Statement of

Steven H. Cook
President
National Association of
Assistant United States Attorneys

Before the United States House of Representatives
Judiciary Committee

Hearing on H.R. 699
"The Email Privacy Act"

December 1, 2015

I. Introduction

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for the opportunity to address you today. I am the president of the National Association of Assistant United States Attorneys, a professional association representing the interests of Assistant United States Attorneys employed by the Department of Justice. Assistant United States Attorneys (AUSAs) are the career-level attorneys in the 94 United States Attorney Offices responsible for federal criminal prosecutions and civil cases involving the United States Government.

AUSAs are responsible for enforcing of the nation's criminal laws, including those addressing violent crime, drug trafficking, firearms, and terrorism. AUSAs also enforce civil laws, including those designed to combat fraud against the government. I am grateful to the Committee for the opportunity to share a career federal prosecutor's perspective on how the enforcement of the nation's laws would be altered by the Email Privacy Act, H.R. 699.

By way of background, I earned my undergraduate degree and law degree, graduating from the University of Tennessee College of Law with high honors. At the conclusion of law school, I served as a law clerk to a judge on the U.S. Court of Appeals for the Sixth Circuit Court. For the last 29 years, I have served as an Assistant United States Attorney in the Eastern District of Tennessee. During that time, I have been assigned to the Organized Crime Drug Enforcement Task Force; the General Crimes Section handling white collar crime, fraud, and public corruption; and as the Narcotics and Violent Crime Section Deputy Criminal Chief. For the past seven years, I have served as the Chief of the Criminal Division. It is important for me to emphasize, however, that the views I express today are mine and those of the National Association of Assistant United States Attorneys, not of the U.S. Department of Justice.

II. The Stored Communications Act and the Email Privacy Act

a. The Stored Communications Act, General Observations and the 180-Day Rule Fix of the Email Privacy Act

The Email Privacy Act, H.R. 699, proposes changes to the Stored Communications Act (SCA) a subpart of the Electronics Communications Privacy Act (ECPA) originally enacted in 1986. As our world has become increasingly reliant on technology, the SCA has come to play a pivotal role in law enforcement. In fact, electronic evidence—access to which is covered in large part by the SCA—is often critical to the apprehension of terrorists, child molesters, carjackers, drug traffickers, kidnappers, and murderers. It would be no exaggeration to say that lives often hang in the balance when law enforcement officials seek information under the SCA. For example, in a kidnapping case electronic information of the type covered by the SCA may provide law enforcement with the location of the kidnapper and child. Time is of the essence in such cases,

which unfortunately happen throughout our nation on a regular basis. Likewise, even in non-exigent circumstances information covered by the SCA very often is the lynchpin to solving crimes. Such information is often important to convicting the offender, vindicating the victim, protecting society, and exonerating the innocent.

Nevertheless, as one respected commentator has observed, "[d]espite its obvious importance, the statute remains poorly understood. Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA."[1] To be more direct, the SCA is a confusing statute even to those who use it regularly and study it carefully. It should therefore be no surprise that the SCA has spawned endless litigation. The result of that litigation has often been inconsistent rulings between the circuit courts, and in some circumstances inconsistency within the same circuit or district.[2] Among the most confusing, some would say illogical, provisions in the SCA is the so-called 180-day rule. As written, this rule allows law enforcement officials to obtain the content of email communications from an electronic communication service (ECS) provider without a showing of probable cause if the email has been stored by the ECS for more than 180 days.

The 180-day rule was a part of a legislative scheme enacted in 1986, and by 2010 the rule was so inconsistent with developing email usage and storage practices that one circuit court held it to be a violation of the Fourth Amendment. *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010). The Email Privacy Act eliminates the 180-day rule and brings the SCA in-line with *Warshak*. More specifically, the Act provides broader privacy protections for email communications by requiring that law enforcement officers obtain a search warrant before accessing email content, regardless of how long the email has been stored by the ECS. NAAUSA applauds this change and is pleased to support that particular provision of the Act.

b. <u>The Email Privacy Act Beyond the 180-Day Rule: Problems Created</u>

The Email Privacy Act, however, goes much further than correcting the problem created by 180-day rule. It is those further steps that are problematic and raise important concerns that the

---

[1] Orin S. Kerr, *The Future Of Internet Surveillance Law: A Symposium To Discuss Internet Surveillance, Privacy & The USA Patriot Act: Surveillance Law: Reshaping The Framework: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It* 72 Geo. Wash. L. Rev. 1208, 1208 (2004). *See also,* Comment: *Blue Skies Ahead: Clearing The Air For Information Privacy In The Cloud,* 55 Santa Clara L. Rev. 467, 468 (2015) (describing the SCA as "outdated and disjointed" and "struggling to maintain applicability and legitimacy").

[2] *See, e.g., In re Application of the United States,* 620 F.3d 304, 310 n. 6 (3d Cir. 2010)(describing the many divergent opinions on just one issue dealing with 3703(d) orders); *In re Cell Tower Records Under 18 U.S.C. § 2703(D),* 90 F. Supp. 3d 673, 674 (S.D. Tex. 2015) (noting a split of authority within the district on whether cell tower records are available to the government under the SCA).

Committee should address. The remainder of my testimony will focus on those concerns. I will briefly mention those concerns before discussing each of them in more detail in later portions of my testimony.

First, and most importantly, the Email Privacy Act fails to recognize the exceptions to the warrant requirement including the emergency aid, exigent circumstances and consent exceptions. These exceptions are longstanding rules of Fourth Amendment law that have been recognized and applied by the Supreme Court for decades. By failing to specify these exception for email searches covered by the Act, Congress will be creating an unprecedented and unnecessary barrier to law enforcement access. It is also creating a dangerous barrier—a barrier that will lead to the loss of potentially lifesaving information in cases where time is of the essence. It is well settled that a warrantless search may be conducted of a person's most private place—his or her home—if exigent circumstances exist. There is simply no reason to provide email communications with more protection than that afforded to a person's home.

Second, the Email Privacy Act will pour more dirt into an already muddy pond by creating internally inconsistent definitions and adding more unfamiliar and unique legal requirements to an already complicated body of law. Third, and relatedly, the Email Privacy Act does very little to address the antiquated, inappropriate, and confusing provisions of the current law.

Finally, in the face of a rising a wave of violent crime, unprecedented heroin and opioid addiction, and well placed heightened concern about the risks and spread of terrorism, this is the wrong time to create new and confusing rules. It is also the wrong time to impose barriers to law enforcement that far exceed those imposed by the Constitution—barriers that will unnecessarily impede saving lives and the search for truth while doing little to protect privacy.

c. The General Structure of the SCA

For purposes of my testimony, the SCA can be divided into three oversimplified parts: (1) section 2701 creates a general rule limiting access to certain stored communications; (2) section 2702 allows the service provider to voluntary disclose stored content (e.g., email and text messages) and non-content information under enumerated circumstances; and (3) section 2703 establishes rules under which the government can compel disclosure of stored content and non-content information from a service provider.

d. By failing to recognize the longstanding search warrant exceptions, the Email Privacy Act will create unnecessary barriers to information critical to law enforcement operations

The Email Privacy Act requires law enforcement officials to obtain a search warrant in order to

access email or other content covered by the SCA. That, again, is a requirement NAASUA supports as a general matter. What NAASUA does not support is the failure of the Act to recognize and incorporate the longstanding and well-settled exceptions to the search warrant requirement. Those exceptions have been created in recognition of the fact that, at times, it may impracticable or imprudent for law enforcement officers to obtain a warrant. There is simply no principled reason why law enforcement officers would *always* need a warrant to obtain information covered by the SCA when they can search a person's most intimate space (the home) without a warrant if certain circumstances are present.

By requiring law enforcement officials to secure a search warrant, Congress, through the Email Privacy Act would provide email content the same level of protection as our most private and intimate possessions, including the home. The home has always been viewed as particularly in need of protection because "[a]t the very core [of the personal rights protected by the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[3] The general rule, therefore, is that law enforcement officers may not search a person's home without a warrant.

The hurdles imposed by the warrant requirement are not insignificant. Fundamentally, law enforcement officials must show that there is probable cause to believe a crime has been committed, they must particularly describe the place to be searched and the items to be seized, and they must present this information for independent judicial review. In addition, state and federal rules and statutes impose often technical requirements that must be met. For example, with respect to federal search warrants, rule 41 of the Federal Rules of Criminal Procedure addresses who has the authority to issue the warrant; lists specific categories of property subject to search; limits who can request the warrant; imposes recording requirements; establishes procedures covering execution including time limits, time of day parameters, requirements for documenting warrant execution times; sets rules regarding creating an inventory and providing a copy of the warrant to the person from whose premises the property was taken; and establishes a requirement for creating a receipt and making a return to the issuing judge. Additionally, rule 41 imposes special rules for seizing electronic storage media and tracking devices. Even beyond that, there are several statutes with additional limitations or directives.[4]

---

[3] *Silverman v. United States,* 365 U.S. 505, 511-12 (1961). *See also Steagald v. United States,* 451 U.S. 204, 211 (1981); *Payton v. New York,* 445 U.S. 573, 586 (1980) ("the 'physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.'") (*quoting United States v. United States District Court*, 407 U.S. 297, 313 (1972)). *Silverman v. United States,* 365 U.S. 505, 511-12 (1961) ("The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") (citation omitted).

[4] *See* 18 U.S.C, § 3105 (persons authorized to serve search warrant); 18 U.S.C. § 3109 ("[b]reaking doors or windows for entry or exit"—or the so-called knock and announce rule); 18

It is important to note that the constitutional rules that require search warrants are not ironclad. They are subject to a limited number of exceptions where the Supreme Court has concluded that it is reasonable to conduct a search without a warrant. Those exceptions include, but are not limited to, exigent circumstances, emergency aid, and consent. If one of those exceptions is present, a law enforcement officer may conduct a search—even of the most sacred enclave, a house—without a search warrant.

As it is currently written, the Email Privacy Act imposes a statutory search warrant requirement mirroring the presumptive warrant requirement of the Fourth Amendment. The Act, however, glaringly fails to recognize any of the longstanding and deeply rooted exceptions to the warrant requirement. Put another way, the Email Privacy Act provides *greater* protection to email communications than *an*y other item or place. That simply does not make good sense. And, it could cripple law enforcement efforts in cases where time is an unavailable luxury.

This concern can be highlighted by an all too likely example. Two gunmen storm a crowded public place and use firearms and explosives to kill and maim dozens of people before escaping. The gunmen are quickly identified as ISIS operatives, and investigators determine that an apartment and particular cell phone numbers and email addresses are associated with them. At this point in the investigation, there are two immediate law enforcement concerns: (1) determining (and preventing) any imminent future attacks the gunmen and/or their affiliates may have planned; and (2) capturing and prosecuting the gunmen.

To address those concerns, law enforcement officials would need to immediately know: (1) where the terrorists had recently been (that is, location information for the recent past); (2) with whom they had been communicating; (3) the content of those communications; and (4) whether there were conspirators, explosives, or other dangerous instrumentalities inside the apartment.[5] The first three categories of information would typically be in the possession of the cell phone service provider(s) and, therefore, covered by the SCA. Although time would be of the essence and the risk of delay potentially catastrophic (in other words, a textbook example for application of the emergency aid and exigent circumstances exceptions), a warrant would be required to obtain the communication information under the proposed provisions of the Email Privacy Act. Ironically, at the same time, well-established law would permit law enforcement authorities to conduct a warrantless search of the apartment—the location that has always received the highest level of protection. Perhaps even more ironic, the Supreme Court recently held that police

---

U.S.C. § 3117 (mobile tracking devices warrant); 18 U.S.C § 3103a (additional grounds for issuing warrant—or the so-called sneak and peek warrant); 18 U.S.C. § 3105 (persons authorized to serve search warrant—broadening the common law rule regarding who can serve a search warrant) 18 U.S.C. § 3107 (service of warrants and seizures by Federal Bureau of Investigation).

[5] Of course, subscriber and toll record information would be available under 18 U.S.C. § 2709 once appropriate approvals were secured.

officers who obtain a suspect's cellular phone may search that phone (which may also serve as a repository for email communications) without a warrant if there are exigent circumstances.[6] The same should be true for searches of information such as email that is covered by the SCA.

Some might point out that in a situation like the one described above, the service provider could voluntarily choose to provide the information to law enforcement under 18 U.S.C. § 2702. While that may be true, it would be a novel and anomalous development in the law to allow the possessor of potentially lifesaving information to stop law enforcement from obtaining information that they could otherwise constitutionally access. Allowing the service provider to decide whether to turn information over in an emergency situation is no different than allowing the terrorists' apartment manager to decide whether to grant the police admission into the apartment to search for explosives or evidence.[7]

And these concerns—about leaving the determination to the service provider rather than law enforcement in an emergency situation—are not remote or hypothetical. Failures have led to disastrous and highly publicized tragedies.

One such example was the abduction of Kelsey Smith. As described in one article:

> Kelsey was an 18-year-old girl from Overland Park, Kan., who was abducted in broad daylight in the parking lot of a Target store just a couple of miles from my house on June 2, 2007.
>
> Sixteen seconds. That's how long it took Kelsey's killer to overtake her when she put a package in her car. He abducted her, raped her and strangled her with her own belt.

---

[6] *Riley v. California*, 134 S. Ct. 2473, 2494 (2014**) (***"In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone. The defendants here recognize — indeed, they stress — that such fact-specific threats may justify a warrantless search of cell phone data.")

[7] *Ryburn v. Huff,* 132 S. Ct. 987, 990 (2012)(construing current emergency aid doctrine and holding that entry into home not a violation of residents' rights because there was a "reasonable basis for concluding that there [was]an imminent threat of violence"); *Michigan v. Fisher,* 558 U.S. 45, 49 (2009) ("Officers do not need ironclad proof of 'a likely serious, life-threatening' injury to invoke the emergency aid exception."); *Brigham City v. Stuart,* 547 U.S. 398, 400(2006) (officers may enter a residence without a warrant when they have "an objectively reasonable basis for believing that an occupant is . . . imminently threatened with [serious injury].")

> It was four days before Kelsey's body was found in a wooded area in Kansas City, Mo. It took those four days for Verizon Wireless, her cellphone carrier, to hand over information about the location of her cellphone, which she had on her when she was abducted. When they did, her body was found within an hour.[8]

In response to this tragedy and others like it, twenty-one states across the country are reported to have enacted legislation, often called the Kelsey Smith Act, to provide mandatory access to law enforcement authorities in certain emergency circumstances.[9] Similarly, a Kelsey Smith Act was introduced in the last Congress in both the House, H.R. 1575, and in the Senate, S. 721.

Consistent with these considerations, any warrant requirement provision in the SCA should contain an emergency aid exception that parallels the applicable, long standing exception recognized in Fourth Amendment jurisprudence. To be clear, law enforcement officials, not service providers, should decide whether the requirements for the exception have been met.

The operation of the consent exception is problematic for the same reason. For example, if a subscriber to the cell phones associated with the terrorists consented to turning the information over to law enforcement authorities, further process would still be required, again, unless the service provider agreed. Allowing the service provider to decide whether to turn over information when the consent exception to the warrant requirement is met turns the law on its head. To use the same analogy, if police investigating terrorist activity secured consent from an occupant to search an apartment believed to be used to build bombs (or for that matter by a petty thief believed to be hiding stolen property) the landlord would not be free to deny the police access. The opposite is true: the landlord is obligated under the law to comply with the police demand for admission.

There is no principled reason for the law to treat service providers any differently than other third parties who are in possession of or have access to evidence or information needed by law enforcement. If law enforcement officials determine that one of the narrow and limited exceptions to the warrant requirement exists and they inform the service provider that they need specific information, the service provider should be duty-bound to provide that information, just as any other third party intermediary would be. These same considerations should apply to the Email Privacy Act. But as written, the Email Privacy Act imposes a warrant requirement for

---

[8] Diana Reese, *Kelsey Smith Act Would Save Lives, Cost Taxpayers Nothing* The Washington Post (April 18, 2013), *available at* https://www.washingtonpost.com/blogs/she-the-people/wp/2013/04/18/kelsey-smith-act-would-save-lives-cost-taxpayers-nothing/

[9] The Kelsey Smith Foundation, http://kelseysarmy.org/#ks-act

certain information, yet does not recognize any of the well-established exceptions to the warrant requirement; it further insulates service providers from the obligation shared by every other member of our society by allowing service providers to decide when they deem it appropriate to disclose information.

It is one thing for Congress to offer enhanced privacy protections for email and related communications by requiring a search warrant. It is quite another thing for Congress to afford such communications an unparalleled level of protection that will potentially jeopardize public safety. NAAUSA respectfully, but strongly, recommends that Congress amend the Email Privacy Act to make clear that the Act's search warrant requirement is subject to same the longstanding exceptions that apply to the Fourth Amendment's search warrant requirement.

e. <u>The Email Privacy Act places rules and burdens on the government that are not imposed for any other searches</u>

The Email Privacy Act imposes other unnecessary rules that go beyond those created by the Fourth Amendment, the United States Code, or the Federal Rules of Criminal Procedure for searches in any other context. It has long been the case that when law enforcement officials execute a search warrant they provide "a copy of the warrant and a receipt for the property taken to the person from whom, or whose premises, the property was taken . . .."[10] The purpose of this rule is obvious: it demonstrates the lawful authority of the law enforcement agency to conduct the search and collect evidence.

Thus, if a law enforcement agency executes a search warrant at a house where the target of the investigation does not live, but has stored, for example, his bomb making materials (or anything else of evidentiary value), the law enforcement agency must provide the resident of the home with a copy of the search warrant. And, although the resident can normally call the target, <u>the law enforcement agency</u> has no obligation to notify the target of when the search occurred, what was seized, under what authority the search was conducted, or even that there was a search at all. That is true even if the law enforcement agencies are conducting an ongoing investigation of the target and even if they know they intend to use the items as evidence against the target in a future criminal prosecution. The search warrant notice provision is not a "red alert" tool designed to notify an individual that he is under investigation, who is investigating him, why he is being investigated, or what evidence the government has developed up to that point.

In the context of electronic evidence, the rules should be the same: if law enforcement agencies serve a search warrant and seize evidence, they should be obligated to provide a copy of the search warrant to the person in possession of the evidence—the service provider. The service provider, therefore, should be treated no differently than the friend of a defendant whose home is

[10] Fed. R. Crim. P. 41(f)(1)(C).

searched because he happens to be storing some material belonging to the defendant. Absent a court order directing otherwise, the service provider (as a matter of contract, customer relations, or otherwise) is, of course, free to disclose that information as it chooses.

The Email Privacy Act goes far beyond requiring that the search warrant be served on the person whose premises is being searched (the service provider) and creates additional unprecedented, problematic burdens and obligations on law enforcement agencies. The Email Privacy Act adds a somewhat complex set of rules requiring the government (and then allowing the government to seek delay(s) in the obligation) to serve a copy of the search warrant not only on the person on whose premises the evidence exists, but on the target of the investigation. That alone is unprecedented. And yet the Email Privacy Act goes even further by requiring the government to provide six categories of information. To be clear, if the government searched from top to bottom the home of a friend of the target where all the evidence of a crime was being hidden, the law would impose no obligation during the investigative stage to serve the search warrant on anyone other than the person in possession of the evidence, much less would it require the law enforcement agencies to disclose these six categories of information.

Most troubling among the six categories of information, the Email Privacy Act would require the government to reveal "the nature of the law enforcement inquiry" to the subscriber. No historical practice or public policy consideration can, on balance, support this new and novel rule. Moreover, exactly how much information is needed to meet this standard—notifying the target of the investigation of "the nature of the law enforcement inquiry"—is not clear and will undoubtedly result in needless and time-consuming litigation. Finally, it should be noted that this new and unprecedented notice requirement is imposed regardless of whether the law enforcement agency has been able to determine the true identity of the subscriber. That is important for the Committee to recognize because very often email accounts used in criminal activities are operated under false names and/or are created in foreign countries.

The Email Privacy Act also creates a set of rules (in fact, two-and-a-half pages of rules) allowing the government to ask the court for permission to delay notice under narrow, specific, and limited circumstances. Assuming a judge agrees with the initial application to delay notice, if, for whatever reason (even clerical mistake), and without regard for the seriousness or nature of the criminal activity under investigation, a deadline is missed for extending the delayed notice, on its face the new early disclosure rules mandate immediate notice to the subscriber.

One final point on the newly-created notice provisions must be made. Many federal investigations are expansive in scope and are frequently interstate and often international in nature. Such investigations also often involve dozens, sometimes hundreds, of targets and span many years. Increasingly evidence of guilt is developed under the SCA and imposing these increased and unprecedented obligations will substantially burden law enforcement while

delivering very little benefits. Someone will have to track every delayed notice, prepare a motion and proposed order for an extension, and present it to a court. The motions, in turn, will be an additional draw on limited judicial resources—resources that could be put to use much more productively—since every motion will have to be processed by the court and then reviewed by a judge.

In summary, the Email Privacy Act creates new and unprecedented notice and information disclosure rules and obligations that far exceed those needed to accomplish the legitimate historical purpose of notice—to demonstrate the lawful authority for and scope of the search. The Email Privacy Act should simply incorporate the same notice requirements that apply for other searches that are carried out daily throughout our country.

f. The Email Privacy Act will further complicate an already confusing area of the law

As observed earlier, courts, commentators, and practitioners alike have found the SCA to be confusing. By creating even more rules and introducing internal inconsistencies, the Email Privacy Act will further complicate the SCA. With regard to new rules, as noted the Email Privacy Act imposes a rule 41 warrant requirement which in and of itself carries with it a wide range of rules and limitations. By then imposing unique notice requirements, delayed notice rules, and ambiguous information disclosure obligations, the Email Privacy Act simply adds more confusion.

In addition to unnecessarily adding to the complexities of the SCA, the Email Privacy Act creates additional ambiguities. For example, section 2705(a) provides in part:

> (1) IN GENERAL.—A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order delaying the notification required under section 2703(b) for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

(underscoring added.)

Since search warrants are uniquely a criminal enforcement tool used to gather evidence of criminal activity (that is to enforce criminal laws), it would seem that by definition the entity seeking the warrant would be a law enforcement agency. Thus, it is difficult to determine what other "government entity" other than federal law enforcement agencies may apply for a warrant. So, when exactly does the 90-day notice provision apply? Perhaps the intent of the provision is

to allow agencies other than law enforcement agencies to be authorized to obtain search warrants for information covered under the SCA. But, given the historical limited use of search warrants, if Congress desires to allow non-law enforcement agencies to apply for warrants under the Email Privacy Act, it must make its intent much more clear. Confusion and litigation is all that will result from the current language.

g. The Email Privacy Act does nothing to address the antiquated, inappropriate, and confusing provisions of the existing version of the SCA

If Congress is going to make revisions to the SCA, it should do so in a way that remedies the antiquated and confusing provisions. As observed earlier, section 2702 is the voluntary disclosure section—that is, after creating a general rule prohibiting disclosure of content and non-content information, this section of the SCA allows, but does not require, the service provider to disclose information under listed circumstances. One voluntary exception allows the service provider to disclose non-content on consent of the subscriber and (under narrower circumstances) content information on consent of a subscriber or party to the communication.[11]

Examples abound when the consent exception could quickly result in apprehension of a dangerous criminal or otherwise avert loss of life or property. In the context of a missing child this exception could prove to be a lifesaver. As is often the case during the first few critical minutes when a child is discovered to be missing, a review of records revealing who the child last communicated with, where he was at the time, and the substance of that communication could lead to a swift and safe recovery of the child. However, delaying until evidence develops demonstrating foul play (thus possibly triggering the voluntary emergency disclosure section should the provider in its discretion elect to assist under that provision) could prove disastrous.

In this setting, a parent is nearly always the subscriber and with the parent's consent the provider may disclose important records information to law enforcement officials without delay. But the provider is not required to do so and, despite this clear authority, providers rarely honor the subscriber's wishes to provide law enforcement this critical information. As noted earlier in connection with the 2703 mandatory disclosure section, this is analogous to allowing the apartment manager the authority to deny police access to a suspect's apartment when the police have consent of the tenant. Any reforms to the SCA should include a fix for this anomaly.

The provision of the SCA addressing the standard for issuing a disclosure order, 18 U.S.C. § 2703(d), should also be clarified. That provision provides in part:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and

[11] 18 U.S.C. § 2702(b)(3) and (c)(2).

> 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.

(Underscoring added.) The underscored language has led to a split in the federal appellate courts on whether the courts are obligated to enter an order when the standard of proof is met. [12] It seems reasonable to conclude that Congress intended that courts would perform their responsibilities to administer this whenever the evidentiary standard is met but the law need to be clarified.[13]

Additionally, section 2703(c)(2) should be amended to require the disclosure of "to/from" information in email communications with a subpoena. This would simply make the SCA consistent with the practice regarding telephone calls where that non-content information is available by subpoena.

Finally, but importantly, by imposing a warrant requirement as the exclusive vehicle through which the government can compel service providers to disclose content information, Congress has essentially placed this evidence beyond the reach of Assistant U.S. Attorneys, Department of Justice trial attorneys and other state civil litigators investigating illegal conduct of all sorts. For example, virtually every U.S. Attorney's office has an Affirmative Civil Enforcement Unit responsible for pursuing, among others, health care fraud and false claim act violations. Since a search warrant is a criminal investigative tool—requiring a showing that a crime has been committed—a wide range of evidence will be shielded by the Email Protection Act from the truth seeking process in these cases.

---

[12] *Compare In re Application of the United States,* 724 F.3d 600 (5th Cir. 2013) (interpreting this provision to require a court to issue a 2703(d) order when the government makes the "specific and articulable facts" showing), *with In re Application of the United States,* 620 F.3d 304 (3d Cir. 2010) (concluding 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 the government makes the requisite showing).

[13] *Cf.* Fed. R. Crim. P. 41(d)(1)("In General. After receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.") (emphasis added).

III. Conclusion

NAAUSA agrees that imposing a warrant requirement for the government to secure stored email in a criminal investigation is appropriate as a general rule. The Email Privacy Act, unfortunately, goes much further and in the process creates more problems than it solves First, and most importantly, the Email Privacy Act creates unprecedented and unnecessary barriers to this often lifesaving information—barriers that substantially exceed what would be required to search any other location, including the search of a home. Second, the Email Privacy Act will further complicate an already confusing area of the law by creating internally inconsistent definitions and layering more unfamiliar, unprecedented and unique legal requirements. Third, the Email Privacy Act does nothing to address the antiquated, inappropriate, and confusing provisions of the existing version of the SCA.

The SCA is desperately in need of comprehensive reform to bring it in-line with modern computing and communication technology. NAAUSA, therefore, is pleased to see that the Committee is considering revisions to the SCA. But, the Email Privacy Act as it is currently written is not an effective way of addressing the problems that currently exist with the SCA. NAAUSA stands ready and willing to further assist the Committee in drafting a bill that appropriately strikes the delicate balance between individual privacy and the need to protect society from dangerous criminals intent on wreaking havoc throughout this great country.