

EMAIL PRIVACY ACT

APRIL 26, 2016.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GOODLATTE, from the Committee on the Judiciary,  
submitted the following

R E P O R T

[To accompany H.R. 699]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 699) to amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

	Page
The Amendment .....	2
Purpose and Summary .....	4
Background and Need for the Legislation .....	5
Hearings .....	10
Committee Consideration .....	11
Committee Votes .....	11
Committee Oversight Findings .....	12
New Budget Authority and Tax Expenditures .....	12
Congressional Budget Office Cost Estimate .....	12
Duplication of Federal Programs .....	13
Disclosure of Directed Rule Makings .....	13
Performance Goals and Objectives .....	13
Advisory on Earmarks .....	13
Section-by-Section Analysis .....	13
Changes in Existing Law Made by the Bill, as Reported .....	16

## The Amendment

The amendment is as follows:

Strike all after the enacting clause and insert the following:

### SECTION 1. SHORT TITLE.

This Act may be cited as the “Email Privacy Act”.

### SEC. 2. VOLUNTARY DISCLOSURE CORRECTIONS.

(a) IN GENERAL.—Section 2702 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking “divulge” and inserting “disclose”;

(ii) by striking “while in electronic storage by that service” and inserting “that is in electronic storage with or otherwise stored, held, or maintained by that service”;

(B) in paragraph (2)—

(i) by striking “to the public”;

(ii) by striking “divulge” and inserting “disclose”; and

(iii) by striking “which is carried or maintained on that service” and inserting “that is stored, held, or maintained by that service”; and

(C) in paragraph (3)—

(i) by striking “divulge” and inserting “disclose”; and

(ii) by striking “a provider of” and inserting “a person or entity providing”

(2) in subsection (b)—

(A) in the matter preceding paragraph (1), by inserting “wire or electronic” before “communication”;

(B) by amending paragraph (1) to read as follows:

“(1) to an originator, addressee, or intended recipient of such communication, to the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication, or to an agent of such addressee, intended recipient, subscriber, or customer;” and

(C) by amending paragraph (3) to read as follows:

“(3) with the lawful consent of the originator, addressee, or intended recipient of such communication, or of the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication;”

(3) in subsection (c) by inserting “wire or electronic” before “communications”;

(4) in each of subsections (b) and (c), by striking “divulge” and inserting “disclose”; and

(5) in subsection (c), by amending paragraph (2) to read as follows:

“(2) with the lawful consent of the subscriber or customer;”.

### SEC. 3. AMENDMENTS TO REQUIRED DISCLOSURE SECTION.

Section 2703 of title 18, United States Code, is amended—

(1) by striking subsections (a) through (c) and inserting the following:

“(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by that service only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—

“(1) is issued by a court of competent jurisdiction; and

“(2) may indicate the date by which the provider must make the disclosure to the governmental entity.

In the absence of a date on the warrant indicating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.

“(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—

“(1) IN GENERAL.—Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of remote computing service of the contents of a wire or electronic communication that is stored, held, or maintained by that service only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—

“(A) is issued by a court of competent jurisdiction; and

“(B) may indicate the date by which the provider must make the disclosure to the governmental entity.

In the absence of a date on the warrant indicating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.

“(2) APPLICABILITY.—Paragraph (1) is applicable with respect to any wire or electronic communication that is stored, held, or maintained by the provider—

“(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communication received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

“(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

“(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—

“(1) IN GENERAL.—Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of a record or other information pertaining to a subscriber to or customer of such service (not including the contents of wire or electronic communications), only—

“(A) if a governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—

“(i) is issued by a court of competent jurisdiction directing the disclosure; and

“(ii) may indicate the date by which the provider must make the disclosure to the governmental entity;

“(B) if a governmental entity obtains a court order directing the disclosure under subsection (d);

“(C) with the lawful consent of the subscriber or customer; or

“(D) as otherwise authorized in paragraph (2).

“(2) SUBSCRIBER OR CUSTOMER INFORMATION.—A provider of electronic communication service or remote computing service shall, in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or any means available under paragraph (1), disclose to a governmental entity the—

“(A) name;

“(B) address;

“(C) local and long distance telephone connection records, or records of session times and durations;

“(D) length of service (including start date) and types of service used;

“(E) telephone or instrument number or other subscriber or customer number or identity, including any temporarily assigned network address; and

“(F) means and source of payment for such service (including any credit card or bank account number);

of a subscriber or customer of such service.

“(3) NOTICE NOT REQUIRED.—A governmental entity that receives records or information under this subsection is not required to provide notice to a subscriber or customer.”;

(2) in subsection (d)—

(A) by striking “(b) or”;

(B) by striking “the contents of a wire or electronic communication, or”;

(C) by striking “sought,” and inserting “sought”; and

(D) by striking “section” and inserting “subsection”; and

(3) by adding at the end the following:

“(h) NOTICE.—Except as provided in section 2705, a provider of electronic communication service or remote computing service may notify a subscriber or customer of a receipt of a warrant, court order, subpoena, or request under subsection (a), (b), (c), or (d) of this section.

“(i) RULE OF CONSTRUCTION RELATED TO LEGAL PROCESS.—Nothing in this section or in section 2702 shall limit the authority of a governmental entity to use an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction to—

“(1) require an originator, addressee, or intended recipient of a wire or electronic communication to disclose a wire or electronic communication (including the contents of that communication) to the governmental entity;

“(2) require a person or entity that provides an electronic communication service to the officers, directors, employees, or agents of the person or entity (for the purpose of carrying out their duties) to disclose a wire or electronic communication (including the contents of that communication) to or from the person or entity itself or to or from an officer, director, employee, or agent of the entity to a governmental entity, if the wire or electronic communication is stored, held, or maintained on an electronic communications system owned, operated, or controlled by the person or entity; or

“(3) require a person or entity that provides a remote computing service or electronic communication service to disclose a wire or electronic communication (including the contents of that communication) that advertises or promotes a product or service and that has been made readily accessible to the general public.

“(j) **RULE OF CONSTRUCTION RELATED TO CONGRESSIONAL SUBPOENAS.**—Nothing in this section or in section 2702 shall limit the power of inquiry vested in the Congress by Article I of the Constitution of the United States, including the authority to compel the production of a wire or electronic communication (including the contents of a wire or electronic communication) that is stored, held, or maintained by a person or entity that provides remote computing service or electronic communication service.”.

**SEC. 4. DELAYED NOTICE.**

Section 2705 of title 18, United States Code, is amended to read as follows:

**“§ 2705. Delayed notice**

“(a) **IN GENERAL.**—A governmental entity acting under section 2703 may apply to a court for an order directing a provider of electronic communication service or remote computing service to which a warrant, order, subpoena, or other directive under section 2703 is directed not to notify any other person of the existence of the warrant, order, subpoena, or other directive.

“(b) **DETERMINATION.**—A court shall grant a request for an order made under subsection (a) for delayed notification of up to 180 days if the court determines that there is reason to believe that notification of the existence of the warrant, order, subpoena, or other directive will likely result in—

“(1) endangering the life or physical safety of an individual;

“(2) flight from prosecution;

“(3) destruction of or tampering with evidence;

“(4) intimidation of potential witnesses; or

“(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

“(c) **EXTENSION.**—Upon request by a governmental entity, a court may grant one or more extensions, for periods of up to 180 days each, of an order granted in accordance with subsection (b).”.

**SEC. 5. RULE OF CONSTRUCTION.**

Nothing in this Act or an amendment made by this Act shall be construed to preclude the acquisition by the United States Government of—

(1) the contents of a wire or electronic communication pursuant to other lawful authorities, including the authorities under chapter 119 of title 18 (commonly known as the “Wiretap Act”), the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this Act; or

(2) records or other information relating to a subscriber or customer of any electronic communication service or remote computing service (not including the content of such communications) pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), chapter 119 of title 18 (commonly known as the “Wiretap Act”), or any other provision of Federal law not specifically amended by this Act.

## **Purpose and Summary**

The purpose of H.R. 699 is to update the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs.

### Background and Need for the Legislation

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to protect both the privacy of an individual's electronic communications and provide the government with a means for accessing these communications and related records. Although passed at the infancy of the Internet, the Stored Communications Act (SCA),<sup>1</sup> a chapter of ECPA, has been interpreted over the years to cover the content of emails, private Facebook messages, YouTube videos, and so-called "metadata," or non-content information, associated with Internet transactions. Congress originally modeled the new law on the Right to Financial Privacy Act in order "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs."<sup>2</sup> The Senate Report also stressed that the legislation was intended to strike a "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."<sup>3</sup>

The scope of the SCA is determined largely by the entities to which it applies, "electronic communication service" (ECS) providers and "remote computing service" (RCS) providers, as defined in the statute. It does not apply to government access to records held by a party to the communication. It is helpful to think of the SCA broken into two core components. First, it creates a broad bar against service providers *voluntarily* disclosing the content of a customer's communications to the government or others, subject to various exceptions. Second, it establishes procedures under which the government can *compel* a provider to disclose customers' communications or records. As to government access, the SCA utilizes a tiered system with different levels of evidence required depending on whether the provider is an ECS or RCS; whether the data sought is content or non-content; the age of the email; and whether notice has been given to the customer.

#### A. HISTORICAL BACKGROUND OF ECPA

Before passage of ECPA in 1986, government access to private electronic communications was governed primarily by the Fourth Amendment and the Federal wiretap law. In 1967, the Supreme Court issued two landmark Fourth Amendment cases. In *Katz v. United States*, the Court held that the Fourth Amendment's prohibition against "unreasonable searches and seizures" entitles individuals to a reasonable expectation of privacy in their private communications.<sup>4</sup> In *Berger v. New York*, the Court struck down a New York wiretap law that failed to include adequate safeguards for the privacy interests of those whose communications were being "tapped."<sup>5</sup>

<sup>1</sup>Known as the "Stored Communications Act", but the statute never actually refers to that term.

<sup>2</sup>S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555.

<sup>3</sup>*Id.*

<sup>4</sup>See U.S. Const. amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); *Katz v. United States*, 389 U.S. 347, 359 (1967).

<sup>5</sup>*Berger vs. New York*, 388 U.S. 41, 63-64 (1967).

One year later, in an effort to regulate wiretapping while also giving law enforcement a lawful means for intercepting telephone conversations, Congress enacted the “Wiretap Act” as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.<sup>6</sup> Title III prohibits the unauthorized interception of wire or oral communications, while simultaneously providing a procedure for law enforcement to conduct such interceptions upon judicial approval.<sup>7</sup> However, Title III only covered the “aural” interception of wire or oral communications—the interception of actual sounds—that are interpreted by hearing, and not sight. This left largely unregulated the transfer of digital communications.<sup>8</sup>

This legal uncertainty as to whether new digital forms of communication would be covered by Title III or other Federal law prompted the introduction of the original version of ECPA in 1985.<sup>9</sup> Fore-shadowing arguments made by proponents of ECPA reform today, the Senate Judiciary Committee observed at the time that this gap in coverage could stifle American technological innovation, expose law enforcement to liability, allow the erosion of American privacy rights, and jeopardize the admissibility of probative evidence in criminal prosecutions.<sup>10</sup> One year later Congress enacted ECPA.<sup>11</sup>

#### B. THE STORED COMMUNICATIONS ACT’S GENERAL FRAMEWORK

While colloquially referred to as ECPA, the SCA portion of the law remains the focus of reform efforts. The SCA (18 U.S.C. §§ 2701–2712) regulates how the government can obtain stored account information from network service providers such as Internet Service Providers (ISPs) and telecommunication carriers. Whenever agents or prosecutors seek stored email, account records, or subscriber information from a network service provider, they must comply with the SCA. The SCA sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers, and governs not just Federal criminal investigators and prosecutors but also Federal civil agencies and all state and local criminal and civil agencies. The SCA applies to any request to obtain stored email content, account records, or subscriber information and is not limited to requests in criminal investigations and prosecutions. Rather, the SCA applies also to any public safety requests and civil investigations in which these types of information are sought.

The SCA applies to the stored content of communications, which includes stored emails, text or instant messages, and documents, videos, and sound recordings stored in the “cloud.” Section 2701 prohibits unlawful access to certain stored communications, subject to criminal penalties if violated. Section 2702 governs voluntary disclosures of contents or records by network service providers. Section 2703 governs required or compelled disclosures of contents or records by network service providers to federal, state, or local gov-

<sup>6</sup>Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90–351, 801, 82 Stat. 197, 212.

<sup>7</sup>See 18 U.S.C. § 2511.

<sup>8</sup>See *United States v. New York Telephone Co.*, 434 U.S. 159, 166–67 (1977); *United States v. Seidlitz*, 589 F.2d 152, 157 (4th Cir. 1978) (“The words ‘aural acquisition’ literally translated mean to come into possession through the sense of hearing.”) (quoting Webster’s Third New International Dictionary, 1967 ed.).

<sup>9</sup>See Office of Technology Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties 46 (1985).

<sup>10</sup>*Id.* at 21.

<sup>11</sup>S. Rept. 99–541, at 5.

ernmental entities. As previously mentioned, for purposes of obtaining email content under Section 2703, the SCA provides a bifurcated system based on whether the provider is an “ECS” (electronic communication service provider) or “RCS” (remote computing service provider).

#### C. VOLUNTARY DISCLOSURE RULES (18 U.S.C. § 2702)

In section 2702, prohibitions to voluntary disclosure by a provider are listed first, followed by exceptions that permit voluntary disclosure to various entities. As to the first component, under 18 U.S.C. § 2702(a)(1), a provider of ECS to the public “shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage.” Section 2702(a)(2) states that a provider of RCS to the public shall not knowingly disclose the contents of a communication which is carried or maintained by that service. There are two other conditions that must be met in order for a communication to remain protected under subsection (a)(2). First, the communication must be maintained “on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service.”<sup>12</sup> Second, the communication must be maintained “solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.”<sup>13</sup> Thus, a RCS provider may access the content of subscriber or customer communications in order to provide computer storage and processing services. Access for the purpose of computer storage or processing may include access in order to filter out child pornography, identify and remove malware or SPAM, protect against unauthorized access, or to deliver targeted advertising to a subscriber or customer. Such access does not remove that content from the prohibition on voluntary disclosure in section 2702.<sup>14</sup> At the same time, the simple act of storing or processing information that may constitute contents of a wire or electronic communication about or on behalf of a subscriber or customer—as many Internet websites or “apps” do today to facilitate the provision of a product or service—including information to which an entity has access—does not transform that website or app into a RCS provider for purposes of either the voluntary disclosure rules in section 2702 or the required disclosure rules in section 2703.

Section 2702(a)(3) prohibits a provider of ECS or RCS to the public from disclosing a “record or other information pertaining to a subscriber to or customer of such service (not including the contents of a communication covered by paragraph (1) or (2)) to any governmental entity.” Note that this rule, which concerns non-content or “metadata,” does not apply to nongovernmental, private entities. This permits companies to share non-content information with other private entities, insofar as the SCA is concerned. There

<sup>12</sup> 18 U.S.C. § 2702(a)(2)(A).

<sup>13</sup> *Id.* at (a)(2)(B).

<sup>14</sup> Nor does such access by a RCS provider remove the content of communications from the compelled disclosure procedures in section 2703 (discussed in greater detail below).

may be other Federal or state laws, however, which prohibit disclosure of particular classes of information.<sup>15</sup>

Section 2702(b) provides exceptions to the prohibitions in subsection (a), for the *voluntary* disclosure of the *content* of communications, including: to an addressee or intended recipient of a communication, as authorized under Section 2703; as may be necessarily incident to the rendition of the service or the protection of the rights of property of the provider of that service; or to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. Section 2702(c) provides similar exceptions for the disclosure of *non-content* information, including as authorized under section 2703; with the lawful consent of the customer or subscriber; and to any person other than a governmental entity.

#### D. COMPELLED DISCLOSURE RULES (18 U.S.C. § 2703)

The second major component of the SCA is the rules concerning *required or compelled* disclosure of customer communications and records. Section 2703 sets up a tiered system with different standards that apply depending on whether an ECS or RCS is holding the record, whether the data sought is content or non-content, whether the email has been opened, and whether advanced notice has been given to the customer. This tiered system permits the government to use greater process when lesser process would satisfy the statute—for instance, the government may use a warrant when a subpoena would suffice.<sup>16</sup> Another way of thinking of the scope of data available through compelled disclosure is that “greater process generally includes access to information that cannot be obtained with lesser process.”<sup>17</sup>

At the highest level, the temporal age of the communication governs the criminal procedure related to compelled disclosure by an ECS or email provider. Specifically, the “180-day rule” arose because Internet users in 1986 were not able to retain a significant number of email messages on their computers simply because of storage limitations at the time. Thus, any emails older than 180 days were deemed abandoned and subject to lesser legal process than newer messages under 180 days old which entailed greater protection. This framework is reflected in section 2703(a), requiring the government to obtain a warrant if it seeks access to the *content* of a communication from an ECS provider that has been in “electronic storage” for 180 days or less.

Moving down a tier, if the communication has been stored for longer than 180 days, or if it is being “held or maintained” by an RCS “solely for the purpose of providing storage or computer processing services,” the government can use a subpoena, or a court order under Section 2703(d), so long as notice is provided to the customer at some point. Section 2703(d) orders require the applicant to prove “specific and articulable facts, showing that there are

<sup>15</sup>See *e.g.*, Right to Financial Privacy Act, 12 U.S.C. § 3401; Video Privacy Protection Act, 18 U.S.C. § 2710; Family Educational Rights and Privacy Act of 1978, 20 U.S.C. § 1232g.

<sup>16</sup>Orin K. Kerr, A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to the Amending It, 72 Geo. Wash. L. Rev. 1208, 1220 (2004).

<sup>17</sup>See, U.S. Department of Justice Computer Crime and Intellectual Property Section Manual, “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,” Third Edition, (2009).

reasonable grounds to believe that the contents of a[n] . . . electronic communication . . . are relevant and material to an ongoing criminal investigation.”

While Section 2703 facially permits government access to the contents of emails stored more than 180 days or those no longer in electronic storage, a 2010 ruling from the Sixth Circuit Court of Appeals called into question the constitutional validity of this provision. In *United States v. Warshak*, the government accessed 27,000 emails directly from the suspect’s Internet service provider (ISP) with a subpoena under section 2703(b) and an ex parte order under section 2703(d).<sup>18</sup> The Sixth Circuit held that such access was unlawful under the Fourth Amendment as subscribers enjoy “a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP” and “to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.”<sup>19</sup>

The Sixth Circuit is the only circuit court in the country which has held that a warrant is required for all communications content, but the decision had an immediate impact on the practices of telecommunications companies and government agencies. In those Federal districts where *Warshak* has become the de facto law, law enforcement has been required to obtain a warrant even in those cases where lesser process is still permitted by statute. Soon after the decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.

In addition to the content of communications, the SCA permits access to non-content information with a warrant, but the government may also use a subpoena or a section 2703(d) order without having to provide the customer notice.<sup>20</sup> To access basic subscriber information, including the customer’s name, address, phone number, length of service, and means of payment (including bank account numbers), the government may follow the more stringent requirements for obtaining a warrant or a section 2703(d) order, but can also use an administrative subpoena, which requires no prior authorization by a judicial officer.<sup>21</sup>

Finally, the SCA outlines when the government must provide notice to customers when their communications have been disclosed to the government. If the government seeks the contents of an electronic communication stored by an ECS for fewer than 180 days or stored by a RCS pursuant to a warrant, the government must follow the procedures set forth in Federal Rule of Criminal Procedure 41, which allow for the warrant to be served at the place the seizure occurs.<sup>22</sup> The government is not required to notify a customer of a compelled disclosure pursuant to a warrant.<sup>23</sup> If the government seeks access to the contents of electronic communications from an ECS or RCS under a section 2703(d) order or pursuant to a subpoena, the government must give prior notice to the customer,

<sup>18</sup> *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

<sup>19</sup> *Id.* at 288.

<sup>20</sup> See 18 U.S.C. § 2703(c). Non-content information such as the to/from line in emails, otherwise known as source and destination information, is generally not protected under the Fourth Amendment. See *United States v. Forrester*, 521 F.3d 500, 509 (9th Cir. 2007).

<sup>21</sup> 18 U.S.C. § 2703(c).

<sup>22</sup> 18 U.S.C. § 2703(a); FRCP 41(f)(1).

<sup>23</sup> See e.g., 18 U.S.C. § 2703(b)(1)(A).

unless the government obtains a delayed-notice order under 18 U.S.C. § 2705. The SCA does not require the government to provide notice to customers when it obtains non-content metadata or billing information from an ECS or RCS.<sup>24</sup>

The SCA permits the government to seek a court order precluding notice to the customer by an ECS or RCS. Section 2705 sets forth the criteria that forms the basis for the order and instructs that an order may command an ECS or RCS, “for such period as the court deems appropriate” not to notify any person of the existence of a warrant, subpoena, or court order.<sup>25</sup>

### Hearings

The Committee on the Judiciary held 1 day of hearings on H.R. 699 on December 1, 2015. Testimony was received from Mr. Andrew J. Ceresney, Director, Division of Enforcement, United States Securities and Exchange Commission, Mr. Steven Cook, President, Board of Directors, National Association of Assistant United States Attorneys, Mr. Richard W. Littlehale, Assistant Special Agent in Charge, Criminal Investigation Division, Tennessee Bureau of Investigation, Mr. Chris Calabrese, Vice President, Policy, Center for Democracy and Technology, Mr. Richard Salgado, Director, Law Enforcement and Information Security, Google, Inc., and Mr. Paul Rosenzweig, Founder, Red Branch Consulting, with additional material submitted by Representative Doug Collins of Georgia, Representative Sheila Jackson Lee of Texas, Representative Kevin Yoder of Kansas, Representative Jared Polis of Colorado, the United States Department of Justice, the FBI Agents Association, the Association of Prosecuting Attorneys (APA), the Association of State Criminal Investigative Agencies (ASCI), the Federal Law Enforcement Officers Association (FLEOA), the Fraternal Order of Police (FOP), the International Association of Chiefs of Police (IACP), the Major Cities Chiefs Association (MCCA), the Major County Sheriffs’ Association (MCSA), the National Association of Assistant United States Attorneys (NAAUSA), the National Association of Police Organizations (NAPO), the National District Attorneys Association (NDAA), the National Fusion Center Association (NFCA), the National Narcotic Officers’ Associations’ Coalition (NNOAC), the National Sheriffs’ Association (NSA), the Virginia Association of Commonwealth Attorneys, CompTIA and the Technology Councils of North America, TechFreedom, 60 Plus Association, American Commitment, American Consumer Institute, Americans for Tax Reform, Center for Financial Privacy and Human Rights, Citizen Outreach Competitive, Enterprise Institute, Council for Citizens Against Government Waste, Digital Liberty, FreedomWorks, Frontiers of Freedom, Heritage Action for America, Institute for Liberty, Institute for Policy Innovation, Less Government, Liberty Coalition, National Taxpayers Union, Niskanen Center, R Street, Taxpayers Protection Alliance, and the Rutherford Institute

<sup>24</sup> 18 U.S.C. § 2703(c)(3).

<sup>25</sup> 18 U.S.C. § 2705.

### Committee Consideration

On April 13, 2016, the Committee met in open session and ordered the bill H.R. 699 favorably reported, with an amendment, by a rollcall vote of 28 to 0, a quorum being present.

### Committee Votes

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following rollcall vote occurred during the Committee's consideration of H.R. 699.

1. Motion to report H.R. 699 favorably to the House. The motion was agreed to by a vote of 28 to 0.

### ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Goodlatte (VA), Chairman .....	X		
Mr. Sensenbrenner, Jr. (WI) .....			
Mr. Smith (TX) .....	X		
Mr. Chabot (OH) .....	X		
Mr. Issa (CA) .....	X		
Mr. Forbes (VA) .....	X		
Mr. King (IA) .....			
Mr. Franks (AZ) .....	X		
Mr. Gohmert (TX) .....			
Mr. Jordan (OH) .....	X		
Mr. Poe (TX) .....	X		
Mr. Chaffetz (UT) .....	X		
Mr. Marino (PA) .....	X		
Mr. Gowdy (SC) .....			
Mr. Labrador (ID) .....			
Mr. Farenthold (TX) .....	X		
Mr. Collins (GA) .....	X		
Mr. DeSantis (FL) .....			
Ms. Walters (CA) .....	X		
Mr. Buck (CO) .....	X		
Mr. Ratcliffe (TX) .....	X		
Mr. Trott (MI) .....	X		
Mr. Bishop (MI) .....	X		
Mr. Conyers, Jr. (MI), Ranking Member .....	X		
Mr. Nadler (NY) .....	X		
Ms. Lofgren (CA) .....	X		
Ms. Jackson Lee (TX) .....	X		
Mr. Cohen (TN) .....	X		
Mr. Johnson (GA) .....	X		
Mr. Pierluisi (PR) .....			
Ms. Chu (CA) .....	X		
Mr. Deutch (FL) .....			
Mr. Gutierrez (IL) .....			
Ms. Bass (CA) .....			
Mr. Richmond (LA) .....			
Ms. DelBene (WA) .....	X		
Mr. Jeffries (NY) .....	X		

**ROLLCALL NO. 1**—Continued

	Ayes	Nays	Present
Mr. Cicilline (RI) .....	X		
Mr. Peters (CA) .....	X		
Total .....	28	0	

**Committee Oversight Findings**

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

**New Budget Authority and Tax Expenditures**

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

**Congressional Budget Office Cost Estimate**

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 699, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,  
CONGRESSIONAL BUDGET OFFICE,  
*Washington, DC, April 25, 2016.*

Hon. BOB GOODLATTE, CHAIRMAN,  
*Committee on the Judiciary,  
House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 699, the "Email Privacy Act."

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz, who can be reached at 226-2860.

Sincerely,

KEITH HALL,  
DIRECTOR.

Enclosure

cc: Honorable John Conyers, Jr.  
Ranking Member

**H.R. 699—Email Privacy Act.**

As ordered reported by the House Committee on the Judiciary  
on April 13, 2016.

H.R. 699 would amend the Electronic Communications Privacy Act of 1986 (Public Law 99-508) to change current law relating to the privacy of certain personal communications. The bill also would change the procedures that government agencies must follow when requiring providers of remote computing services or electronic communication services to disclose stored communications. Many of those changes are technical in nature. CBO estimates that enacting the bill would have no significant cost to the federal government.

Enacting the legislation would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply. CBO estimates that enacting H.R. 699 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2027.

H.R. 699 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was approved by Theresa Gullo, Assistant Director for Budget Analysis.

#### **Duplication of Federal Programs**

No provision of H.R. 699 establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111-139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

#### **Disclosure of Directed Rule Makings**

The Committee estimates that H.R. 699 specifically directs to be completed no specific rule makings within the meaning of 5 U.S.C. § 551.

#### **Performance Goals and Objectives**

The Committee states that, pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 699 updates the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs.

#### **Advisory on Earmarks**

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 699 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of Rule XXI.

#### **Section-by-Section Analysis**

*Sec. 1. Short title.* Section 1 sets forth the short title of the bill as the “Email Privacy Act.”

*Sec. 2. Voluntary Disclosure Corrections.* Section 2 of the bill makes a series of technical and conforming changes to section 18 U.S.C. § 2702. For instance, to harmonize the statutory language in sections 2702 and 2703, the bill changes “divulge” to “disclose” and

inserts “wire or electronic” before “communication,” where relevant. The phrase “to the public” following “remote computing service” in paragraph (2) of subsection (a) is removed as redundant.<sup>26</sup> Section 2 also incorporates language such as “in electronic storage with, or otherwise stored, held, or maintained by” to clarify that the voluntary disclosure prohibitions and exceptions to that prohibition in section 2702 apply to the content of communications regardless of whether the communication has been opened or read.<sup>27</sup> This section also makes conforming changes to the lawful consent exceptions to voluntary disclosure in subsections (b) and (c) of section 2702.

*Sec. 3. Amendments to Required Disclosure Section.* Section 3 of the bill amends 18 U.S.C. §2703 to remove the tiered system of standards for compelling disclosure of communications content from a third party provider. Except as provided in subsections (i) and (j) of section 2703, subsections (a) and (b) require the government to obtain a warrant to compel disclosure by an ECS or RCS provider of stored wire or electronic communication content in a criminal investigation. It adds language authorizing the court to include a date by which providers must disclose the information sought in a warrant. In the absence of a date of disclosure, the provider must “promptly” respond to the warrant. Prompt response includes disclosure pursuant to the warrant, objection to the warrant, or a request for additional time to disclose pursuant to the warrant. Merely acknowledging receipt of a warrant or simply informing the governmental entity of when a provider intends to disclose contents pursuant to a warrant does not constitute “prompt” response under this section.

As with the amendments to section 2702, section 3 amends section 2703 to incorporate language such as “in electronic storage with, or otherwise stored, held, or maintained by” to clarify that the warrant standard applies to the content of communications regardless of whether the communication has been opened or read.<sup>28</sup>

Section 3 makes several technical and conforming changes to subsection (c) of section 2703 and instructs that subsection (c) is subject to the authorities preserved by subsections (i) and (j) of section 2703. Section 3 also amends subsection (d) to remove the authority to acquire the content of communications with a 2703(d) court order.

Section 3 creates a new subsection (h) acknowledging that an ECS or RCS provider may notify a subscriber or customer of receipt of a warrant, court order, subpoena, or request under subsections (a), (b), (c), or (d) of section 2703, unless prohibited from doing so pursuant to an order issued under section 2705.

Section 3 creates a new subsection (i) preserving the authority of a governmental entity to compel disclosure of a wire or electronic communication (including its content) directly from the originator, addressee, or intended recipient of a communication and preserving the authority of a governmental entity to compel disclosure of a wire or electronic communication (including its content) directly from a person or entity that provides an electronic communication service to its officers, directors, employees, or agents. Many—if not

<sup>26</sup> See definition of “remote computing service” in 18 U.S.C. §2711(2).

<sup>27</sup> See *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

<sup>28</sup> *Id.*

most—modern day businesses and governmental entities offer email services to their employees and officers, which constitutes an “electronic communication service” under the definition in the SCA.<sup>29</sup> Paragraph (2) of subsection (i) makes clear that the warrant standard in subsections (a) and (b) does not preclude the use of a subpoena to compel disclosure of wire or electronic communications directly from any individual, business, or governmental entity.

Paragraph (3) of the new subsection (i) preserves the ability of a governmental entity to compel disclosure of public commercial content with process other than a warrant.

Section 3 creates a new subsection (j) preserving the authority of Congress, through its constitutional power of inquiry, to require disclosure, including through use of a congressional subpoena, of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by an ECS or RCS provider.

*Sec. 4. Delayed Notice.* Section 4 amends the delayed notice provisions contained in 18 U.S.C. §2705. It strikes subsection (a) of section 2705, which currently sets forth procedures by which the government obtains a delayed-notice order against itself when it seeks to obtain the contents of a communication with a subpoena or 2703(d) order since, under subsections (a) and (b) of section 2703 as amended by this Act, a warrant is required to compel disclosure of the contents of a communication from an ECS or RCS.

Subsection (b) of existing section 2705 has been amended and renumbered as a new subsection (a). It allows the government to seek a court order instructing an ECS or RCS provider not to notify any other person of the existence of a warrant, order, subpoena, or other directive. The new subsection (b) authorizes a court to issue a delayed-notice order for a period of up to 180 days if the court determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will likely result in one of the following adverse results:

- (A) endangering the life or physical safety of an individual;
- (B) flight from prosecution;
- (C) destruction of or tampering with evidence;
- (D) intimidation of potential witnesses; or
- (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

The existing statute requires the court to find that notice “will” produce an adverse result. The new subsection (b) establishes a standard of “will likely” result. This does not require the government to demonstrate with a certainty that one of the outcomes will, in fact, result. The government need only demonstrate that the result is likely.

Section 4 creates a new subsection (c) to section 2705 to permit a governmental entity to seek one or more extensions of the delayed-notice order for periods of up to 180 days each.

<sup>29</sup> See 18 U.S.C. §2711(10) (cross-referencing the definitions in the Wiretap Act, 18 U.S.C. §2510. The definition of electronic communication service can be found at 18 U.S.C. §2510(15).

*Sec. 5. Rule of Construction.* Section 5 clarifies that nothing in the Act precludes acquisition of wire or electronic communications, including their contents, pursuant to the Wiretap Act, the Foreign Intelligence Surveillance Act, or any other provision of law not specifically amended by the Act.

### **Changes in Existing Law Made by the Bill, as Reported**

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

## **TITLE 18, UNITED STATES CODE**

\* \* \* \* \*

### **PART I—CRIMES**

\* \* \* \* \*

#### **CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS**

\* \* \* \* \*

#### **§ 2702. Voluntary disclosure of customer communications or records**

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly [divulge] *disclose* to any person or entity the contents of a communication [while in electronic storage by that service] *that is in electronic storage with or otherwise stored, held, or maintained by that service*; and

(2) a person or entity providing remote computing service [to the public] shall not knowingly [divulge] *disclose* to any person or entity the contents of any communication [which is carried or maintained on that service] *that is stored, held, or maintained by that service—*

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) [a provider of] *a person or entity providing* remote computing service or electronic communication service to the

public shall not knowingly **[divulge]** *disclose* a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may **[divulge]** *disclose* the contents of a *wire or electronic* communication—

**[(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;]**

*(1) to an originator, addressee, or intended recipient of such communication, to the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication, or to an agent of such addressee, intended recipient, subscriber, or customer;*

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

**[(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;]**

*(3) with the lawful consent of the originator, addressee, or intended recipient of such communication, or of the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication;*

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime;

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may **[divulge]** *disclose* a record or other information pertaining to a subscriber to or customer of such service (not including the contents of *wire or electronic* communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

**[(2) with the lawful consent of the customer or subscriber;]**

*(2) with the lawful consent of the subscriber or customer;*

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or seri-

ous physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8);

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges; and

(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).

### **§ 2703. Required disclosure of customer communications or records**

[(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

[(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

[(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

[(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

[(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

[(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

[(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

[(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

[(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

[(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

[(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

[(B) obtains a court order for such disclosure under subsection (d) of this section;

[(C) has the consent of the subscriber or customer to such disclosure;

[(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

[(E) seeks information under paragraph (2).

[(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

[(A) name;

[(B) address;

[(C) local and long distance telephone connection records, or records of session times and durations;

[(D) length of service (including start date) and types of service utilized;

[(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

[(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a

Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

【(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.】

(a) *CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.*—*Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by that service only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—*

(1) *is issued by a court of competent jurisdiction; and*

(2) *may indicate the date by which the provider must make the disclosure to the governmental entity.*

*In the absence of a date on the warrant indicating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.*

(b) *CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.*—

(1) *IN GENERAL.*—*Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of remote computing service of the contents of a wire or electronic communication that is stored, held, or maintained by that service only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—*

(A) *is issued by a court of competent jurisdiction; and*

(B) *may indicate the date by which the provider must make the disclosure to the governmental entity.*

*In the absence of a date on the warrant indicating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.*

(2) *APPLICABILITY.*—*Paragraph (1) is applicable with respect to any wire or electronic communication that is stored, held, or maintained by the provider—*

(A) *on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communication received by means of electronic transmission from), a subscriber or customer of such remote computing service; and*

(B) *solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.*

(c) *RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.*—

(1) *IN GENERAL.*—*Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of a record or other information pertaining to a sub-*

scriber to or customer of such service (not including the contents of wire or electronic communications), only—

(A) if a governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—

(i) is issued by a court of competent jurisdiction directing the disclosure; and

(ii) may indicate the date by which the provider must make the disclosure to the governmental entity;

(B) if a governmental entity obtains a court order directing the disclosure under subsection (d);

(C) with the lawful consent of the subscriber or customer; or

(D) as otherwise authorized in paragraph (2).

(2) **SUBSCRIBER OR CUSTOMER INFORMATION.**—A provider of electronic communication service or remote computing service shall, in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or any means available under paragraph (1), disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service used;

(E) telephone or instrument number or other subscriber or customer number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number);

of a subscriber or customer of such service.

(3) **NOTICE NOT REQUIRED.**—A governmental entity that receives records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) **REQUIREMENTS FOR COURT ORDER.**—A court order for disclosure under subsection [(b) or] (c) 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,] *sought* are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this [section] *subsection*, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) **NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.**—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance

with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(h) NOTICE.—*Except as provided in section 2705, a provider of electronic communication service or remote computing service may notify a subscriber or customer of a receipt of a warrant, court order, subpoena, or request under subsection (a), (b), (c), or (d) of this section.*

(i) RULE OF CONSTRUCTION RELATED TO LEGAL PROCESS.—*Nothing in this section or in section 2702 shall limit the authority of a governmental entity to use an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction to—*

(1) *require an originator, addressee, or intended recipient of a wire or electronic communication to disclose a wire or electronic communication (including the contents of that communication) to the governmental entity;*

(2) *require a person or entity that provides an electronic communication service to the officers, directors, employees, or agents of the person or entity (for the purpose of carrying out their duties) to disclose a wire or electronic communication (including the contents of that communication) to or from the person or entity itself or to or from an officer, director, employee, or agent of the entity to a governmental entity, if the wire or electronic communication is stored, held, or maintained on an electronic communications system owned, operated, or controlled by the person or entity; or*

(3) *require a person or entity that provides a remote computing service or electronic communication service to disclose a wire or electronic communication (including the contents of that communication) that advertises or promotes a product or service and that has been made readily accessible to the general public.*

(j) RULE OF CONSTRUCTION RELATED TO CONGRESSIONAL SUBPOENAS.—*Nothing in this section or in section 2702 shall limit the power of inquiry vested in the Congress by Article I of the Constitution of the United States, including the authority to compel the pro-*

*duction of a wire or electronic communication (including the contents of a wire or electronic communication) that is stored, held, or maintained by a person or entity that provides remote computing service or electronic communication service.*

\* \* \* \* \*

**【§ 2705. Delayed notice**

**【(a) DELAY OF NOTIFICATION.—**(1) A governmental entity acting under section 2703(b) of this title may—

**【(A)** where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

**【(B)** where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

**【(2)** An adverse result for the purposes of paragraph (1) of this subsection is—

**【(A)** endangering the life or physical safety of an individual;

**【(B)** flight from prosecution;

**【(C)** destruction of or tampering with evidence;

**【(D)** intimidation of potential witnesses; or

**【(E)** otherwise seriously jeopardizing an investigation or unduly delaying a trial.

**【(3)** The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

**【(4)** Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

**【(5)** Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—

**【(A)** states with reasonable specificity the nature of the law enforcement inquiry; and

**【(B)** informs such customer or subscriber—

**【(i)** that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

**【(ii)** that notification of such customer or subscriber was delayed;

[(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

[(iv) which provision of this chapter allowed such delay.

[(6) As used in this subsection, the term “supervisory official” means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency’s headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney’s headquarters or regional office.

[(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

[(1) endangering the life or physical safety of an individual;

[(2) flight from prosecution;

[(3) destruction of or tampering with evidence;

[(4) intimidation of potential witnesses; or

[(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.]

**§2705. DELAYED NOTICE.**

(a) *IN GENERAL.*—A governmental entity acting under section 2703 may apply to a court for an order directing a provider of electronic communication service or remote computing service to which a warrant, order, subpoena, or other directive under section 2703 is directed not to notify any other person of the existence of the warrant, order, subpoena, or other directive.

(b) *DETERMINATION.*—A court shall grant a request for an order made under subsection (a) for delayed notification of up to 180 days if the court determines that there is reason to believe that notification of the existence of the warrant, order, subpoena, or other directive will likely result in—

(1) *endangering the life or physical safety of an individual;*

(2) *flight from prosecution;*

(3) *destruction of or tampering with evidence;*

(4) *intimidation of potential witnesses; or*

(5) *otherwise seriously jeopardizing an investigation or unduly delaying a trial.*

*(c) EXTENSION.—Upon request by a governmental entity, a court may grant one or more extensions, for periods of up to 180 days each, of an order granted in accordance with subsection (b).*

\* \* \* \* \*

○