Department of Justice

STATEMENT OF
ELANA TYRANGIEL
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL

BEFORE THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"REFORMING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT"

PRESENTED
SEPTEMBER 16, 2015

Statement of
Elana Tyrangiel
Principal Deputy Assistant Attorney General

Before the
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"Reforming the Electronic Communications Privacy Act"

September 16, 2015

Chairman Grassley, Ranking Member Leahy, 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). This topic is particularly important to the Department because of the wide-ranging impact the statute has on public safety and both criminal and civil law enforcement operations. We are pleased to engage with the Committee in discussions about how ECPA is used and how it might be updated and improved.

ECPA includes the Pen Register Statute and the Stored Communications Act (SCA), as well as amendments to the Wiretap Act. These statutes are part of a set of laws that control the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. Although originally enacted in 1986, ECPA has been updated several times since, with significant revisions occurring in both 1994 and 2001.

I intend to focus the majority of my testimony on the SCA, which contains three primary 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 service providers of customer communications and records, both to government and non-governmental entities. Third, section 2703 of Title 18 regulates the government's ability to compel disclosure of both stored content and non-content information from a service provider; it creates a set of rules that governmental entities generally must follow in order to compel disclosure of stored communications and other records.

Since its inception, the SCA has served multiple purposes. It provides rules governing how providers of communications services disclose stored information—including contents of communications, such as the body of an email, and non-content information—to a wide variety of government entities. In doing so, it imposes requirements on the government and providers to ensure that the privacy of individuals is protected. The statute thus seeks to ensure public safety

and other law enforcement imperatives, while at the same time ensuring individual privacy. It is important that efforts to amend the SCA remain focused on maintaining both of these goals.

I. The Stored Communications Act Plays an Important Role in Government Investigations

Any consideration of the SCA must begin with an understanding of the statute's extremely broad scope. The paradigm that generally comes to mind in discussions of the SCA is a law enforcement agency conducting a criminal investigation and seeking a target's email from a service provider that makes its services available to the public. And, indeed, the SCA is critical to all sorts of criminal investigations into murder, kidnapping, organized crime, sexual abuse or exploitation of children, financial fraud, and more. As technology has advanced, electronic communications and electronic data storage have augmented traditional means of communicating and storing information. Appropriate governmental access to electronic communications and stored data, including both content and non-content information, has thus become even more important to upholding our law enforcement and national security responsibilities.

Even within these criminal investigations, it is important to understand the kind of information that the government obtains under the SCA as well as how that information is used. Under the SCA, the government may use legal process to compel service providers to produce both content and non-content information related to electronic communications. It is clear 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 can also be essential to building a case.

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. Non-content information about a communication may include, for example, information about the identity of the parties to the communication, and the time and duration of the communication. 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 a mechanism to obtain 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 example, the SCA has been critical to tracking down violent criminals. In one case, law enforcement obtained graphic photographs of a man sexually abusing his prepubescent son. Because of the offender's careful protection of his true identity, including the use of an anonymous online network, investigators needed to engage in a number of steps to ascertain the offender's location. Using information obtained from undercover chat sessions, officers identified a "proxy computer" – an intermediate computer used to obscure the offender's communication. Law

enforcement obtained computer routing information from the proxy computer, and from that routing information, identified an IP address from which the offender's internet traffic appeared to originate. After taking additional steps to confirm that the IP address was associated with the unlawful conduct, pursuant to ECPA agents served a subpoena on the offender's Internet service provider to obtain his physical address, leading to the eventual arrest of three individuals involved in the offense and the rescue of a minor victim from extreme, ongoing abuse.

Similarly, agents used evidence gathered using a process under ECPA in the investigation of the Boston Marathon bombing. Subpoenas to phone companies provided subscriber information and call detail records, which were critical during the investigation to help identify the bombers and their associates, and some of which were used at trial to show the communications between the bombers at critical times.

The SCA has broad effect in other ways as well. The statute applies not only to public and widely accessible service providers but also to non-public providers, such as companies or governments that provide email to their employees. Moreover, federal criminal investigations are only a subset of the circumstances in which the SCA applies. The statute applies to the federal government in civil contexts as well as to state and local governments when they seek to obtain content or non-content information from a service provider. This means that the statute also applies when the government is acting as a civil regulator—or even as an ordinary civil litigant. For instance, the SCA applies in all of the following circumstances that could arise, just within the Department of Justice:

- Civil Rights Enforcement: DOJ's Civil Rights Division brings a civil suit against a landlord who is sending racially harassing text messages to tenants. The target of the messages deletes them, and the landlord denies ownership of the account from which they were sent. The SCA governs the Division's ability to obtain those messages from the provider during civil discovery.

- False Claims Act: The DOJ Civil Division investigates a business for submitting false claims to the Federal government. The Division has reason to believe that the defendant's employees used email messages sent via the business's customer service email accounts to orchestrate the fraud. However, the defendant claims that it did not use email for business purposes. The SCA governs the ability of the Division to compel the internet service provider that hosted the company's website to disclose the contents of the business's email account.

- Environmental Litigation: The Department's Environment and Natural Resources Division brings a civil enforcement suit under the Superfund statute, a company relevant to the litigation has gone bankrupt, and the company's cloud provider has the only copies of that company's relevant corporate email. The SCA governs the Division's ability to obtain that email during civil discovery.

- Antitrust Investigations: The Department's Antitrust Division is conducting a civil investigation of several companies for engaging in an unlawful agreement to restrain trade. During the course of the investigation, DOJ attorneys discover that executives of those companies are using their personal email accounts to continue communications about the agreement. The SCA governs the Division's ability to obtain that email from the service provider.

- Tax Enforcement: The DOJ Tax Division investigates a tax preparation service that advertises via social networking sites. The company fraudulently inflates the amount of refunds due to the taxpayer and profits from taking a significant share of the fraudulent refund. Based on complaints about the preparer, the social networking site closes the company's account. The SCA governs the Tax Division's ability to obtain the posts advertising the company's tax preparation services.

During any discussions of possible changes to the SCA and ECPA more broadly, it is important to keep in mind its wide-ranging application and scope.

II. Modernizing the Rules for Compelled Disclosure of Email and Other Similar Stored Content Information

As I mentioned, ECPA was originally enacted in 1986—a time when the internet was still a nascent technology and landline telephones predominated. Although ECPA has been updated several times since its enactment, the statute—and specifically the portion of the SCA addressing law enforcement's ability to use legal process to compel disclosure of the stored contents of communications from a service provider—has been criticized for making outdated distinctions and failing to keep up with changes in technology and the way people use it today.

Many have noted—and we agree—that some of the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications. We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened.

Acknowledging that the so-called "180-day rule" and other distinctions in the SCA no longer make sense is an important first step. The harder question is how to update those outdated rules and the statute in light of new and changing technologies while maintaining protections for privacy and adequately providing for public safety and other law enforcement imperatives.

Personal privacy is critically important to all Americans—including those of us who serve in the government. It is also of increasing importance to individuals around the world, many of whom use communications services provided by U.S. companies. All of us use email and other

technologies to share personal and private information, and we want it to be protected appropriately. We also know that companies in the United States and elsewhere depend on privacy as a driver of innovation and competitiveness. Some have suggested that the best way to enhance privacy under the SCA would be to require law enforcement to obtain a warrant based on probable cause to compel disclosure of stored email and similar stored content information from a service provider. We appreciate the appeal of this approach and believe that it has considerable merit, provided that Congress consider contingencies for certain, limited functions for which this may pose a problem.

In the past several years, we have worked to help facilitate a better understanding of how the warrant requirement affects the Department of Justice's ability to enforce the law. And the Department appreciates, for example, that most recent proposals (*i.e.*, the "ECPA Amendments Act" (S. 356)), would not impose a warrant requirement in investigations involving corporate email. This type of provision would help preserve the manner in which corporate investigations have historically been conducted. Corporations often act as "electronic communications service providers" under the SCA when they provide email and internet service to their employees. It would be anomalous, however, for the SCA to afford greater protection to electronic corporate records than to the identical records in hard copy, and such a rule could be abused by organizations and individuals seeking to avoid accountability for violating the law. Retaining the current use of subpoenas in that context therefore makes sense.

The Department remains concerned, however, about the effect a blanket warrant requirement would have on its civil operations. Civil regulators and litigators do extremely important work. But they typically are investigating conduct that, while unlawful, is not a crime. Criminal search warrants are only available if an investigator can show probable cause that a crime has occurred. Lacking warrant authority, civil investigators enforcing civil rights, environmental, antitrust, and a host of other laws would be left unable to obtain stored communications content from providers. As information is increasingly stored electronically, and as wrongdoers take new steps to shield that information from civil investigators, the amount of critical information off-limits to government regulators and litigators will only increase. It is also not the case that these civil regulators and litigators can ask criminal law enforcement officers to obtain a warrant on their behalf, because such warrants can only be obtained in furtherance of a criminal investigation—a step that would be impermissible unless the underlying conduct appeared to be criminal in nature.

Nor could civil litigators and regulators reliably obtain email and other content information solely by serving a subpoena directly on a subscriber (rather than a provider). As several of the examples described above demonstrate, serving a subpoena on a provider may be the only way for civil law enforcement to obtain certain stored communications. For example, where the subscriber no longer exists—as in the case of a bankrupt corporation or a deceased individual—or a purported subscriber denies ownership of the communications and therefore refuses to comply with a subpoena, civil litigators and investigators without the ability to obtain

relevant evidence from a provider would be unable to obtain that evidence. Moreover, many individuals who violate the law may be tempted to destroy their communications rather than turn them over. Having the ability to seek records only from the individual, rather than the provider, could serve to encourage such illegal obstruction of justice. Thus, it is important that any proposed changes to ECPA take into account the ability of civil regulators and litigators to ask a court to compel disclosure of information from providers.

The Department also has several more technical, yet important, concerns that we believe merit consideration, including ensuring that the definition of "remote computing service" is appropriately scoped.

Finally, given the increasing prevalence of electronic communications, critical investigations involving widespread or complex crimes – such as those involving terrorism, transnational crime, financial fraud, or child exploitation – can last years and involve hundreds of search warrants, court orders, and subpoenas issued pursuant to ECPA to a variety of providers. ECPA reform proposals should account for investigations of this type and avoid enacting new obstacles to investigations that are already among the most challenging and important ones that law enforcement undertakes.

Efforts to update ECPA can reflect these considerations and, at the same time, incorporate strong mechanisms that protect individual privacy and ensure appropriate judicial oversight of government access to individual's communications.

III. The Need for Additional Updates to the SCA and ECPA

Although discussions about updating ECPA have often focused on the standard for governmental access to stored content information, we also believe there are a number of other parts of the statute that merit further examination during any process of updating and clarifying the statute.

(A) Clarifying Exceptions to the Pen Register Statute

First, Congress could consider clarifying the exceptions to the Pen Register statute. The Pen Register statute governs the real-time collection of non-content "dialing, routing, addressing, or signaling information" associated with wire or electronic communications. This information includes phone numbers dialed as well as the "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. The exceptions to the Pen Register statute, however, are actually less extensive than the exceptions to the Wiretap Act. This makes little sense—if the government is authorized to intercept communications in real-time, it is reasonable that the government should also be permitted to acquire the accompanying non-content information. Congress could harmonize the exceptions in these two sections of the statute by amending the Pen Register Act to bring it into line with the Wiretap Act. Moreover, the Pen Register Act's consent provision may be read so that a user can only consent to the use of a pen/trap device by

the provider as opposed to by the government or the user herself. The Pen Register Act's consent provision could be clarified to allow the user to provide direct consent for implementation of a pen/trap device by the government.

(B) Clarifying the Standard for Issuing 2703(d) Orders

Second, Congress could consider clarifying the standard for the issuance of a court order under § 2703(d) of the SCA, which can be used by criminal law enforcement authorities to compel disclosure of various types of stored records. According to that provision of 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 [records] sought are relevant and material to an ongoing criminal investigation."

The Fifth Circuit has interpreted this provision to require a court to issue a 2703(d) order when the government makes the "specific and articulable facts" showing specified by § 2703(d). *See In re Application of the United States*, 724 F.3d 600 (5th Cir. 2013). However, the Third Circuit has 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 makes the issuance of § 2703(d) orders unpredictable and potentially inconsistent; some judges may impose additional requirements, while others may not.

(C) Making the Standard for Non-content Records Technology-Neutral

Third, Congress could consider modernizing the SCA so that the government can use the same legal process to compel disclosure of addressing information associated with modern communications, such as email addresses, as the government already uses to compel disclosure of telephone addressing information. Historically, the government has used a subpoena to compel a phone company to disclose historical dialed number information associated with a telephone call, and ECPA endorsed this practice. However, ECPA treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls. Therefore, while law enforcement can obtain records of calls made to and from a particular phone using a subpoena, the same officer can only obtain "to" and "from" addressing information associated with email using a court order or a warrant, both of which are only available in criminal investigations. 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 and national security investigations. Congress could consider updating the SCA to set the same

standard for addressing information related to newer technologies as that which applies in traditional telephony.

(D) Clarifying that Subscribers May Consent to Law Enforcement Access to Communications Content

Fourth, Congress could consider clarifying the consent provision of the SCA. Under section 2702, a provider *may* disclose the contents of communications with the consent of a user or customer, but the provider is not required to do so. This has the impact of allowing the provider to overrule its customer's direction to disclose content associated with the customer's account. Thus when the victim of a crime seeks to share his or her own emails or other messages that may provide evidence, providers can refuse to disclose that information to law enforcement, even when provided with a written release from the account owner or subscriber.

(E) Appellate Jurisdiction for Ex Parte Orders in Criminal Investigations

Fifth, Congress could consider clarifying that higher courts have appellate jurisdiction over denials of warrants or other ex parte court orders in criminal investigations. 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. Congress may wish to consider clarifying that these denials are appealable so that the disagreements among courts are resolved and the law becomes standardized.

IV. Obtaining Stored Information Abroad

Some discussion concerning ECPA has focused on changing the standards and protocols for law enforcement access to content that a provider has chosen for its own business reasons to store outside the United States. The Administration is studying these legislative proposals, but the Department has significant concerns about aspects of these proposals.

* * *

In conclusion, I would like to reemphasize that in discussing any efforts to modernize ECPA, it is important to take into account the statute's broad application. As technology continues to advance, ECPA's importance to both criminal and civil law enforcement will only increase.

The Department of Justice stands ready to work with the Committee as it considers potential 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.