CRM-231-1

RIF

Department of Justice

STATEMENT OF

JAMES A. BAKER
ASSOCIATE DEPUTY ATTORNEY GENERAL

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED

"THE ELECTRONIC COMMUNICATIONS PRIVACY ACT:
GOVERNMENT PERSPECTIVES ON PROTECTING PRIVACY IN THE DIGITAL AGE"

PRESENTED

APRIL 6, 2011

RIF

Good afternoon, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice regarding the Electronic Communications Privacy Act (ECPA). ECPA, which includes the Stored Communications Act and the Pen Register statute, is part of a set of laws that controls the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. These laws serve two functions. They are critical tools for law enforcement, national security, and cyber security activities, and they are essential for protecting the privacy interests of all Americans.

ECPA has never been more important than it is now. Because many criminals, terrorists and spies use telephones or the Internet, electronic evidence obtained pursuant to ECPA is now critical in prosecuting cases involving terrorism, espionage, violent crime, drug trafficking, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. In addition, because of the inherent overlap between criminal and national security investigations, ECPA's standards affect critical national security investigations and cyber security programs.

ECPA has three key components that regulate the disclosure of certain communications and related data. First, section 2701 of Title 18 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties. Second, section 2702 of Title 18 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-governmental entities. Third, section 2703 of Title 18 regulates government access to stored communications; it creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications. ECPA was initially enacted in 1986 and has been amended repeatedly since then, with substantial revisions in 1994 and 2001.

Mr. Chairman, the Department of Justice is charged with the responsibility of enforcing the laws, safeguarding the constitutional rights of Americans, and protecting the national security of the United States. As such, we welcome these hearings on this important topic. We appreciate the concerns that some in Congress, the courts, and the public have expressed about ECPA. We know that some believe that ECPA has not kept pace with technological changes or the way that people today communicate and store records, notwithstanding the fact that ECPA has been amended several times for just that purpose. We respect those concerns, and we appreciate the opportunity to discuss them here today. We also applaud your efforts to undertake a renewed examination of whether the current statutory scheme appropriately accommodates such concerns and adequately protects privacy while at the same time fostering innovation and economic development. It is legitimate to have a discussion about our present conceptions of privacy, about judicially-supervised tools the government needs to conduct vital law enforcement and national security investigations, and how our statutes should accommodate both. For example, we appreciate that there are concerns regarding ECPA's treatment of stored communications – in particular, the rule that the government may use lawful process short of a

RIF

warrant to obtain the content of emails that are stored for more than 180 days. We are ready and willing to engage in a robust discussion of these matters to ensure that the law continues to provide appropriate protections for the privacy and civil liberties of Americans as technology develops.

As we engage in that discussion, what we must not do – either intentionally or unintentionally – is unnecessarily hinder the government's ability to effectively and efficiently enforce the criminal law and protect national security. The government's ability to access, review, analyze, and act promptly upon the communications of criminals that we acquire lawfully, as well as data pertaining to such communications, is vital to our mission to protect the public from terrorists, spies, organized criminals, kidnappers, and other malicious actors. We are prepared to consider reasonable proposals to update the statute – and indeed, as set forth below, we have a few of our own to suggest – provided that they do not compromise our ability to protect the public from the real threats we face.

Significantly, ECPA protects privacy in another way as well: by authorizing law enforcement officers to obtain evidence from communications providers, ECPA enables the government to investigate and prosecute hackers, identity thieves, and other online criminals. Pursuant to ECPA, the government obtains evidence critical to prosecuting these privacy-related crimes.

I. ECPA Plays a Critical Role in Protecting Public Safety.

The government is responsible for catching and punishing criminals, deterring crime, protecting national security, and guarding against cyber threats. The government also plays a significant role in protecting the privacy and civil liberties of all Americans. The government enforces laws protecting privacy, and pursues cyber criminals and others who engage in identity theft and other offenses that violate privacy laws. Over the decades, government access to certain electronic communications, including both content and non-content information, has become even more important to upholding our law enforcement and national security responsibilities.

Pursuing criminals and tracking national security threats, however, is no simple task. Not only does the rapidly changing technological environment affect individual privacy, it also can impact adversely on the government's ability to investigate crime and respond to national security and cyber threats. As originally enacted, ECPA endeavored to establish a framework for balancing privacy and law enforcement interests – and to do so notwithstanding technological change. But the actual pace of change puts pressure on that framework that has in the past necessitated periodic amendments to it. As noted above, we look forward to working with the Congress to assess whether amendments to ECPA are appropriate at this time to keep pace with changes in technology.

RIF

It is important to understand both the kind of information that the government obtains under ECPA and how that information is used in criminal investigations. Under ECPA, the government may compel service providers to produce both content and non-content information related to electronic communications. It is obvious that the contents of a communication – for example, a text message related to a drug deal, an email used in a fraud scheme, or an image of child pornography – can be important evidence in a criminal case. But non-content information may be equally important, particularly at the early stages of a criminal or national security investigation.

Generally speaking, service providers use non-content information related to a communication to establish a communications channel, route a communication to its intended destination, or bill customers or subscribers for communications services. Service providers often collect and store such records in order to operate their networks and for other legitimate business purposes. Non-content information about a communication – also referred to as "metadata" – may include information about the identity of the parties to the communication, the time and duration of the communication, and the communicants' location. During the early stages of an investigation, it is often used to gather information about a criminal's associates and eliminate from the investigation people who are not involved in criminal activity. Importantly, non-content information gathered early in investigations is often used to generate the probable cause necessary for a subsequent search warrant. Without ready access to non-content information, it may be impossible for an investigation to develop and reach a stage where agents have the evidence necessary to obtain a warrant for a physical search.

In my September 22, 2010, testimony before the Committee, I discussed several examples of how ECPA currently assists law enforcement in accomplishing our mission to protect public safety. For the sake of completeness of the record before the Committee in this Congress, I repeat them below.

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 agents obtained an arrest warrant 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 the suspect's 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 non-content 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 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 effectively available law enforcement resources. They successfully captured the fugitive in nine hours without placing officers, or the public, at undue risk.

These are only a few examples of how ECPA has become a critically important public safety tool. The Department of Justice thinks it is important that any changes to ECPA be made with full awareness of whether, and to what extent, the changes could adversely affect the critical goal of protecting public safety and the national security of the United States. For example, if an amendment were unduly to restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost.

Congress should also recognize that raising the standard for obtaining information under ECPA may substantially slow criminal and national security investigations. In general, it takes longer for law enforcement to prepare a 2703(d) order application than a subpoena, and it takes longer to obtain a search warrant than a 2703(d) order. In a wide range of investigations, including terrorism, violent crimes, and child exploitation, speed is essential. In drug investigations, where targets frequently change phones or take other steps to evade surveillance, lost time can eliminate law enforcement's ability to collect useful evidence.

RTF

II. Portions of ECPA May Be Appropriate for Further Legislation or Clarification.

ECPA was enacted in 1986, but it has been amended on numerous subsequent occasions in light of the advance of technology and privacy concerns. Congress amended its provisions as recently as 2009; substantial revisions occurred in 1994 and 2001.

As we previously have testified, the Department of Justice stands ready to work with the Committee as it considers changes to portions of ECPA and the Pen Register statute (which was also enacted as part of the Electronic Communications Privacy Act in 1986). Although the Department does not endorse any particular legislative changes in today's testimony, we discuss matters that may be appropriate for amendment and the problems we see in those areas. In particular, this testimony addresses eight separate issues: the standard for obtaining prospective cell-site information, providing appellate jurisdiction for ex parte orders in criminal investigations, clarifying the standard for issuing 2703(d) orders, extending the standard for non-content telephone records to other similar forms of communication, clarifying the exceptions in the Pen Register statute, restricting disclosures of personal information by service providers, provider cost reimbursement, and the compelled disclosure of the contents of communications.

(1) Prospective cell-site information

One appropriate subject for further legislation is the legal standard for obtaining, on a prospective basis, cell tower information associated with cell phone calls. Cellular telephones operate by communicating through a carrier's infrastructure of fixed antennas. For example, whenever a user places or receives a call or text message, the network is aware (and makes a record) of the cell tower and usually which of three pie-slice "sectors"" covered by that tower serving the user's phone. This information, often called "cell-site information," is useful or even critical in a wide range of criminal cases, even though it reveals the phone's location only approximately (since it can only place the phone somewhere within that particular "cell" and sector). It is also often useful in early stages of criminal or national security investigations, when the government lacks probable cause for a warrant.

The appropriate legal standard for obtaining prospective cell-site information is not entirely uniform across the country. Judges in many districts issue prospective orders for cell-site information under the combined authority of a pen/trap order under the Pen Register statute and a court order under ECPA based upon "specific and articulable facts." (CALEA prohibits providers from making wireless location information available "solely pursuant" to the Pen Register statute.) Starting in 2005, however, some magistrate and district judges began rejecting this approach and holding that the only option for compelled ongoing production of cell location information is a search warrant based on probable cause. Courts' conflicting interpretations of the statutory basis for obtaining prospective cell-site information have created uncertainty regarding the proper standard for compelled disclosure of cell-site information, and some courts'

RIF

requirement of probable cause has hampered the government's ability to obtain important information in investigations of serious crimes. Legislation to clarify and unify the legal standard and the proper mechanism for obtaining prospective cell-site information could eliminate this uncertainty.

It should be noted that cell-site information is distinct from GPS coordinates generated by phones as part of a carrier's Enhanced 911 Phase II capabilities. Such data is much more precise, although wireless carriers generally do not keep it in the ordinary course of business. When the government seeks to compel the provider to disclose this sort of GPS data prospectively, it relies on a warrant. When prosecutors seek to obtain prospective E-911 Phase II geolocation data (such as that derived from GPS or multilateration) from a wireless carrier, the Criminal Division of the Justice Department recommends the use of a warrant based on probable cause. Some courts, however, have conflated cell site location information with more precise GPS (or similar) location information.

(2) Appellate jurisdiction for ex parte orders in criminal investigations

A second potential topic for legislation is to clarify the basis for appellate jurisdiction for denials of warrants or other ex parte court orders in criminal or national security investigations. Appellate review serves to clarify the law. Differences among district courts are typically resolved through review by a court of appeals, and the normal way to resolve differences among courts of appeals is through Supreme Court review. But under existing law, the government may have no mechanism to obtain review of the denial of a court order or search warrant, even when the denial is based primarily on questions of law rather than questions of fact.

The lack of clear jurisdiction for appeals of denials of *ex parte* orders in criminal cases has led to some confusion in the federal courts. For example, although there are numerous written opinions from magistrates and district courts on hybrid orders for prospective cell-site information, there remains no appellate authority addressing this issue. Congress could examine this issue further.

RIF

(3) Clarifying the standard for issuing 2703(d) orders

A third potentially appropriate topic for legislation is to clarify the standard for issuance of a court order under § 2703(d) of ECPA. ECPA provides that the government can use a court order under § 2703(d) to compel the production of non-content data, such as email addresses, IP addresses, or historical location information stored by providers. These orders can also compel production of some stored content of communications, although compelling content generally requires notice to the subscriber.

According to the statute, "[a] court order for disclosure... may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Until recently, no court had questioned that the United States was entitled to a 2703(d) order when it made the "specific and articulable facts" showing specified by § 2703(d). However, the Third Circuit recently held that because the statute says that a 2703(d) order "may" be issued if the government makes the necessary showing, judges may choose not to sign an application even if it provides the statutory showing. *See In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit's approach thus makes the issuance of § 2703(d) orders unpredictable and potentially inconsistent; some judges may impose additional requirements, while others may not. For example, some judges will issue these orders based on the statutory "reasonable grounds" standard, while others will devise higher burdens.

In considering the standard for issuing 2703(d) orders, it is important to consider the role they play in early stages of criminal and national security investigations. In the Wikileaks investigation, for example, this point was recently emphasized by Magistrate Judge Buchanan in the Eastern District of Virginia. In denying a motion to vacate a 2703(d) order directed to Twitter, Judge Buchanan explained that "at an early stage, the requirement of a higher probable cause standard for non-content information voluntarily released to a third party would needlessly hamper an investigation." *In re 2703(d)*, 2011 WL 900120, at *4 (E.D. Va. March 11, 2011).

Other statutes and rules governing the issuance of legal process, such as search warrants and pen/trap orders, *require* a magistrate to issue legal process when it finds that the United States has made the required showing. The Third Circuit's interpretation of § 2703(d), under which a court is free to reject the government's application even when it meets the statutory standard, is at odds with this approach. Legislation could address this issue.

RIF

(4) Extending the standard for non-content telephone records to other similar forms of communication

A fourth potential subject for legislation is the standard appropriate for compelling disclosure of addressing information associated with communications, such as email addresses. Traditionally, the government has used a subpoena to compel a phone company to disclose historical dialed number information associated with a telephone call, and ECPA has followed this practice. However, ECPA treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls. Although an officer can obtain records of calls made to and from a particular phone using a subpoena, "to" and "from" addressing information associated with email can be obtained only with a court order or a warrant. This results in a different level of protection for the same kind of information (e.g. addressing information) depending on the particular technology (e.g. telephone or email) associated with it.

Addressing information associated with email is increasingly important to criminal investigations as diverse as identity theft, child pornography, and organized crime and drug organizations, as well as national security investigations. Moreover, email, instant messaging, and social networking are now more common than telephone calls, and it makes sense to examine whether there is a reasoned basis for distinguishing between the processes used to obtain addressing information associated with wire and electronic communications. In addition, it is important to recognize that addressing information is an essential building block used early in criminal and national security investigations to help establish probable cause for further investigative techniques. Congress could consider whether this is an appropriate area for clarifying legislation.

(5) Clarifying the exceptions in the Pen Register statute

A fifth potential topic of legislation is to clarify the exceptions to the Pen Register statute. The Pen Register statute governs the collection of "dialing, routing, addressing, or signaling information" associated with wire or electronic communications. This information includes phone numbers dialed and "to" and "from" fields of email. In general, the statute requires a court order authorizing such collection on a prospective basis, unless the collection falls within a statutory exception.

It makes sense that a person using a communication service should be able to consent to another person monitoring addressing information associated with her communications. For example, a person receiving threats over the Internet should be able to consent to the government collecting addressing information that identifies the source of those threats. And indeed, the Pen Register statute does contain an exception for use of a pen/trap device with the consent of the user. But there is an issue with the consent provision: it may only allow the use of the pen/trap device by a provider of electronic communication service, not the user or some other party

RTF

designated by the user. So in the Internet threats example, the provider is the ISP, not the victim herself or the government. If the provider is unwilling or unable to implement the pen/trap device, even with the user's consent, the statute may prohibit the United States from assisting the victim. Clarifying the Pen Register statute on this point may be appropriate.

(6) Restricting disclosures of personal information by service providers

A sixth potentially appropriate topic for legislation is the disclosure by service providers of customer information for commercial purposes. Under § 2702(c)(6) of ECPA, there are currently no explicit restrictions on a provider disclosing non-content information pertaining to a customer or subscriber "to any person other than a government entity." This approach may be insufficiently protective of customer privacy. Congress could consider whether this rule strikes the appropriate balance between providers and customers.

(7) Provider cost reimbursement

A seventh potential subject for legislation is ECPA's § 2706 cost reimbursement provision. Currently, ECPA does not require the government to pay providers when it obtains "telephone toll records and telephone listings" from a communications common carrier, unless the information obtained is unusually voluminous or burdensome. Other than this narrow category of information, ECPA requires the government to pay providers for producing information under ECPA.

As an initial matter, ambiguity has arisen in the phrase "telephone toll records and telephone listings," as most users now have nationwide calling plans. Some phone service providers claim that because of the billing methods they use, they do not maintain "toll records" or "telephone listings," and thus they seek payment for all compliance with legal process. Legislation could clarify this issue.
In addition, as criminals, terrorists, spies and other malicious actors shift from voice telephone to other types of electronic communications, the category of "telephone toll records and telephone listings," is diminishing in importance. Moreover, the cost to law enforcement to pay providers for responding to subpoenas is substantial. For example, it is not unusual for the United States to be billed $40.00 by a provider merely to produce a customer's name, address, and related identifying information. Congress may wish to consider the extent to which it remains appropriate to require law enforcement agencies to pay for records of non-telephone forms of communication.

(8) Compelled disclosure of the contents of communications

Finally, the eighth and last potentially appropriate topic for legislation is the standard for compelling disclosure of the contents of stored communications. As noted above, we appreciate that there are concerns regarding ECPA's treatment of stored communications – in particular, the rule that the government may use lawful process short of a warrant to obtain the content of emails that are stored for more than 180 days. Indeed, some have argued recently in favor of a

RIF

probable cause standard for compelling disclosure of all such content under all circumstances. Because communication services are provided in a wide range of situations, any simple rule for compelled disclosure of contents raises a number of serious public safety questions. In considering whether or not there is a need to change existing standards, several issues are worthy of attention.

First, current law allows for the acquisition of certain stored communications using a subpoena where the account holder receives prior notice. This procedure is similar to that for paper records. If a person stores documents in her home, the government may use a subpoena to compel production of those documents. Congress should consider carefully whether it is appropriate to afford a higher evidentiary standard for compelled production of electronically-stored records than paper records.

Second, it is important to note that not all federal agencies have authority to obtain search warrants. For example, the Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) conduct investigations in which they need access to information stored as the content of email. Although those entities have authority to issue subpoenas, they lack the ability to obtain search warrants. Raising the standard for obtaining stored email or other stored communications to a search warrant could substantially impair their investigations.

Third, Congress should recognize the collateral consequences to criminal law enforcement and the national security of the United States if ECPA were to provide only one means – a probable cause warrant – for compelling disclosure of all stored content. For example, in order to obtain a search warrant for a particular email account, law enforcement has to establish probable cause to believe that evidence will be found in that particular account. In some cases, this link can be hard to establish. In one recent case, for example, law enforcement officers knew that a child exploitation subject had used one account to send and receive child pornography, and officers discovered that he had another email account, but they lacked evidence about his use of the second account.

Thus, Congress should consider carefully the adverse impact on criminal as well as national security investigations if a probable cause warrant were the only means to obtain such stored communications.

RIF

* * *

In conclusion, these topics appear appropriate for further clarification or legislation, but I want to emphasize that Congress should take care not to disrupt the current balance of interests that is reflected in ECPA. ECPA is complex because our nation's communications systems are complex, and because governing the government's access to that system must resolve competing interests between privacy, innovation, international competitiveness, public safety and the national security in many different contexts. When making changes to ECPA, public safety, national security, and legitimate privacy interests must not be compromised.

The Department of Justice stands ready to work with the Committee as it considers whether changes to ECPA are called for. But we urge Congress to proceed with caution. Congress must protect privacy and foster innovation, but it also should refrain from making changes that would unduly impair the government's ability to obtain critical information necessary to build criminal, national security, and cyber investigations.

Law enforcement agents and prosecutors have extensive experience with actual application of ECPA, and this experience can serve as an important resource in evaluating the tangible impact of changes to ECPA. We appreciate the opportunity to discuss this issue with you, and we look forward to continuing to work with you.

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