FBI agent downloaded images of child pornography and used an ECPA subpoena to identify the computer involved. Using that information to obtain and execute a search warrant, agents discovered that the person running the server was a high school

special-needs teacher, a registered foster care provider, and a respite care provider who had adopted two children. The investigation revealed that he had sexually abused and produced child pornography of 19 children: his two adopted children, eight of their friends, three former foster children, two children for whom he provided respite care, and four of his special needs students. This man pleaded guilty and is awaiting sentencing.

One final example illustrates how communications service providers' records are important not only to regular criminal investigations, but also to keeping our law enforcement officers safe. Recently, a homicide detective in Prince George's County, Maryland, reported that, at 2:00 a.m., he and his partner were chasing a man wanted for a triple murder. Consistent with ECPA, they made use of cell tower information about the fugitive's mobile phone. Having this information immediately accessible increased officer safety and allowed them to marshal available law enforcement resources effectively. They successfully captured the fugitive in nine hours without placing officers, or the public, at undue risk.

These are only a few of the countless examples of how ECPA has become a critically important public safety tool. Accordingly, we think it is important that any changes to ECPA be made with full awareness of whether, and to what extent, the changes could affect the critical goal of protecting public safety. If an amendment were to unduly restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, it would have a very real and very human cost.

As the Department of Commerce notes in its testimony, some U.S. companies say that they find themselves at a competitive disadvantage in foreign markets because some foreign countries have misperceptions about the terms on which U.S. government agencies may obtain communications information. As a result of these misperceptions, U.S. firms have said that they have difficulty offering cloud computing services in some foreign markets if personal information is to be stored in the United States. While not discounting economic considerations, the Department believes that such concerns must be addressed without inadvertently compromising its ability to carry out its mission of enforcing the law and protecting the public from harm.

2. ECPA is Important in Law Enforcement's Efforts to Prevent Privacy Crimes.

Americans today face a wide range of threats to their privacy interests. In particular, foreign and domestic actors of all types, including cyber criminals, and, at times, the governments that harbor them, routinely and unlawfully access data pertaining to individuals that most people would regard as highly personal and private. Unlike the government – 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. ECPA plays a key role in that effort.

Criminals pose a significant day-to-day threat to the privacy of American computer users. For example, 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.

Investigators seeking to protect Americans from this type of crime online must work within ECPA's access restrictions and make use of its tools. For example, the FBI is investigating a vast botnet that was active in 2007 and 2008 and consisted of approximately fifteen million infected computers. The criminals used it to send spam messages to perpetrate online stock manipulation schemes and to illegally sell online pharmaceuticals. Researchers estimate that this botnet was responsible for 20 percent of all spam email in the first quarter of 2008, and that the criminal enterprise collected profits of $3.5 million per year from the online pharmaceutical sales alone. Investigators used ECPA subpoenas and pen register/trap and trace orders to map the administrative structure of the botnet and identify those servers that should be searched with warrants. ECPA subpoenas also revealed that a single customer leased the most important servers and identified certain communication accounts used by that person. ECPA court orders identified that person's IP address.

Similarly, the FBI initiated an investigation in 2008 into an extensive identity theft and computer intrusion scheme. A gang of identity thieves obtained personal data from online sources, such as identity databases, credit reports, and land records. Armed with this information, the criminals contacted the victims' banks, impersonated the victims, and transferred huge sums of money to accounts they controlled. The scheme went on for at least three years and resulted in an estimated $30 million in losses. Investigators used ECPA subpoenas and court orders to obtain subscriber information and trace communications. They also used ECPA court orders to gain real-time location information for the suspects' mobile phones, which helped to identify and ultimately arrest them. To date, fourteen people (eight in the United States) have been convicted, although the primary suspect remains at large.

Safeguarding privacy includes keeping information 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 the use of tools that ECPA regulates. In particular, pen register and trap and trace orders have proven invaluable in mapping the complex web of command and control servers used by criminals. These tools, commonly used at the start of an investigation, allow law enforcement to gather the building blocks necessary to establish probable cause for more advanced investigative measures, such as wiretaps. Were ECPA to be amended in a way that increases the burdens on the government's use of these tools, this could decrease our ability to protect citizens from this type of privacy crime, and, consequently, decrease privacy overall.

3. Significant ECPA Changes Must Be Carefully Considered.

The Department of Justice stands ready to work with the Committee as it considers whether changes to ECPA are appropriate. But we urge Congress to proceed with caution; and to avoid amendments that would disrupt the fundamental balance between privacy protection and

public safety. Congress should refrain from making changes that would impair the government's ability to obtain critical information necessary to build criminal, national security, and cyber investigations, particularly if those changes would not provide any appreciable or meaningful improvement in privacy protection. In addition to compromising consumers' privacy, these types of crimes have significant economic ramifications on business and financial institutions that suffer millions of dollars in losses.

Although it was enacted in 1986, Congress substantially amended ECPA in 1994, and then again in 2001; with each amendment, ECPA evolved to account for changing times. The 2001 amendments, for example, extended the protections afforded to the collection of numbers dialed on a phone to the collection of e-mail addresses. In addition, Congress has also amended ECPA on a smaller scale on several additional occasions, most recently in 2009, when this Congress updated its provisions to permit U.S. investigators to assist foreign law enforcement.

Moreover, the statute, as written in 1986, has proven adaptable over time, although some courts have struggled with applying its terms to the Internet and other modern communications and information technologies. To give one example of ECPA's adaptability, in 1986, most electronic mail was sent without using the Internet by relying on dial-up online services or store-and-forward networks. When e-mail shifted to the Internet, ECPA easily accommodated it and came to offer equivalent privacy protections. In fact, there was no serious legal debate about whether ECPA applied to the Internet; its general language left room for no other conclusion than that it did.

To give another example, ECPA was forward-looking and flexible on the issue of cloud computing. With cloud computing, data is stored and processed by online services, rather than by one's personal computer. Yet ECPA was written at a time when this "remote computing" was relatively new. Because of the expense and complexity of computers in 1986, companies routinely sent their sensitive customer and payroll data to third parties for storage and processing. Thus, ECPA has explicitly covered so-called "remote computing services" since its enactment almost 25 years ago. Of course, as discussed in the testimony of my colleague from the Department of Commerce, cloud computing has expanded dramatically in recent years, and the number of people using such services has continued to grow.

It is true that ECPA and other statutes that regulate the collection and disclosure of communications, communications metadata, and stored data constitute a complex legal regime. Such complexity raises serious issues for investigators and privacy advocates alike. But ECPA is complicated because it endeavors to reconcile many competing priorities in a technologically complex realm. EPCA recognizes many distinctions that are critical to maintaining the proper balance between privacy and public safety.

For all these reasons, we believe Congress should proceed carefully before enacting changes that may delay time-sensitive investigations and make crucial evidence and information harder to obtain.

* * *

Technology continues to evolve, and it is natural to ask whether changes to ECPA are appropriate. Should Congress determine that ECPA should be amended again to address changes in technology, amendments will need to adequately protect privacy while not compromising the government's ability to protect the public from terrorists, spies, malicious cyber actors, and other criminals in a timely, efficient, and effective manner. Additionally, the concerns raised by U.S. commercial firms regarding international competition and the economic challenges they face, as highlighted in the testimony of the Commerce Department, must also be taken into account.

The law enforcement agents and prosecutors who work with ECPA on a daily basis have considerable knowledge about the statute's benefits and shortcomings. We believe that knowledge and combined experience will be invaluable to the Committee as it considers particular amendments to ECPA, and what the collateral effects of such amendments are likely to be.

We therefore appreciate the opportunity to share with you information about how the Department uses the legal procedures under ECPA to fight crime, improve public safety, and defend the national security while protecting the privacy of all Americans. We look forward to continuing to work with Congress as it considers these matters.

This concludes my remarks. I would be pleased to answer your questions.