G:\OFFICE\RAMSEYER\R18\RPT\H4639JD_RPT.XML

118TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
118–

FOURTH AMENDMENT IS NOT FOR SALE ACT

JANUARY --, 2024.—Ordered to be printed

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

R E P O R T

together with

_____ VIEWS

[To accompany H.R. 4639]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 4639) to amend section 2702 of title 18, United States Code, to prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value, to address communications and records in the possession of intermediary internet service providers, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

Table of Contents

Purpose and Summary 3
Background and Need for the Legislation 3
Hearings 8
Committee Consideration 8
Committee Votes 8
Committee Oversight Findings 10
New Budget Authority and Tax Expenditures 10
Congressional Budget Office Cost Estimate 10
Committee Estimate of Budgetary Effects 12
Duplication of Federal Programs 12
Performance Goals and Objectives 12
Advisory on Earmarks 12
Federal Mandates Statement 12
Advisory Committee Statement 12
Applicability to Legislative Branch 12
Section-by-Section Analysis 13
Changes in Existing Law Made by the Bill, as Reported 14

Purpose and Summary

H.R. 4639, the Fourth Amendment Is Not For Sale Act, introduced by Rep. Warren Davidson (R-OH), closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement, intelligence agencies, and other government agencies without the agency first acquiring a warrant. If the agency were to gather this information itself, it would be required to obtain a warrant, subpoena, or other legal order. By closing this loophole, the bill prevents government agencies from conducting an end-run around the protections of the Fourth Amendment.

Background and Need for the Legislation

i. Electronic Communications Privacy Act

Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) to limit the government's ability to access digital communications.[1] Under ECPA, the government must seek a warrant or other court order before compelling certain electronic communications services providers to disclose the contents and records of electronic communications. These warrant and order requirements, however, only apply to certain communications services providers.

ECPA prevents a Remote Computing Service (RCS) and an Electronic Communications Service (ECS) provider from knowingly disclosing communications contents to third parties under certain circumstances. An RCS provider engages in the "provision to the public of computer storage or processing services by means of an electronic communications system."[2] An ECS provider offers "any service which provides to users thereof the ability to send or receive wire or electronic communications."[3] These include phone companies like AT&T and Verizon, and tech companies like Google, Microsoft, and Facebook.

An ECS provider is prohibited from disclosing to third parties "the contents of a communication while in electronic storage by that service,"[4] while an RCS provider cannot disclose "the contents of any communication which is carried or maintained on that service."[5] Both providers are prohibited from knowingly divulging non-content information to the government absent an exception.[6] The government may obtain subscriber information, like names, addresses, and phone numbers, from an RCS or ECS by obtaining a subpoena.[7] The government may obtain more sensitive non-content information, like traffic or transactional

[1] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, Center for Democracy & Technology at 15 (2021).
[2] 18 U.S.C. § 2711(2).
[3] 18 U.S.C. § 2510(15).
[4] 18 U.S.C. § 2702(a)(1).
[5] 18 U.S.C. § 2702(a)(2).
[6] *See* 18 U.S.C. § 2702(a)(3), (b).
[7] *See* 18 U.S.C. § 2703(c)(2).

information, by obtaining a separate order after demonstrating "specific and articulable facts showing that there are reasonable grounds to believe" that the information is "relevant and material to an ongoing criminal investigation."[8] When the government seeks to obtain the content of electronic communications, it must obtain a probable cause warrant.[9]

However, ECPA does not restrict the ability of these electronic communications services providers to voluntarily providing non-content information to non-government third parties.[10] As long as those third parties are not RCS or ECS providers, then ECPA does not apply to them and does not prohibit their selling the information to the government.[11] This has led to a loophole whereby RCS and ECS providers can transfer data to private third parties and the government is able to purchase the data from those third parties without obtaining the otherwise required court order, subpoena, or warrant.

At a hearing of the Subcommittee on Crime and Federal Government Surveillance on July 14, 2023, witnesses addressed this data broker loophole.[12] One witness testified that "the law is woefully outdated. It does not cover digital data brokers or many app developers, for the simple reason that they did not exist in 1986, when the law was passed. This gap creates an easy end-run around the law's protections."[13] Data brokers serve as a "middleman" and allow the government to sidestep the requirements of the Fourth Amendment.[14]

ii. Supreme Court Precedent on Location Data

Over 40 years ago, the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[15] The Court has relied on this "third-party doctrine" over the years to find that the Fourth Amendment does not protect records or information voluntarily shared with someone else.[16] In 2018, in *Carpenter v. United States*, however, the Court held "that the Government must generally obtain a warrant supported by probable cause before acquiring" cell-site location information for a seven-day period.[17] Writing for the Court, Chief Justice Roberts highlighted the "seismic shifts in digital technology" that makes tracking a person's location possible.[18] The Court recognized that location information "provides an intimate window into a person's life, revealing not only his particular

---

[8] Shenkman, et al. *supra* note 1 at 16; See *also* 18 U.S.C. § 2703(d).
[9] Shenkman, et al. *supra* note 1 at 16.
[10] *Id.*
[11] *Id.*
[12] *See Fixing FISA, Part II: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).
[13] *Id.* (Testimony of Elizabeth Goitein at 39).
[14] *Id.*
[15] *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (citing *United States v. Miller*, 425 U.S. 435, 442-44 (1976)).
[16] *See* Amy Howe, *Opinion analysis: Court holds that police will generally need a warrant for sustained cellphone location information*, SCOTUSblog (Jun. 22, 2018), https://www.scotusblog.com/2018/06/opinion-analysis-court-holds-that-police-will-generally-need-a-warrant-for-cellphone-location-information/.
[17] *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018).
[18] *Id.* at 2219.

movements, but through them, his 'familial, political, professional, religious, and sexual associations.'"[19]

While the Court's decision in *Carpenter* dealt with cell-site location information, rather than commercially available geolocation data available for purchase from data brokers, "the Court's reasoning surrounding the privacy concerns of location data strongly suggest that collection of a multitude of sensitive digital information . . . is also covered by the Fourth Amendment's warrant requirement."[20] However, the government has construed *Carpenter*'s holding as limited to the facts of the case. Indeed, the Court "expressly declined to consider what other types of information might qualify for Fourth Amendment protection despite being disclosed to a third party."[21]

iii. Data Collection, Retention, and Sale

Today, data is often referred to as the world's most valuable resource, even surpassing oil.[22] It can include information from public sources, such as "demographic information, property records, court filings, criminal convictions, professional licenses, census data, birth certificates, marriage licenses, divorce records," bankruptcy records, and voter registration information, among others.[23] Commercially-sourced data may include "purchase history, warranty registration, credit information, employment registration, loyalty card data, membership data, subscriptions, etc."[24] And still yet, even more intimate data can be procured through the collection of information originating from "social media profiles, web browsing activity, mobile apps, media reports, websites, mail-in rebate forms, forum posts, web browser cookies, plugins, addons, device data, IP fingerprints, network data, metadata" and so on.[25]

Data brokers aggregate, package, and sell the data acquired from a variety of sources, including those described above. Often, data brokers have thousands of different data points reflecting information about a person that, when combined, reveal valuable and intimate insights about an individual that would otherwise be unavailable.[26] In other words, for data brokers, consumers and their information are the product.[27] For example, data brokers can receive geolocation data, sometimes accurate to just a few yards, from a mobile device up to 14,000 times per day.[28] This data allows a purchaser to identify patterns that can reveal where a person

---

[19] *Id.* at 2217 (citing *United States v. Jones*, 565 U.S. 400, 415 (Sotomayor, J., concurring)).
[20] Shenkman, et al. *supra* note 1 at 18.
[21] *See Fixing FISA, Part II: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023) (Testimony of Elizabeth Goitein at 41).
[22] Kiran Bhageshpur, *Data Is The New Oil – And That's A Good Thing*, FORBES (Nov. 15, 2019).
[23] Henrik Twetman, *Gundars Bergmanis-Korats, Data Brokers and Security: Risks and vulnerabilities related to commercially available data*, NATO STRATEGIC COMMC'NS CTRE. OF EXCELLENCE 11 (Jan. 20, 2020).
[24] *Id.*
[25] *Id.*
[26] *What Are Data Brokers – And What Is Your Data Worth*?, WEBFX (Mar. 16, 2020).
[27] *See* Data Brokers, Electronic Privacy Information Center, https://epic.org/issues/consumer-privacy/data-brokers/.
[28] Jennifer Valentino-DeVries, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018).

lives, where they work, and where they spend their free time.[29] This information can be useful in commercial applications, such as advertising.[30] But it can also be exploited to learn about a person's daily life and to track their historic movements.[31]

As a result of the nature of this information, it is extremely attractive to government agencies, and recent reporting indicates that data-based policing is becoming increasingly prevalent. For example, the Internal Revenue Service (IRS), Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Department of Defense (DOD) have all purchased geolocation information from data brokers.[32] And other experts have found that the practice of law enforcement and intelligence agencies buying sensitive data—ranging from geolocation to personal communications—is increasing, with some agencies spending "tens of millions of dollars on multi-year contracts."[33]

In recent years, the government has turned to data brokers like Venntel to purchase location data from Americans' smartphones. The IRS purchased access to a commercial database that "records the locations of millions of American cellphones" to attempt to "identify and track potential criminal suspects."[34] Another data broker, Clearview AI, developed a facial recognition software to create a database of photos from sites like Facebook, LinkedIn, and Twitter and marketed to law enforcement.[35] Because ECPA does not protect consumers from data brokers that collect their information, the government purchases data as way to avoid seeking a warrant as would otherwise be required by the Fourth Amendment.[36]

Last year, the FBI admitted to buying "precise geolocation data derived from mobile-phone advertising."[37] At a hearing before the Senate Select Committee on Intelligence, Director Wray stated that the FBI now seeks court orders when obtaining phone data from commercial vendors, but the data broker loophole in ECPA would permit the FBI to resume purchasing such data in the future.[38] Leaked documents also revealed that Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) purchased cell phone location data, and ICE

---

[29] *See Id*.
[30] *Id*.
[31] *Id*.
[32] Elizabeth Goitein, *The government can't seize your digital data. Except by buying it.*, WASH. POST (Apr. 26, 2021).
[33] Sharon Bradford Franklin, Greg Nojeim & Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 9, 2021).
[34] *See* Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL STREET JOURNAL (Jun. 19, 2020).
[35] *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, THE NEW YORK TIMES (Jan. 18, 2020).
[36] *See* Alex Deise, *Bill of the Month: The Fourth Amendment is Not for Sale Act*, FREEDOMWORKS (Jul. 29, 2022).
[37] *See* Byron Tau, *FBI Once Bought Mobile-Phone Data for Warrantless Tracking. Other Agencies Still Do.*, WALL STREET JOURNAL (Mar. 10, 2023).
[38] *Id.*

also purchased utility data and information from private license plate reader databases.[39] Defense contractors reportedly purchased location data from Muslim prayer apps and dating apps.[40] The Secret Service and DOD have also purchased smart phone location data.[41]

As part of the Committee on the Judiciary's investigation into the IRS's troubling visit to the home of journalist Matt Taibbi on the day he testified before the Select Subcommittee on the Weaponization of the Federal Government, the Committee discovered that the IRS collected personal data from data brokers to use in its investigation of Taibbi.[42] For example, the IRS collected data from the data broker Anywho, a People Search Website.[43] It is concerning enough that the IRS would take the extreme step of visiting someone's home on the day he testified before Congress, but the IRS also compiled its information from a data broker, potentially accessing vast amounts of Taibbi's private information.

These actions allow government agencies and law enforcement to evade the Fourth Amendment and collect limitless information of Americans. The Fourth Amendment Is Not For Sale Act closes this legal loophole and stops data brokers from selling Americans' personal information to the government by requiring the government to obtain a court order before acquiring customer or subscriber information from a third party.

On July 19, 2023, the Committee unanimously approved H.R. 4639, the Fourth Amendment Is Not For Sale Act.[44] During the markup of H.R. 4639, Members expressed a concern regarding warrantless government surveillance of Americans' data.[45] Specifically, Members criticized the developing practice wherein government agencies are able to exploit a legal loophole to purchase massive amounts of Americans' information from data brokers, even though that same information would ordinarily require the agency to obtain a court order if gathering the information themselves.[46]

As technology continues to advance and Americans incidentally share more data through the devices we use every day, it is important for Congress to protect privacy interests and ensure that government agencies and law enforcement abide by the Fourth Amendment. In the Fourth Amendment Is Not For Sale Act, Congress has the opportunity to codify the Supreme Court's decision in *Carpenter* and address "additional categories of highly sensitive information that merit the protection of a warrant regardless of whether they are held by third parties."[47]

---

[39] *See* Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, BRENNAN CENTER FOR JUSTICE (Apr. 16, 2021).
[40] *Id.*
[41] *Id.*
[42] *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Daniel Werfel, Commissioner, Internal Revenue Service (May 24, 2023).
[43] *See* Yael Grauer, *Here's a Long List of Data Broker Sites and How to Opt-Out of Them*, VICE (Mar. 27, 2018).
[44] *Markup of H.R. 1531, H.R. 4250, and H.R. 4639 Before the H. Comm. On the Judiciary*, 118th Cong. (2023).
[45] *See generally id.*
[46] *Id.*
[47] *Id.*

Hearings

For the purposes of clause 3(c)(6)(A) of House rule XIII, the following hearing was used to develop H.R. 4639: "Fixing FISA, Part II," a hearing held on July 14, 2023, before the Subcommittee on Crime and Federal Government Surveillance, of the Committee on the Judiciary. The Subcommittee heard testimony from the following witnesses:

- Professor Jonathan Turley, George Washington University Law School;
- Mr. Phil Kiko, Principal, Williams & Jensen;
- Mr. Gene Schaerr, General Counsel, Project for Privacy and Surveillance Accountability; and
- Ms. Elizabeth Goitein, Senior Director, Liberty & National Security Program, Brennan Center for Justice.

The hearing addressed the need for protections regarding the federal government's purchase of data from data brokers.

Committee Consideration

On July 19, 2023, the Committee met in open session and ordered the bill, H.R. 4639, favorably reported without amendment, by a roll call vote of 30-0-1, a quorum being present.

Committee Votes

In compliance with clause 3(b) of House rule XIII, the following roll call votes occurred during the Committee's consideration of H.R. 4639:

1. Vote on favorably reporting H.R. 4639—passed 30 ayes to 0 nays, 1 present.

COMMITTEE ON THE JUDICIARY

Date: 7/19/23

118th CONGRESS

25-19

ROLL CALL

Vote on: Final Passage of H.R. 4639

Roll Call #: 2

REPUBLICANS	AYE	NO	PRESENT	DEMOCRATS	AYE	NO	PRESENT
MR. JORDAN (OH) *Chairman*	✓			MR. NADLER (NY) *Ranking Member*	✓		
MR. ISSA (CA)	✓			MS. LOFGREN (CA)	✓		
MR. BUCK (CO)				MS. JACKSON LEE (TX)	✓		
MR. GAETZ (FL)	✓			MR. COHEN (TN)	✓		
MR. JOHNSON (LA)	✓			MR. JOHNSON (GA)			✓
MR. BIGGS (AZ)	✓			MR. SCHIFF (CA)	✓		
MR. McCLINTOCK (CA)	✓			MR. SWALWELL (CA)	✓		
MR. TIFFANY (WI)	✓			MR. LIEU (CA)			
MR. MASSIE (KY)				MS. JAYAPAL (WA)	✓		
MR. ROY (TX)				MR. CORREA (CA)	✓		
MR. BISHOP (NC)	✓			MS. SCANLON (PA)	✓		
MS. SPARTZ (IN)	✓			MR. NEGUSE (CO)			
MR. FITZGERALD (WI)				MS. McBATH (GA)			
MR. BENTZ (OR)				MS. DEAN (PA)	✓		
MR. CLINE (VA)	✓			MS. ESCOBAR (TX)	✓		
MR. GOODEN (TX)				MS. ROSS (NC)	✓		
MR. VAN DREW (NJ)				MS. BUSH (MO)			
MR. NEHLS (TX)				MR. IVEY (MD)	✓		
MR. MOORE (AL)	✓			MS. BALINT (VT)	✓		
MR. KILEY (CA)	✓						
MS. HAGEMAN (WY)	✓						
MR. MORAN (TX)	✓						
MS. LEE (FL)	✓						
MR. HUNT (TX)							
MR. FRY (SC)	✓						

Roll Call Totals: Ayes: 30 Nays: 0 Present: 1

Passed: X Failed: _____

Committee Oversight Findings

In compliance with clause 3(c)(1) of House rule XIII, 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 does not apply where a cost estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the *Congressional Budget Act of 1974* has been timely submitted prior to filing of the report and is included in the report. Such a cost estimate is included in this report.

Congressional Budget Office Cost Estimate

With respect to the requirement of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the *Congressional Budget Act of 1974*, the Committee has received the enclosed cost estimate for H.R. 4639 from the Director of the Congressional Budget Office:

Congressional Budget Office
Cost Estimate

November 14, 2023

H.R. 4639, Fourth Amendment Is Not For Sale Act

As ordered reported by the House Committee on the Judiciary on July 19, 2023

By Fiscal Year, Millions of Dollars	2024	2024-2028	2024-2033
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	a	a	a

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2034?	No	Statutory pay-as-you-go procedures apply?	No
		Mandate Effects	
	No	Contains intergovernmental mandate?	Excluded from UMRA

Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2034?	Contains private-sector mandate?	**Excluded from UMRA**
a = CBO has no basis to estimate the effects on spending subject to appropriation from implementing H.R. 4639.		

H.R. 4639 would prohibit law enforcement and intelligence agencies from purchasing personal information about customers or subscribers of electronic and remote computing service providers (for example, social media, cell phone, email, and cloud-computing companies) from a third party. Current law prohibits those entities from disclosing such information, which includes names, addresses, phone numbers, and location, directly to government agencies without a court order. However, those companies are permitted to voluntarily disclose such information to third parties, which can then provide it to the government. H.R. 4639 would require a law enforcement or intelligence agency to obtain a court order before acquiring customer or subscriber information from a third party. Under the bill, any information purchased from a third party would be inadmissible as evidence in court.

H.R. 4639 would affect the operating costs of federal law enforcement and intelligence agencies, which are subject to annual appropriations. The magnitude and direction of those effects is subject to significant uncertainty. The bill could reduce costs by preventing those agencies from purchasing customer or subscriber information. The bill could increase costs for those agencies' investigative and intelligence-gathering activities if they require additional administrative resources or personnel to obtain information they currently purchase at a lower cost. CBO has no basis on which to estimate the net cost of those changes. Any change in spending from implementing H.R. 4639 would be subject to future appropriation actions.

CBO has not reviewed H.R. 4639 for intergovernmental or private-sector mandates. Section 4 of the Unfunded Mandates Reform Act excludes from the application of that act any legislative provisions that would enforce the constitutional rights of individuals. CBO has determined that the bill falls within that exclusion because it extends protections against the unreasonable search and seizure of personal data.

The CBO staff contacts for this estimate are Jeremy Crimm (for the Departments of Justice and Homeland Security), Bill Ma (for the Department of Defense), and Erich Dvorak (for mandates). The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

Phillip L. Swagel
Director, Congressional Budget Office

Committee Estimate of Budgetary Effects

With respect to the requirements of clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the *Congressional Budget Act of 1974*.

Duplication of Federal Programs

Pursuant to clause 3(c)(5) of House rule XIII, no provision of H.R. 4639 establishes or reauthorizes a program of the federal government known to be duplicative of another federal program.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of House rule XIII, H.R. 4639 closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement, intelligence agencies, and other government agencies without the agency first acquiring a warrant.

Advisory on Earmarks

In accordance with clause 9 of House rule XXI, H.R. 4639 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clauses 9(d), 9(e), or 9(f) of House Rule XXI.

Federal Mandates Statement

The Committee adopts as its own the estimate of federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the *Unfunded Mandates Reform Act*.

Advisory Committee Statement

No advisory committees within the meaning of section 5(b) of the *Federal Advisory Committee Act* were created by this legislation.

Applicability to Legislative Branch

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the *Congressional Accountability Act* (Pub. L. 104-1).

Section-by-Section Analysis

Sec. 1. Short Title.

- The Act is the "Fourth Amendment Is Not For Sale Act."

Sec. 2. Protection of Records Held By Data Brokers.

- Defines various terms and prevents law enforcement and intelligence agencies from buying data about a United States person, located anywhere in the world, or data about any person located in the United States that:
    - Is data about a person's device, from their online account, or created or shared by a technology and telecommunications company providing a service to that person;
    - Was obtained from a technology or communications company providing service to the target in a manner that violated a contract, or the company's terms of service or privacy policy;
    - Was obtained by deceiving the person whose information was obtained; or
    - Was obtained by accessing the person's device or online account without authorization.
- Also prohibits the use or sharing by the government of any information obtained in violation of this section. This section further requires the Attorney General to adopt specific procedures to minimize the acquisition and retention of this information, and to prohibit its dissemination.

Sec. 3. Required Disclosure.

- Extends the protections in the Electronic Communications Privacy Act – which requires the government to obtain a warrant to compel technology and communications companies to turn over their customers' data – to the categories of data protected in Section 2 held by data brokers.

Sec. 4. Intermediary Service Providers.

- Extends the protections in the Electronic Communications Privacy Act to data held by intermediary service providers, which are entities that directly or indirectly deliver, store, or process communications for or on behalf of technology or communications firms.

Sec. 5. Limits on Surveillance Conducted for Foreign Intelligence Purposes Other than Under the Foreign Intelligence Surveillance Act of 1978.

- Narrows a legal carveout in FISA permitting the intelligence community, without an order issued by a court, to buy or obtain through other methods, metadata about calls, texts, emails, and web browsing, where at least one end of the communication is located abroad. This section limits the carveout such that it only applies to the acquisition of foreign intelligence information of non-Americans located outside the United States.

- Specifies that FISA authorities shall be the exclusive means by which the government obtains information inside the U.S. or from U.S. technology or communications companies electronic communications transactions records, call detail records, or other metadata about the communications of United States persons, located anywhere in the world, or any person located in the United States.

- Specifies that Title I and sections 303, 304, 703, 704, and 705 of FISA shall be the exclusive means by which the government obtains inside the location information of U.S. persons or persons inside the United States, web browsing history, Internet search history, or any other data that would require a court order to compel, about United States persons, located anywhere in the world, or any person located in the United States.

Sec. 6. Limit on Civil Immunity for Providing Information, Facilities, or Technical Assistance to the Government Absent a Court Order.

- Removes the Attorney General's authority to grant civil immunity to those that provide unlawful assistance for government surveillance not required or permitted by federal law. Immunity remains for any surveillance assistance ordered by a court.

Changes in Existing Law Made by the Bill, as Reported

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 119—WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

* * * * * * *

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

[(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that

all statutory requirements have been met, and that the specified assistance is required,]

(B) a certification in writing—

(I) by a person specified in section 2518(7) or the Attorney General of the United States;

(II) that the requirements for an emergency authorization to intercept a wire, oral, or electronic communication under section 2518(7) have been met; and

(III) that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

[(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.]

(iii) For assistance provided pursuant to a certification under subparagraph (ii)(B), the limitation on causes of action under the last sentence of the matter following subparagraph (ii)(B) shall only apply to the extent that the assistance ceased at the earliest of the time the application for a court order was denied, the time the communication sought was obtained, or 48 hours after the interception began.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

[(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.**]**

(f)(i)(A) Nothing contained in this chapter, chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934 (47 U.S.C. 151 et seq.) shall be deemed to affect an acquisition or activity described in clause (B) that is carried out utilizing a means other than electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(B) An acquisition or activity described in this clause is—

(I) an acquisition by the United States Government of foreign intelligence information from international or foreign communications that—

(aa) is acquired pursuant to express statutory authority; or

(bb) only includes information of persons who are not United States persons and are located outside the United States; or

(II) a foreign intelligence activity involving a foreign electronic communications system that—

(aa) is conducted pursuant to express statutory authority; or

(bb) only involves the acquisition by the United States Government of information of persons who are not United States persons and are located outside the United States.

(ii) The procedures in this chapter, chapter 121, and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which electronic surveillance, as de-

fined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

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

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

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

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)(i) If the communication is—

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection—

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

* * * * * * *

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 to any person or entity the contents of a communication while in electronic storage by that service; **[**and**]**

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried 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 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 remote computing service or electronic communication service to the public shall not knowingly divulge 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[.]*; and*

(4) an intermediary service provider shall not knowingly divulge—

(A) to any person or entity the contents of a communication while in electronic storage by that provider; or

(B) to any governmental entity a record or other information pertaining to a subscriber to or customer of, a recipient of a communication from a subscriber to or customer of, or the sender of a communication to a subscriber to or customer of, the provider of electronic communication service to the public or the provider of remote computing service for, or on behalf of, which the intermediary service provider directly or indirectly delivers, transmits, stores, or processes communications.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

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

(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;

(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; or

(8) 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 communications relating to the emergency; or

(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of 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;

(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 serious 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;

(6) to any person other than a governmental entity; or

(7) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(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).

(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR ANYTHING OF VALUE CERTAIN RECORDS AND INFORMATION BY LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.—

(1) DEFINITIONS.—In this subsection—

(A) the term "covered customer or subscriber record" means a covered record that is—

(i) disclosed to a third party by—

(I) a provider of an electronic communication service to the public or a provider of a remote com-

puting service of which the covered person with respect to the covered record is a subscriber or customer; or

(II) an intermediary service provider that delivers, stores, or processes communications of such covered person;

(ii) collected by a third party from an online account of a covered person; or

(iii) collected by a third party from or about an electronic device of a covered person;

(B) the term "covered person" means—

(i) a person who is located inside the United States; or

(ii) a person—

(I) who is located outside the United States or whose location cannot be determined; and

(II) who is a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

(C) the term "covered record" means a record or other information that—

(i) pertains to a covered person; and

(ii) is—

(I) a record or other information described in the matter preceding paragraph (1) of subsection (c);

(II) the contents of a communication; or

(III) location information;

(D) the term "electronic device" has the meaning given the term "computer" in section 1030(e);

(E) the term "illegitimately obtained information" means a covered record that—

(i) was obtained—

(I) from a provider of an electronic communication service to the public or a provider of a remote computing service in a manner that—

(aa) violates the service agreement between the provider and customers or subscribers of the provider; or

(bb) is inconsistent with the privacy policy of the provider;

(II) by deceiving the covered person whose covered record was obtained; or

(III) through the unauthorized accessing of an electronic device or online account; or

(ii) was—

(I) obtained from a provider of an electronic communication service to the public, a provider of a remote computing service, or an intermediary service provider; and

(II) collected, processed, or shared in violation of a contract relating to the covered record;

(F) the term "intelligence community" has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003);

(G) the term "location information" means information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, or device;

(H) the term "obtain in exchange for anything of value" means to obtain by purchasing, to receive in connection with services being provided for consideration, or to otherwise obtain in exchange for consideration, including an access fee, service fee, maintenance fee, or licensing fee;

(I) the term "online account" means an online account with an electronic communication service to the public or remote computing service;

(J) the term "pertain", with respect to a person, means—

(i) information that is linked to the identity of a person; or

(ii) information—

(I) that has been anonymized to remove links to the identity of a person; and

(II) that, if combined with other information, could be used to identify a person; and

(K) the term "third party" means a person who—

(i) is not a governmental entity; and

(ii) in connection with the collection, disclosure, obtaining, processing, or sharing of the covered record at issue, was not acting as—

(I) a provider of an electronic communication service to the public; or

(II) a provider of a remote computing service.

(2) LIMITATION.—

(A) IN GENERAL.—A law enforcement agency of a governmental entity and an element of the intelligence community may not obtain from a third party in exchange for anything of value a covered customer or subscriber record or any illegitimately obtained information.

(B) INDIRECTLY ACQUIRED RECORDS AND INFORMATION.—The limitation under subparagraph (A) shall apply without regard to whether the third party possessing the covered customer or subscriber record or illegitimately obtained information is the third party that initially obtained or collected, or is the third party that initially received the disclosure of, the covered customer or subscriber record or illegitimately obtained information.

(3) LIMIT ON SHARING BETWEEN AGENCIES.—An agency of a governmental entity that is not a law enforcement agency or an element of the intelligence community may not provide to a law enforcement agency of a governmental entity or an element of the intelligence community a covered customer or subscriber

record or illegitimately obtained information that was obtained from a third party in exchange for anything of value.

(4) PROHIBITION ON USE AS EVIDENCE.—A covered customer or subscriber record or illegitimately obtained information obtained by or provided to a law enforcement agency of a governmental entity or an element of the intelligence community in violation of paragraph (2) or (3), and any evidence derived therefrom, may not be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

(5) MINIMIZATION PROCEDURES.—

(A) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, of information pertaining to a covered person that is acquired in violation of paragraph (2) or (3).

(B) USE BY AGENCIES.—If a law enforcement agency of a governmental entity or element of the intelligence community acquires information pertaining to a covered person in violation of paragraph (2) or (3), the law enforcement agency of a governmental entity or element of the intelligence community shall minimize the acquisition and retention, and prohibit the dissemination, of the information in accordance with the procedures adopted under subparagraph (A).

§ 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 and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) 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 and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) 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 and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) 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 en-

gaged 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.

(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, 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, 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) COMITY ANALYSIS AND DISCLOSURE OF INFORMATION REGARDING LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—

(1) DEFINITIONS.—In this subsection—

(A) the term "qualifying foreign government" means a foreign government—

(i) with which the United States has an executive agreement that has entered into force under section 2523; and

(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

(B) the term "United States person" has the meaning given the term in section 2523.

(2) MOTIONS TO QUASH OR MODIFY.—(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—

(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.

(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the

opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that—

(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

(iii) the customer or subscriber is not a United States person and does not reside in the United States.

(3) COMITY ANALYSIS.—For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate—

(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;

(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

(E) the nature and extent of the provider's ties to and presence in the United States;

(F) the importance to the investigation of the information required to be disclosed;

(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

(4) DISCLOSURE OBLIGATIONS DURING PENDENCY OF CHALLENGE.—A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion brought under this subsection, unless the court finds that immediate production is necessary to prevent an adverse result identified in section 2705(a)(2).

(5) DISCLOSURE TO QUALIFYING FOREIGN GOVERNMENT.—(A) It shall not constitute a violation of a protective order issued under section 2705 for a provider of electronic communication service to the public or remote computing service to disclose to the entity within a qualifying foreign government, designated in an executive agreement under section 2523, the fact of the existence of legal process issued under this section seeking the contents of a wire or electronic communication of

a customer or subscriber who is a national or resident of the qualifying foreign government.

(B) Nothing in this paragraph shall be construed to modify or otherwise affect any other authority to make a motion to modify or quash a protective order issued under section 2705.

(i) COVERED CUSTOMER OR SUBSCRIBER RECORDS AND ILLEGITIMATELY OBTAINED INFORMATION.—

(1) DEFINITIONS.—In this subsection, the terms "covered customer or subscriber record", "illegitimately obtained information", and "third party" have the meanings given such terms in section 2702(e).

(2) LIMITATION.—Unless a governmental entity obtains an order in accordance with paragraph (3), the governmental entity may not require a third party to disclose a covered customer or subscriber record or any illegitimately obtained information if a court order would be required for the governmental entity to require a provider of remote computing service or a provider of electronic communication service to the public to disclose such a covered customer or subscriber record or illegitimately obtained information that is a record of a customer or subscriber of the provider.

(3) ORDERS.—

(A) IN GENERAL.—A court may only issue an order requiring a third party to disclose a covered customer or subscriber record or any illegitimately obtained information on the same basis and subject to the same limitations as would apply to a court order to require disclosure by a provider of remote computing service or a provider of electronic communication service to the public of a record of a customer or subscriber of the provider.

(B) STANDARD.—For purposes of subparagraph (A), a court shall apply the most stringent standard under Federal statute or the Constitution of the United States that would be applicable to a request for a court order to require a comparable disclosure by a provider of remote computing service or a provider of electronic communication service to the public of a record of a customer or subscriber of the provider.

* * * * * * *

§ 2711. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" includes—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title;

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; or

(C) a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice) to which a military judge has been detailed; **[**and**]**

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof**[**.**]***; and*

(5) the term "intermediary service provider" means an entity or facilities owner or operator that directly or indirectly delivers, stores, or processes communications for or on behalf of a provider of electronic communication service to the public or a provider of remote computing service.

* * * * * * *