universität wien

MASTER-THESIS

Titel der Master-Thesis

„MAINWAY and the Constitution - an analysis of the contradicting interpretation of the constitutional and statutory authorization of the bulk telephone metadata collection by original US Federal Courts“

Verfasserin
Mag. Dr. Brigitte Raicher-Siegl

angestrebter akademischer Grad
Master of Laws (LL.M.)

Wien, 2014

Universitätslehrgang:	Informations- und Medienrecht
Studienkennzahl lt. Studienblatt:	A 992 942
Betreuer:	MMag. Franz Heidinger LL.M.

To my Mom, Günther, Kathi and Lloyd who
mentor, encourage and inspire me every day

As for our common defense, we reject as false the choice between our safety and our ideals. Our Founding Fathers, faced with perils that we can scarcely imagine, drafted a charter to assure the rule of law and the rights of man -- a charter expanded by the blood of generations. Those ideals still light the world, and we will not give them up for expedience sake.

President Barack Obama - Inaugural Address 2009

Table of Contents

Abbreviations

Abr	Text
ACLU	American Civil Liberties Union
ACLUF	American Civil Liberties Union Foundation,
CRS	Congressional Research Service
DNI	Director National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
FAA	FISA Amendment Act of 2009
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
n.	footnote
NSA	National Security Agency
NYCLU	New York Civil Liberties Union
NYCLUF	New York Civil Liberties Union Foundation
ODNI	Office of the Director National Intelligence
p	Page
PCLOB	Privacy and Civil Liberties Oversight Board
POTUS	President of the United States
RAS	Reasonable articulable suspicion
SCOTUS	Supreme Court of the United States
SID	Signal Intelligence Director

1. Introduction

This thesis only analyses the collection of telephone metadata of US citizens' electronic communication for the MAINWAY database within the territory of the United States under Section 215 of the USA PATRIOT Act and not the National Security Agency's (NSA) data mining programs outside the United States (e.g. PRISM).

1.1 Timeline

Starting in June of 2013 the Guardian published a series of articles based on files collected by Edward Snowden while working at the NSA as an employee of Booz Allen Hamilton.

One of the articles dated June 6, 2013, revealed that the NSA, based on an order by Judge Roger Vinson of the United States Foreign Intelligence Surveillance Court (FISC) Washington, D.C., was collecting telephone metadata of US-citizens.

The following day on June 6, 2013, Larry Klayman, filed a complaint against President Barack Obama, Attorney General Eric H. Holder Jr., the Director of the NSA Keith B. Alexander, the Chief Executive Officer of Verizon Communications Lowell C. McAdam, and Judge Roger Vinson, citing inter alia a violation of his Constitutional rights, his reasonable expectation of privacy, free speech and due process (First, Fourth and Fifth Amendment violation)[1].

On June 11, 2013, the American Civil Liberties Union (ACLU), the American Civil Liberties Union Foundation, the New York Civil Liberties Union, and the New York Civil Liberties Union Foundation filed a complaint against the Director of National Intelligence (DNI) James R. Clapper, the Director of the NSA Keith B. Alexander, the Secretary of Defense Charles T. Hagel, the Attorney General Eric H. Holder and the Director of the Federal Bureau of Investigation (FBI) Robert S. Mueller III to obtain "*a declaration that the Mass Call Tracking is unlawful*" (violation of First and Fourth Amendment) and exceeding the authority granted section 215 of the USA PATRIOT Act (codified as 50 U.S.C. § 1861)[2], thus violating 5 U.S.C. § 706[3].

Following the public attention, on July 31, 2013, the Office of the Director of National

[1] *Klayman v. Obama et al. - Complaint.* 13-cv-0851 (United States District Court for the District of Columbia, June 6, 2013)
[2] throughout this thesis both designations are synonymously used depending on the original source
[3] *ACLU et al. v. Clapper et al. - Complaint.* 13-cv-3994 (United States District Court for the Southern District of New York, June 11, 2013)

Intelligence declassified[4] and released the primary order for business records collection under section 215 of the USA PATRIOT Act as well as the 2009[5] and 2011[6] report on the NSA's bulk collection program for USA PATRIOT Act Reauthorization.

On December 16, 2013, the memorandum opinion in Klayman et al. v. Obama et al. granted plaintiffs' request for an injunction, stating that they "*have standing to challenge the constitutionality of the government's bulk collection and querying of phone record metadata*"[7], while the memorandum and order in ACLU et al. v. James R. Clapper et al. dated December 27, 2013, considered "*the NSA's bulk telephony metadata collection program [to be] lawful*"[8].

2. Legislative Background

2.1 United States Constitution

2.1.1 The First Amendment – Freedom of Religion, Press, Expression

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[9]

2.1.2 The Fourth Amendment – Search and Seizure

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.[8]

[4] Department of Justice - Director of Public Affairs. *Office of the Director of National Intelligence.* July 31, 2013. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/908-dni-clapper-declassifies-and-releases-telephone-metadata-collection-documents (accessed July 7, 2014)
[5] Department of Justice - Office of Legislative Affairs. *Office of the Director of National Intelligence.* July 31, 2013. http://www.dni.gov/files/documents/2009_CoverLetter_Report_Collection.pdf (accessed July 28, 2014)
[6] Department of Justice - Office of Legislative Affairs. *Office of the Director of National Intelligence.* July 31, 2013. http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf (accessed July 28, 2014)
[7] Klayman et al. v. Obama et al. - Memorandum Opinion. 13-civ-0851, 13-civ-0881 (December 16, 2013).
[8] ACLU et al. v. James R. Clapper et al. - Memorandum & Order. 13-civ-3994 (United States District Court Southern District of New York, December 27, 2013).
[9] The Declaration of Independence and The Constitution of the United States (Bantam Classic) [Kindle Edition] 2008

2.1.3 The Fifth Amendment – Trial and punishment, Compensation for Takings

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.[8]

2.2 US Code[10]

2.2.1 USA PATRIOT Act

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Public Law 107-56, 107th Congress – October 26, 2001, was signed into law by President George W. Bush.

2.2.1.1 50 U.S.C. § 1861(c)(1)

(c) Ex parte[11] judicial order of approval

(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b), the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) be followed.

2.2.1.2 50 U.S.C. § 1861(c)(2)(D)

(2) An order under this subsection–

.....

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum[12] issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things; and

---

[10] all U.S.C. stipulations: Office of the Law Revision Counsel, www.uscode.house.gov

[11] "*An ex parte judicial proceeding is one brought for the benefit of one party only, without notice to or challenge by an adverse party*" (Gifis, Steven H. Law Dictionary. 6th edition. New York: Barron's Educational Series, Inc., 2010 – p 199)

[12] "*An order issued by a court at the request of one of the parties to a suit requiring a witness to bring to court or to a deposition any relevant document that are under the witness's control*" (Gifis, Steven H. Law Dictionary. 6th edition. New York: Barron's Educational Series, Inc., 2010 – p 523)

....

2.2.1.3 5 U.S. C. § 706

Scope of review

To the extent necessary to decision and when presented, the reviewing court shall decide all relevant questions of law, interpret constitutional and statutory provisions, and determine the meaning or applicability of the terms of an agency action. The reviewing court shall-

(1) compel agency action unlawfully withheld or unreasonably delayed; and

(2) hold unlawful and set aside agency action, findings, and conclusions found to be-

(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

(B) contrary to constitutional right, power, privilege, or immunity;

(C) in excess of statutory jurisdiction, authority, or limitations, or short of statutory right;

(D) without observance of procedure required by law;

(E) unsupported by substantial evidence in a case subject to sections 556 and 557 of this title or otherwise reviewed on the record of an agency hearing provided by statute; or

(F) unwarranted by the facts to the extent that the facts are subject to trial de novo by the reviewing court.

In making the foregoing determinations, the court shall review the whole record or those parts of it cited by a party, and due account shall be taken of the rule of prejudicial error.

2.2.2 Stored Communications Act

The Stored Communications Act (Pub.L. 99-508), as Title II part of the Electronic Communications Act, was signed into law by President Regan in 1986. It is codified in Title 18 of the U.S. Code.

2.2.2.1 18 U.S.C. § 2702(a)(1) and (a)(2)[13]

§2702. Voluntary disclosure of customer communications or records[14]

[13] Electronic Storage Privacy Act, Title II Stored Wire and Electronic Communications and Transactional Records Access, Public Law 99- 508, 99th Congress – Oct.21, 1986,

(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

…..

2.2.3 Foreign Intelligence Surveillance Act of 1978 (FISA)

In 1979 President Carter signed the Foreign Intelligence Surveillance Act of 1978 into law to "*authorize electronic surveillance to obtain foreign intelligence information*".[15] The scope of and the procedures necessary to authorize the surveillance are laid down in Section 102 of the FISA. It was amended in 2008.

2.2.3.1 50 U.S.C. § 1881a

§1881a. Procedures for targeting certain persons outside the United States other than United States persons

(a) Authorization

Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence

[14] Title 18 – Crimes and Criminal Procedure, Chapter 121 – Stored Wire and Electronic Communications and transactional records access

[15] Foreign Intelligence Surveillance Act of 1978, Public Law 95-511, 95th Congress – October 25, 1978

information.

(b) .....

(h) Directives and judicial review of directives

(1) Authority

With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to-

(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) .....

3. The FISC Court Order

3.1 General Information

The process to obtain a FISC court order for the production of "any tangible things"[16] is detailed in the declaration of Robert J. Holley, the Assistant Director of the Counterterrorism Division of the FBI[17], filed in the ACLU lawsuit and introduced as Exhibit D in Government Defendants' Opposition to Plaintiffs' Motion for Preliminary Injunction in Klayman et al. v. Obama et al.:

After considering the FBI's application and an occasional hearing, where additional proof is presented in oral arguments, the court issues a "primary order". This order details the court's reasoning for authorizing the proposed collection of this data, and sets the date on which the order expires. As a general rule, when a collection of telephony metadata is sought, the primary order will specifically prohibit the collection of infor-

[16] business records such as the telephony metadata discussed here, but also books, records, papers, documents etc.

[17] *ACLU et al. v. Clapper et al. - Declaration of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation.* 13-cv-3994 (United States District Court for the Southern District of New York, October 1, 2013)

mation that can identify the caller or subscriber (name, address, financial information), and the content of the call.

The "secondary order" is directed at the respective service providers listed in the "primary order" to generate the data as specified in the "primary order".

The court order dated April 25, 2013, that triggered the actions discussed here was originally classified Top Secret/SI/NOFORN[18]. It is one of the documents leaked by Edward Snowden, published by „The Guardian" on June 6, 2013, and was still available on the Guardian's Website on September 23, 2013. On July 31, 2013, a primary order also issued on April 25, 2013, was declassified and published by the Office of the Director of National Intelligence (ODNI) on the office's web site, with several parts of the text redacted. As for the purpose of this thesis, only documents that were declassified and made available to the general public by the appropriate U.S. authorities are being used, all quotes and findings refer to this declassified primary order.

3.2 The legal basis

The court found the application of the FBI to be compliant with the conditions laid down in 50 U.S.C § 1861(c)(1) and (2)(D), in particular, that "*there are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States*"[19]. Other requirements for granting the order were that the data collected could have been obtained with a "*subpoena duces tecum*", and that the applicant would enumerate "*the minimization procedures the government proposes to follow*"[20].

3.3 The Order

According to the order the respondent had to produce electronic copies of call detail records (telephony metadata). The court specified, "*for purposes of this Order "teleph-*

[18] SI – Special Intelligence (Sensitive Compartmented Information [SCI] Control System Marking), NOFORN – No Foreign National; for more information on US Classification see „Under Secretary of Defense for Intelligence. "Manual - DoD Information Security programm: Marking of Classified Information." Defense Technical Information Center. February 24, 2012. http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf"

[19] *In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Primary Order.* BR 13-80 (U.S. Foreign Intelligence Surveillance Court, April 25, 2013) – p 2

[20] Foreign Intelligence Surveillance Act of 1978, Public Law 95-511, 95th Congress – October 25, 1978

ony metadata" includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI[21]) number, International Mobile Station Equipment Identity (IMEI[22]) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer"[23]. The metadata should be made available to the NSA on a daily basis.

The order imposed the obligation that the FBI should follow the Attorney General's "Guidelines for Domestic FBI Operations"[24], and laid down minimization procedures for the NSA. These minimization procedures refer to the purpose of the collection, the nature of the storage, the way of processing the data, limited access to the data, and training of personnel. In addition, the order comprised detailed rules on how to query the metadata, with whom results may be shared, who is responsible for approval of selection terms, and under which circumstances this approval can be granted.[25] A time limit for the effectiveness of selection terms is set with "*one hundred eighty days for any selection term reasonably believed to be used by a U.S. person and one year for all other selection terms*"[26]. The order also specified procedures and restrictions for the handling and dissemination of the collected metadata, and ordered all data to be destroyed no later than five years (60 months) after the initial collection[27]. The court also established monitoring and oversight of the training of the involved personnel, "*the implementation and use of the software and other controls*", and obligated the NSA's Office of General Counsel to "*consult with NSD/DoJ* [National Security Department of the Department of Justice] *on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority*"[28], and to assess, inter alia, if the NSA acted in compliance with the order at least once during the 12 weeks it was valid (April 25 – July 19, 2013).

---

[21] the IMSI is a unique number attributed to a user of a mobile network for identification purposes
[22] the IMEI is a unique number attributed to a mobile device for identification purposes
[23] *In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Primary Order* – p 3, n.1
[24] for further information on the Attorney General's Guidelines for Domestic FBI Operations see http://www.justice.gov/ag/readingroom/guidelines.pdf
[25] *In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Primary Order* – p 5–8
[26] Ibidem – p 10
[27] Ibidem – p 14
[28] Ibidem – p 15

4. The Guardian Article

On June 6, 2013, the Guardian published an article with the headline: "NSA collecting phone records of millions of Verizon customers daily". On the Guardian's webpage http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order there is a link to the Top Secret court order. All plaintiffs had therefore access to the complete order that probably was displayed in full[29].

5. The Complaints

5.1 Klayman v. Obama et al. – Complaint

The initial complaint submitted on June 6, 2013, to the United States District Court for the District of Columbia claims that the court order, directing inter alia Verizon, the plaintiff's telephone company, to provide call detail records[30] on a daily basis, violates the plaintiffs constitutional rights as the telephone metadata "*are being collected indiscriminately and in bulk – regardless of whether they* [the affected U.S. citizens/persons] *are suspected of any wrongdoing*"[31].

Citing Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics[32] the Plaintiff argues

- a violation of the right of freedom of speech and association (First Amendment) by "*significantly minimizing and chilling Plaintiff's freedom of expression and association" by "instilling […] the fear that [their] personal and business conversations with U.S. citizens and foreigners are in effect tapped and illegally surveilled*"[33]
- an unreasonable search of the plaintiff's phone records without "*describing with particularity the place to be searched or the person or things to be seized*" and without stating "*with any particularity who and what may be searched*"[34] (Fourth Amendment)
- a violation of the plaintiff's "*liberty interest in his personal security and* [in] *be-*

[29] the link on the website was only used to check, if the court order would have been available online but the document itself was not accessed, supra chapter 3.1, p 15
[30] this comprised inter alia information on the originating and terminating telephone number, the International Mobile Subscriber Identity Number (IMSI), the International Mobile Station Equipment Identity Number (IMEI), as well as the time and duration of the call – supra p 16
[31] *Klayman v. Obama et al. – Complaint* – p 5
[32] Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics Agents - 403 U.S. 388 (1971)
[33] *Klayman v. Obama et al. – Complaint* – p 7
[34] Ibidem – p 9

ing free from the government's use of unnecessary and excessive force or intrusion against his person", as well as his "*liberty of not being deprived of life without due process of law*"[35] (Fifth Amendment).

5.2 Klayman et al v. Obama et al. – Amended Complaint

On June 10, 2013, the complaint was amended[36]. Two plaintiffs[37] were added, and the claims were brought on not only on the plaintiff's behalf, but also as a nationwide class action.[38]

The original five claims were only slightly changed: The allegation that the phone records would allow to build "*easily and indiscriminately a comprehensive picture and profile of any individual contacted, how and when, and possibly from where, retrospectively"*[39] was extended by adding "*and into the future*"[40]. And while on June 6 the Plaintiff claimed that "*Defendants Obama, Holder, Alexander, and Vinson's acts "chill speech*…[41]", in the amended complaint it is maintained that the defendants acts "*chill, if not "kill,*" speech.[42] In addition, in a sixth claim for relief the plaintiffs maintain a violation of 18 U.S.C §§2702(a)(1) and/or (a)(2)[43] by Verizon and it's CEO, as providers of an electronic communication service, and providers of remote computing service to the public, by "*knowingly or intentionally [divulging] to one or more persons or entities the contents of Plaintiffs' and Class members' records*"[44], and by not notifying the data subjects. In a seventh claim the plaintiffs are citing 18 U.S.C. § 2702(a)(1) and/or (a)(2), but argue a violation of 18 U.S.C. § 2702 (a)(3)[45] by the defendants Verizon and McAdam.

[35] *Klayman v. Obama et al. - Complaint* – p 5
[36] *Klayman et al. v. Obama et al. - Class Action Amended Complaint.* 13-civ-0851 (United States District Court for the District of Columbia, June 10, 2013)
[37] Charles and Mary Ann Strange
[38] *Klayman et al. v. Obama et al. - Class Action Amended Complaint* – p 38 „*All American citizens in the United States and overseas who are current subscribers or customers of Defendant Verizon's telephone services at any material time, including but not limited to, April 25, 2013 to July 19, 2013"*
[39] *Klayman v. Obama et al. - Complaint* – p 9
[40] *Klayman et al. v. Obama et al. - Class Action Amended Complaint* – p 17
[41] *Klayman v. Obama et al. - Complaint* – p 7
[42] *Klayman et al. v. Obama et al. - Class Action Amended Complaint* – p 15
[43] Ibidem – p 20
[44] Ibidem – p 21
[45] 18 U.S.C. § 2702 (a)(1) and (a)(2) prohibit the divulging of contents of a communication – (a)(3) prohibits the divulging of records or other information

5.3 ACLU et al. v. Clapper et al.

On June 11, 2013, the American Civil Liberties Union[46] filed a complaint against the Director of National Intelligence, James R. Clapper, Keith B. Alexander, the Director of the National Security Agency, the Secretary of Defense Charles T. Hagel, the Attorney General Eric H. Holder and the Director of the FBI, Robert S. Mueller III. with the United States District Court Southern District of New York[47].

At the time the complaint was filed all plaintiffs were or have been[48] customers of Verizon Business Network Services Inc. and/or Verizon Wireless, and therefore claimed to be affected by the court order. The plaintiffs assert that although section 215 of the USA PATRIOT Act broadens the authority for the collection of business records, originally aimed at records of hotels or car rentals etc., and lowered the requirements to be met by the FBI to obtain a court order, the current metadata collection is not covered by this provision and therefore violates 5 U.S.C. § 706. As the majority of the clients of the plaintiffs and their contacts in government, agencies, and Congress communicate with the ACLU on the condition of anonymity, the complaint states that the mere fact of the communication is sensitive and privileged[49]. According to the ACLU, the knowledge that the information on who contacted them electronically or by telephone is now available to the government will deter potential clients from contacting the them, and discourage these contacts to talk to and work with the ACLU. The collection of metadata consequently also violates the First and the Fourth Amendment.

The ACLU action's documents[50] include declarations and *Amici* Briefs in favor of the ACLU[51]. The plaintiffs asked Prof. Edward Felten, Professor of Computer Science and Public Affairs and Director of the Center for Information Technology Policy at Princeton University, to explain the sensitive nature of metadata, and while Prof. Felten's statement is very valid, the sensitivity of the data is not in question here. If the legislature as well as the government and the judiciary oversight were not well aware of the

[46] together with the American Civil Liberties Union Foundation, the New York Civil Liberties Union and New York Civil Liberties Union Foundation
[47] *ACLU et al. v. Clapper et al. - Complaint.* 13-cv-3994 (United States District Court for the Southern District of New York, June 11, 2013)
[48] the contracts of NYCLU and NYCLUF expired in April
[49] *ACLU et al. v. Clapper et al. - Complaint* – p 6
[50] all ACLU Legal Documents including the declaration of Prof. Dr. Felten can be found on the ACLU webpage https://www.aclu.org/national-security/aclu-v-clapper-legal-documents
[51] Additional declarations than the ones mentioned in the text were submitted by Michael German, Senior Policy Counsel on National Security Immigration and Privacy; Steven R. Shapiro, Legal Director of the ACLU; the reporters committee for freedom of the press and 18 news media organization; the National Rifle Association of America, Inc.; Prof. Michael P. Lynch, Professor of Philosophy, University of Connecticut; and Pen America Center

potentially sensitive nature of the data, not that much length would have been invested in minimization procedures and oversight. What might be of relevance though is the supplemental declaration of Prof. Felten, in which he disagrees with the government's assertion that without a comprehensive historic database of all metadata a three-hop[52] analysis would not be feasible.

An *Amicus Curiae* brief[53] by Gary Hart and Walter Mondale as former members of the Church Committee (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities), and 29 Law professors[54] was submitted on August 30, 2013. Most of the document is dedicated to detail the history of the FISA and the FISC and the framework in which it operates. The brief is intended to demonstrate that the program at issue here "*contradicts FISA's purpose and design*", and quite contrary to the argument of Judge Eagan in her "Amended Memorandum Opinion"[55] also Congress's intent.

5.4 Analysis

5.4.1 General Remarks

The complaint in Klayman v. Obama et al. was written within 24 hours of the publication of the article disclosing the metadata collection program. It is exclusively based on alleged violation of constitutional rights. The provision on which the order was based (50 U.S.C. § 1861) is not addressed even once throughout the document. And while both complaining parties, Klayman and the ACLU, agree on a violation of the First and the Fourth Amendment, only plaintiff Klayman argues a violation of the Fifth Amendment.

The due process clause in the Fifth Amendment not only limits the power of the Federal Government, but also obliges to certain standards in law making, as an interference in constitutionally guaranteed civil liberties covered by law may still violate due process. This interpretation of the Fifth Amendment dates back to Murray's Lessee v. Hoboken Land & Improvement Co., 59 U.S. (18 How.) 272 (1856) and its reading has been developed ever since.

---

[52] infra p 48

[53] *ACLU et al. v. James R. Clapper et al. - Brief of former members of the Church Committee and Law Professors as Amicus Curiae supporting Plaintiff*. 12-cv-03994 (United States District Court for the Southern District of New York, August 30, 2013)

[54] a list of the professors is included as Annex 3

[55] *In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Amended Memorandum Opinion.* BR 13-109 (U.S. Foreign Intelligence Surveillance Court, August 29, 2013) – infra p 45

According to Allen Ides and Christopher N. May in Constitutional Law - Individual Rights, citing Wolff v. McDonnell, 418 U.S. 539, 558 (1974), the principle goal of the Fifth Amendment's due process clause "*is protection of the individual against arbitrary action of government*", and citing Country of Sacramento v. Lewis, 523 U.S. 833, 846 (1998), "*only the most egregious official conduct can be said to be arbitrary in the constitutional sense*[56]" – exactly what the complaint insinuates.

As opposed to procedural due process which is "*concerned with the procedures employed in enforcing a law*", substantive due process "*insists that the law itself be fair and reasonable and have an adequate justification regardless of how fair or elaborate the procedures might be for implementing it*."[57] A claim of a violation of the Fifth Amendment requires a court to review the law with "strict scrutiny" in case a fundamental liberty interest is infringed"[58]. If only economic liberties are concerned courts use the "rational basis test", in which it is sufficient that the intention of the challenged law is to further a legitimate goal[59]. In consideration of the fact that in both complaints only infringements of liberties enumerated in the Amendments of the Constitution are asserted no further consideration is given to the rational basis test.[60]

Looking at these asserted infringements one argument in particular attracts attention. In Paragraph 51 the plaintiff argues that he "*enjoys a liberty of not being deprived of life without due process of law*".

This begs the question whether "loss of life" can be argued in a figurative sense, or if "loss of liberty" would be the better argument? This is a tough question to answer, as the Congressional Research Service (CRS) in "The Constitution of the United States of America – Analysis and Interpretation[61]" does not address the issue of deprivation of life. And it's obviously for a reason that the last chapter on substantive due process in "Constitutional Law – Individual Rights" is called "What happened to life?". According to Ides and May "*there have been almost no cases in which the Court has considered the application of substantive due process to governmental conduct that impairs a per-*

[56] internal quotation marks omitted
[57] both quotes from Ides, Allen, and Christopher N. May. *Constitutional Law - Individual Rights.* 6th Edition. New York: Wolters Kluwer Law & Business, 2013 – p 58
[58] Ibidem – p 60
[59] Ibidem – p 68
[60] for further information on Due Process and economic and noneconomic as well as enumerated an unenumerated liberties, and the "Basic Fundamental Rights Model" see Ides, Allen, and Christopher N. May. *Constitutional Law - Individual Rights* – pp 61-86
[61] Congressional Research Service. *The Constitution of the United States of America - Analysis and Interpretation.* Washington, DC: US Government Printing Office, 2013 "

son's fundamental interest in life"[62]. Given that this includes such controversial issues as abortion and the death penalty this is more than surprising. Also doctrine and cases on subsistence benefits available for the purpose of this thesis do not support the idea of claiming deprivation of life. Ides and May, citing DeShaney v. Winnebago County Dept. of Social Servs., 489 U.S. at 196, conclude that "*Governmental decisions denying, terminating, or reducing these benefits do not impinge on (and thus do not trigger) the constitutional interest in life, no matter how severe their actual impact on a person's life"*[63].

To close the analysis of the due process argument, it must be mentioned that in addition to a substantive due process claim plaintiffs could have a procedural due process argument as well. Procedural due process seeks "*to ensure abstract fair play to the individual*" by "*forcing the government to use a "fair process of decisionmaking" when it implements a law"*.[64] This fair process usually implies that the person is entitled to receive a notice prior to the government action infringing liberty or property interests, and that the person has the opportunity to argue his or her case.

But a closer look at the cases presented by the Congressional Research Service in the "Constitution Annotated"[65] seems to indicate that a judicial review of an administrative act is often seen as satisfying the due process requirement of a hearing. A particularly interesting case can be found on page 1539, as the argument factors in several elements that are also subject matter in the process in question here – a judicial review and exceptional circumstances[66]. In analyzing "Administrative Proceedings" and the necessity of a fair hearing, the Congressional Research Service cites Bowles v. Willingham, 321 Z.S. 503, 521 (1944) where "*the court sustained orders fixing maximum rents issued without a hearing at any stage, saying where Congress has provided for judicial review after the regulations or orders have been made effective it has done all that due process under the war emergency requires"*[67].

Not much information can be found in the "Constitution Annotated" on the aspect of

[62] Ides, Allen, and Christopher N. May. *Constitutional Law - Individual Rights* – p 129
[63] Ibidem – p 129
[64] Ibidem – p 175
[65] Congressional Research Service. *The Constitution of the United States of America - Analysis and Interpretation* – p 1539
[66] the orders obviously have been made effective during world war II. The government would most likely argue, that the need of fighting terrorism has put the country in an exceptional situation that needs exceptional measures
[67] Congressional Research Service. *The Constitution of the United States of America Analysis and Interpretation* – p 1539

prior notice. According to the CRS, due process "*must be held to guarantee not particular forms of procedures, but the very substance of individual rights of life, liberty, and property*", and "*the phrase "due process of law" does not necessarily imply a proceeding in a court or a plenary suit and trial by jury in every case where personal or property rights are involved. In all cases, that kind of procedure is due process of law, which is suitable and proper to the nature of the case, and sanctioned by the established customs, and usages of the courts. What is unfair in one situation may be fair in another*"[68]. And also Ides and May elaborate on the content, but not on the necessity of a notice.

Given the requirements laid out in 50 U.S.C § 1861 and the detailed process specified in the court order, and be it that the court decides to uphold the stipulation, one question of law in the opinion will probably be whether the measures taken satisfy due process with respect to prior notice and hearing.[69]

In his second claim for relief at paragraph 56 of the amended complaint[70], Klayman argues a violation of the First Amendment, maintaining defendants "*abridged and violated Plaintiffs' and Class members' First Amendment right of freedom of speech and association by significantly minimizing and chilling Plaintiffs' and Class members' freedom of expression and association*".

The Constitutional right of freedom of speech has been interpreted in numerous Supreme Court cases. Still the Congressional Research Service, citing T. Emerson "The System of Freedom of Expression", indicates that the meaning and scope of the liberty guaranteed has yet to be comprehensively adjudicated[71].

But that probably will not happen anytime soon. New forms of "speech" have developed in the past and continue to develop in the age of the Internet and Social Media, posing the question if they are entitled to the protection guaranteed by the First Amendment.

In June 1994, the Supreme Court held the U.S. Court of Appeals for the Eighth Circuit's

---

[68] Congressional Research Service. *The Constitution of the United States of America - Analysis and Interpretation* – p 1538 (quotations marks partly omitted, footnote reference omitted – Footnotes refer to Hurtado c. California, 110 U.S. 532, 535, 537 (1884); Ex parte Wall, 107 U.S. 265, 289 (1883); and compare Murray's Lessee v. Hoboken Land & Improvement Co., 59 U.S. (18 How.) 272 (1856) to Ng Fung Ho v. White, 259 U.S. 276 (1922))

[69] see Ides, Allen, and Christopher N. May. *Constitutional Law - Individual Rights* – pp 175

[70] *Klayman et al. v. Obama et al. - Class Action Amended Complaint* – p 15

[71] Congressional Research Service. *The Constitution of the United States of America - Analysis and Interpretation* – p 1134; Quotation (n. 389): "T. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 15 (1970). The practice in the Court is largely to itemize all the possible values the First Amendment has been said to protect. See, e.g., Consolidated Edison Co. v. PSC, 447 U.S. 530, 534–35 (1980); First Nati'l Bank of Boston v. Bellotti, 435 U.S. 765, 776–77 (1978)"

Opinion that an ordinance by the City of Ladue, banning residential signs, violated the Ladue resident's right to free speech: "*Although Ladue has a concededly valid interest in minimizing visual clutter, it has almost completely foreclosed an important and distinct medium of expression to political, religious, or personal messages. Prohibitions foreclosing entire media may be completely free of content or viewpoint discrimination, but such measures can suppress too much speech by eliminating a common means of speaking*."[72].

In Reno v. ACLU, 521 U.S. 844 (1997) SCOTUS found, that "[t]*hrough the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, the content on the Internet is as diverse as human thought*"[73]. And the court established "*We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium*."

And while in April 2012 the District Court for the Eastern District of Virginia in Bland et al. v. Roberts concluded "*that merely liking a Facebook page is insufficient speech to merit constitutional protection*"[74], the U.S. Court of Appeals for the Fourth Circuit saw it quite differently. Basing its conclusions inter alia on an *Amicus* Brief by Facebook the Court stated, "*Once one understands the nature of what Carter* [one of the plaintiffs] *did by liking the Campaign Page, it becomes apparent that his conduct qualifies as speech*."[75].

A challenging legal argument therefore will probably be, whether the collection of metadata and its analysis, even with the minimization procedures in place, actually impairs the free speech of an individual and significantly minimizes the freedom of expression.[76]

In the third claim of relief plaintiffs argue the collection of the telephony metadata constitutes an unreasonable search and seizure, without reasonable suspicion or probable cause, and that the court order did not meet the Fourth Amendment's requirement of describing with particularity the place to be searched, or the person or things to be seized.

[72] City of Ladue v. Gilleo, 512 U.S. 43 (1994)
[73] internal quotation marks omitted
[74] Bland et al. v. Roberts Case 4:11-cv-00045-RAJ-TEM p 6
[75] Bland et al v. Roberts US Court of Appeals fort he Fourth Circuit No 12-1671
[76] *Klayman et al. v. Obama et al. - Class Action Amended Complaint* – p 15, para 56

When plaintiffs argue an unreasonable search and seizure, no reasonable suspicion, and no probable cause, they touch on a dispute as old as the Fourth Amendment: are there any "reasonable" searches that do not have to fulfill the need for a warrant based on probable cause?

The SCOTUS's view on this question has not been consistent. The CRS[77] cites several opinions and the court's findings fluctuate from: the question is not "*whether it is reasonable to procure a search warrant, but whether the search was reasonable*", and that whether a search is reasonable "*must find resolution in the facts and circumstances of each case*", to: "*the requirement that no Warrants shall issue, but upon probable cause, plays a crucial part"*[78]*,* and "*the police must, whenever practicable, obtain advance judicial approval of searches and seizures through a warrant procedure*".

Still over the years the court obviously established multiple exceptions to the need for a warrant to be within the limits of the Fourth Amendment. The CRS alleges, "*the most important category of exception is that of administrative searches justified by special needs beyond the normal need for law enforcement*"[79]. Apparently the court decided in favor of warrantless searches if they were reasonable and the government had prevailing interests. And Solove and Schwartz in "Information Privacy Law"[80] cite several Supreme Court cases where the court had accepted warrantless searches and seizures[81].

Furthermore the authors address the subject of individualized suspicion, as this qualification can be outweighed by public interest as well.

Very interesting in this context is the court's approach to new technology and telecommunication. While discussing the evolving privacy aspect of the Fourth Amendment the CRS states the following:

"*In the context of norms for the use of rapidly evolving communications devices, the Court was reluctant to consider "the whole concept of privacy expectations" at all, preferring other decisional grounds: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society*

[77] all quotes in this paragraph: Congressional Research Service. *The Constitution of the United States of America - Analysis and Interpretation* – pp 1366-1367; opinions cited by the CRS: United States v. Rabinowitz, 339 U.S. 56, 66 (1950); Chimel c. California, 395 U.S. 752, 761 (1969); and Terry v. Ohio, 392 U.S. 1, 20 (1968)
[78] internal quotation marks omitted
[79] Congressional Research Service. *The Constitution of the United States of America - Analysis and Interpretation* – pp 1368
[80] Solove, Daniel J., and Paul M. Schwartz. *Information Privacy Law* . New York: Wolters Kluwer Law & Business, 2011 – pp 251
[81] inter alia Griffin v. Wisconsin, 483 US. 868 (1987); O'Conner v. Ortega, 480 U.S. 709 (1987)

has become clear"[82].

The CRS draws the conclusion, that over time a standard has emerged requiring *"an assessing of the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement*"[83].

With regard to probable cause, the CRS explains that though being a central issue the term itself is not defined by statutory provisions, but only by judicial interpretation. A relevant aspect of probable cause could be an eventual First Amendment implication, as, according to the CRS, SCOTUS usually requires higher standards with regard to probable cause and particularity if the First Amendment protects the subject of the search or seizure.

The Supreme Court's evolving opinion on seizure for mere evidence could also be relevant. While in Gouled v. United States 255 U.S. 298, (1921) the court repudiated such a seizure, the CRS now considers it "*settled that such evidentiary items as fingerprints, blood, urine samples, fingernail and skin scrapings, voice and handwriting exemplars, conversations, and other demonstrative evidence may be obtained trough the warrant process or without a warrant where "special needs" of government are shown*"[84]. And though there are limits to what can be searched and seized without infringing personal liberties and private property, in Andresen v. Maryland, 427 U.S. 463 (1976) "*the court observed that, although some innocuous documents would have to be examined to ascertain which papers were to be seized, authorities, just as with electronic "seizures" of telephone conversations, must take care to assure that* [searches] *are conducted in a manner that minimizes unwarranted intrusions of privacy*"[85].

The sixth and seventh claims of relief in the amended complaint are based on 18 U.S.C. § 2702 (a) (1) and/or (a)(2), although the seventh claim argues a violation of (a)(3).

Already the title of the section, "voluntary disclosure of customer communications or records", raises the question why this section was specified as a basis of the complaint. There can be no doubt that Verizon did not voluntarily disclose the customer records, but rather was obligated by a court order not only to do so, but also not to divulge the

[82] Congressional Research Service. *The Constitution of the United States of America Analysis and Interpretation.* pp 1373, quotation from City of Ontario v. Quon, 560 U.S.
[83] ibidem
[84] ibidem pp 1392-1393 (internal quotations omitted)
[85] ibidem pp 1394-1395 (internal quotations omitted)

disclosure.

Also a look at the text of the sections gives cause to concern[86]:

§ 2702(a)(1) states, that

> *"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 § 2702(a)(2) says,

> *"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;"*

Both paragraphs address the contents of communications and nothing in the court order gives reason to believe that content of communication was handed over to the NSA. The only subsection of § 2707 that addresses customer records is subsection (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."*

A closer look at Title 18, Part I, Chapter 121 – Stored Wire and Electronic Communications and Transactional Records Access shows that 18 U.S. § 2703(c)(1) and (2), and 18 U.S. § 2703(d) could be of more relevance for the purpose of this claim. Subsections (c) and (d) state:

> *"(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-*

[86] emphasis added

(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) ....

(D) .... or

(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."*

The reason why this section was not chosen possibly is subsection (e):

> *"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."*

A claim based on a violation of 18 U.S.C. § 2703 (c) would prohibit any action against Verizon or it's CEO. But all the other claims and especially substantial due process could be based on this section with much more authority than a claim based on 18 U.S.C. § 2702.

Another section cannot go unmentioned here. 18 U.S.C. 2709 "Counterintelligence access to telephone toll and transactional records" specifies that certain records shall be provided by a wire or electronic communication service provider in case of a request be the Director of the FBI. This section is not addressed in any of the petitions, neither by Klayman, nor by the ACLU's.

When analyzing the Klayman complaints[87] also the following inaccuracies and peculiarities need to be addressed:

In paragraph 3, plaintiffs claim that "*there is nothing in the order requiring the government to destroy the records after a certain amount of time nor is there any provisions limiting who can see and hear the data*". This statement is ignoring the minimization procedures laid out by the court, inter alia procedures for access and a limitation for the duration of retention (supra 3.3, p 10-11). Also the last part of the sentence "hear the data" seems to imply recorded content of telephone conversations, as metadata cannot be "heard".

In paragraph 29, Judge Vinson is accused that he ordered not to disclose "*that the FBI or NSA has sought or obtained tangible things … in an attempt to keep his illegal acts and those of other Defendants as a secret*". This completely ignores the provisions laid out in 50 U.S.C. § 1861(c)(2)(e) and (d).

Further paragraph 41 of the complaint is noteworthy as it states, that the defendant Judge Vinson, when issuing the order, was "*acting on behalf of the federal government and therefore Defendant Obama as he is the chief executive of the federal government*".

[87] Paragraphs refer to the amended complaint as the first complaint uses almost identical arguments but is even less elaborate than the class action; all quotes from *Klayman et al. v Obama et al. - Class Action Amended Complaint*

According to the History of the Federal Judiciary on the website of the Federal Judicial Center[88], the FISC was established by Congress in 1978, and it's originally seven, now eleven Judges, drawn from different judicial circuits are designated by the Chief Justice of the United States. Their term is non-renewable and lasts a maximum of seven years[89]. Though the FISC is a "Court of Special Jurisdiction" it is still a court of the Federal Judiciary, intended to provide impartial judicial oversight for intelligence activities, thus the Executive Branch, carried out inside the USA, and not to act on behalf of the government.

In paragraph 57 plaintiff alleges that defendants' acts instill "*in Plaintiff and millions of other Americans the fear that their personal and business conversations with U.S. citizens and foreigners are in effect tapped and illegally surveilled*". This allegation is completely unfounded as on Page 3 the order specifically states that substantive content of communications as defined by 18 U.S.C. § 2510(8)[90], as well as name, address, or financial information of a subscriber or customer, may not be included in the data to be provided to the NSA.

Much of the above said is also valid for ACLU et al v. Clapper et al. Apart from not claiming a violation of the Fifth Amendment and different defendants[91], the most striking distinction to the Klayman complaints is the reference to 50 U.S.C. § 1861 and 5 U.S.C. § 706, and the thorough depiction of the development of section 215 of the USA PATRIOT Act.

For the ACLU this was not the first lawsuit brought against the USA PATRIOT Act. In 2003 the ACLU filed a complaint on behalf of six organizations, claiming a violation of the First, Fourth and Fifth Amendment. After three years, on October 27, 2006, the ACLU released a statement that it had withdrawn the lawsuit it had filed in 2003 to challenge section 215 of the USA PATRIOT Act because of improvements during the 2006 reauthorization process.[92] [93]

---

[88] an education and research agency for the federal courts created by Congress in 1967, www.fjc.gov
[89] originally seven judges, number increased by the USA PATRIOT Act of 2001 (Federal Judicial Center 1967)
[90] 18 U.S.C. § 2510(8): "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication
[91] the Klayman complaints as well as the ACLU name Keith B. Alexander, the Director of the NSA and Eric H. Holder, the Attorney General, additionally the ACLU names the Secretary of Defense Charles T. Hagel and the Director oft he FBI Robert S. Mueller III; the ACLU does not name POTUS or Verizon as defendants.
[92] https://www.aclu.org/national-security/citing-improvements-law-aclu-withdraws-section-215-case-vows-fight-individual-orde last visited July 20, 2014
[93] infra 5.4.2.1).

But this complaint was not the only concern raised against the USA PATRIOT Act. The complaint states, that "*members of Congress have been warning the public that the Executive Branch was exceeding the limits of the Patriot Act*"[94].

5.4.2 The Provisions of the USA PATRIOT Act and their appraisal in political and public debate before June 2013

Apart from the text of the USA PATRIOT Act itself, obviously several critical statements, articles, and press releases not only on section 215, but also on the government's interpretation, were available to Congress. Some, if not all of them, were also accessible to the public well before the publication of the FISA Court Order June 6, 2013.

5.4.2.1 The USA PATRIOT Act and the changes in 50 U.S.C. § 1861 as entered into law by the USA PATRIOT Improvement and Reauthorization Act of 2006

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 was introduced to the House of Representatives on October 23, 2001, by Congressman Sensenbrenner Jr., six weeks after the September 11 attacks. According to www.govtrack.us it passed the House of Representatives one day later with 357 votes in favor, with 66 Nays[95] and 9 No-Votes. It passed the Senate the day after with only Senator Feingold voting Nay, and was signed into law by President George W. Bush on October 26, 2001.

The USA PATRIOT Act not only brought changes to the Stored Communications Act, specifically 18 U.S.C. § 2702 and § 2703, but § 215 inserted the so called "Business Records Provision" into the Foreign Intelligence Surveillance Act.

Section 215 was not specifically mentioned in section 224 of the Act, so it was originally set to expire under the sunset clause on December 31, 2005, but was extended first by Public Law 109-160 on December 30, 2005, until February 3, 2006, and then till March 10, 2006. On March 9, 2006, the USA PATRIOT Improvement and Reauthorization Act of 2005, altered on the same day by the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, extended the sunset clause until December 31, 2009.

Both Acts were considered to significantly improve the impact on civil liberties by strengthening congressional oversight and allowing for a judicial review. The USA PATRIOT Improvement and Reauthorization Act of 2005 mandated inter alia an audit on

[94] ACLU et al. v. James R. Clapper et al. - *Complaint* – paragraph 21, p 5
[95] 62 Democrats, 3 Republicans, 1 Independent (for more information see https://www.govtrack.us/congress/votes/107-2001/h398)

the access to certain business records under 50 U.S.C. § 1861 (§ 106A)[96] and amended the rules and Procedures for FISA Courts (§ 109(d)).

The most important changes to 50 U.S.C. § 1861 were:[97]

- Subsection (a)(3) that limits the possibility to delegate the authority for an application of an order to produce records that could contain information that would identify a person to just one level below the Director of the FBI,
- Subsection (b)(2) that considerably broadens the substance of an application under this section,
- Subsection (c) that, though leaving the order to be "*ex parte*", added mandatory minimization procedures and several rules of procedure inter alia a certain standard of particularity,
- Subsection (d) that detailed the principles for the nondisclosure order,
- Subsection (f) that renders challenging the legality of the production order as well as the nondisclosure order possible,
- Subsection (g) that mandates the adoption of minimization procedures by the Attorney General and
- Subsection (h) that details the use of the information gathered under this section.

The CRS in "USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis"[98] shared this view. According to the authors, the government seems to have filed only few applications for a court order under 50 U.S.C. § 1861.

The paper details the implications of the Act and especially emphasizes the increased Congressional oversight facilitated by unclassified comprehensive annual reports to the Judiciary and Intelligence Committees of both House and Senate. Yeh and Doyle also appraise the enhanced requirements, that the application now must include factual information, to establish that the information requested is of relevance to investigations with the intended purpose to obtain foreign intelligence information not concerning a

[96] all sections refer to the USA PATRIOT Improvement and Reauthorization Act of 2006
[97] the changes made by the USA PATRIOT Improvement and Reauthorization Act of 2006 and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 are depicted in detail in Annex 1
[98] Yeh, Brian T., and Charles Doyle. USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis - Kindle Edition. Washington D.C.: Congressional Research Service, 2006 – p 4 n 18: „*Section 215 authority appears to have been relatively little used. In April 2005, Justice Department officials testified to the House Judiciary Committee that, as of March 31, 2005, only 35 orders have been issued under section 215 authority, non of which involved library, book store, medical, or gun sale records.*"

U.S. Person[99], or to protect against international terrorism, or clandestine intelligence activities, as an improvement. But they also state that several provisions of the Act were criticized, especially in the Senate. In particular, the absence of an express right to challenge the nondisclosure order[100], and the limitations in challenging the production order (only the legality of the order can be challenged, but neither a modification nor a dismissal can be requested), or the application requirements, were cause for concern for several Members of Congress.

Throughout the 6 pages dedicated to the business records provision, telephony or Internet metadata are not even mentioned once as types of records that could be subject to a court order under 50 U.S.C § 1861. The expression used is "tangible things" or "tangible items", specifying "*including books, records, papers, and other documents*" on page 4, and enumerating "*library circulation records, library patron lists, book sales records, or book customer lists, firearms sales records, tax return records, educational records and medical records*" as sensitive information on page 5, the request of which needs to be disclosed in the annual report. When commenting on the new Paragraph (3) of 50 U.S.C. § 1861 Yeh and Doyle state: "… *an application for a 215 order for the production of certain sensitive categories of records, such as library, bookstore, firearm sales, tax return, educational, and medical records, must be personally approved by one of the following three high-level officials: the FBI Director, the FBI Deputy Director, or the Executive Assistant Director for National Security. This provision was included as an attempt to allay concerns over federal authorities abusing section 215 authority to obtain sensitive types of records*"[101].

5.4.2.2 Information available to Congress

The first hint on the collection of telephony and Internet records can be found in a CRS paper on Data Mining[102]. According to the author, two articles in the Washington Post published on December 18, 2005, and January 1, 2006, had revealed the existence of a classified NSA terrorist surveillance program, operated by the NSA since 2002. The

[99] a U.S. Person is a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association with a substantial number of members who are citizens of the U.S. or are aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the U.S. (http://www.nsa.gov/about/faqs/oversight.shtml#oversight3)

[100] these concerns were met by the USA PATRIOT Act Additional Reauthorizing Amendments Act, granting a challenge of the nondisclosure order after one year.

[101] Yeh, Brian T., and Charles Doyle. *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis* – p 6

[102] Seifert, Jeffrey W. *Data Mining and Homeland Security: An Overview - Kindle Edition.* Washington, DC: Congressional Research Service, 2007

program, though classified, was an issue in President Bush's Radio Address on December 17, 2005. Based on this broadcast and subsequent statements by government officials, it was assumed "*that the NSA terrorist surveillance program focused only on international calls, with a specific goal of targeting the communications of al Qaeda and related terrorist groups, and affiliated individuals*"[103] – an impression that was substantiated by a January 27, 2006, statement released by the Department of Justice (DoJ).

But on page 19 and 20 of the CRS Paper, Mr. Seifert states:

> *„In May 2006 news reports alleged additional details regarding the NSA terrorist surveillance program, renewing concerns about the possible existence of inappropriately authorized domestic surveillance. According to these reports, following the September 11, 2001 attacks, the NSA contracted with AT&T, Verizon, and BellSouth to collect information about domestic telephone calls handled by these companies. The NSA, in turn, reportedly used this information to conduct "social network analysis" to map relationships between people based on their communications.*
>
> *It remains unclear precisely what information, if any, was collected and provided to the NSA. Some reports suggest that personally identifiable information (i.e., names, addresses, etc.) were not included. It also has been reported that the content of the calls (what was spoken) was not collected. Since the emergence of these news reports, BellSouth has issued a public statement saying that according to an internal review conducted by the company, "no such [alleged] contract exists" and that the company has "not provided bulk customer calling records to the NSA." Similarly, Verizon has issued a public statement saying that due to the classified nature of the NSA program, "Verizon cannot and will not confirm or deny whether it has any relationship to the classified NSA program," but that "Verizon's wireless and wireline companies did not provide to NSA customer records or call data, local or otherwise." Together, AT&T, Verizon, and BellSouth are the three largest telecommunications companies in the United States, serving more than 200 million customers, accounting for hundreds of billions of calls each year.[104]"*

The "news reports" are articles in USA Today (NSA has Massive Database of Americans' Phone Calls), The Washington Times (Bush Denies Report of "Trolling" by NSA"), and The Washington Post (Data on Phone Calls Monitored).

The issues the author suggests, "*Congress may decide to consider related to implementation and oversight*", are Data Quality, Interoperability, Mission Creep[105] and finally one paragraph on privacy – the question whether such a program could be constitutional

[103] Seifert, Jeffrey W. *Data Mining and Homeland Security: An Overview - Kindle Edition.* Washington, DC: Congressional Research Service, 2007 – p 18
[104] Ibidem – pp 19-20; internal footnotes omitted.
[105] Use for purposes other than the originally intended

was not addressed.

The First and Fourth Amendment implications were discussed in the CRS report "Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization" written in December 2009, when the sunset clauses of the USA PATRIOT Act needed reauthorization. With regard to the Fourth Amendment the authors discuss the problem of warrantless search. The most important conclusions of the paper are that the Supreme Court, in United States v. U.S. District Court, 407 U.S. 297, 31-14, 321-24 (1972), had indicated that though national security purposes do not vindicate a warrantless electronic surveillance, the Court might come to a different decision if a foreign power and/or their agents were involved, that on any account warrantless searches would be subjected to a "reasonableness test", and that "*individuals have a lesser expectation of privacy with regard to information held by third parties"*[106].

The document also addresses First Amendment implications. Apart from the obvious negative effect that a possible government intrusion might have on free speech, also concerns about the consequences of nondisclosure orders are raised.

Finally two reports, declassified by the DNI in July 2013, clearly show that Congress was well aware of the program.

Following a request by the Chairman of the House Permanent Select Committee on Intelligence, the Office of Legislative Affairs of the DoJ on December 14, 2009, submitted a document, aimed at informing not only the members of the aforementioned committee, but also all Members of Congress, about the program implemented under the business record provision of the USA PATRIOT Act, to facilitate the discussion on the extension of the sunset clause. The 5-page document was originally classified Top Secret/COMINT[107]/ NOFORN. Detailing the program, it explains the reason why it was set up, emphasizes that neither the content of telephone conversations, nor that of emails are collected, and that the government evaluates only a fraction of the data collected, as "*the information is not responsive to the limited queries that are authorized for intelligence purposes*"[108]. The document also states that not only calls to a foreign country, but also calls within the US are affected, but that the type of information collected in this program is not protected by the Fourth Amendment according to longstanding Supreme

[106] Henning, Anna C., Elisabeth B. Bazan, Charles Doyle, and Edward C. Liu. *Government Collection of Privat Information: Background and Issues Related to the USA PATRIOT Act Reauthorization - Kindle Edition.* Washington, DC: Congressional Research Service, 2009 – pp 2-3
[107] COMINT – Communications Intelligence (SCI Control System Marking – supra n.16)
[108] Department of Justice - Office of Legislative Affairs – 2009 Cover Letter – p 1

Court precedent. While it does not elaborate on the Constitutional implication some light is shed on how the collected data is used. The document is partly redacted, but it illustrates that a process has been set up, so that only telephone numbers or email addresses that raise a "reasonable articulable suspicion" can be queried, and only "*information pertaining to one of the foreign powers listed in the relevant Court Order is provided to NSA personnel for further intelligence analysis*"[109]. Concluding, the DoJ rates the program to be indispensable, as no other tool is available providing an "*equivalent capability*" to identify contacts of suspected terrorists in the US and abroad.

Obviously the extension of the sunset clause has been subject to some discussion, as it took four separate Acts to finally approve it. With approval still pending, the Office of Legislative Affairs of the U.S. Department of Justice provided another paper to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence[110], but no new information was offered. Finally, on May 26, 2011, the sunset clause for section 215 of the USA PATRIOT Act was extended without any changes to the text.

5.4.2.3 Other documents and webpages cautioning against the Interpretation of 50 U.S.C. § 1861 by the Government

- Belfer Center for Science and International Affairs – John F. Kennedy School of Government – Harvard University, The USA-PATRIOT Act, originally a Memo in the report "Confrontation or Collaboration? Congress and the Intelligence Community", Authors Eric Rosenbach and Aki J. Peritz, July 2009, with a chapter on "The "Business and Other Tangible Records" Provision"[111]
- Common Dreams, Press Release by Senator Russ Feingold, September 23, 2009, "Hearing on Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security" on the need for reforming the USA PATRIOT Act in the light of overbroad authority and misuse[112]
- ACLU – Surveillance Under the USA PATRIOT Act, December 10, 2010, stating that section 215 of the PATRIOT Act violated the First and the Fourth Amend-

[109] Department of Justice - Office of Legislative Affairs. *Office of the Director of National Intelligence.* July 31, 2013. http://www.dni.gov/files/documents/2009_CoverLetter_Report_Collection.pdf (accessed July 28, 2014) - p 4
[110] Department of Justice - Office of Legislative Affairs. *Office of the Director of National Intelligence.* July 31, 2013. http://www.dni.gov/files/documents/2009_CoverLetter_Report_Collection.pdf (accessed July 28, 2014)
[111] http://belfercenter.ksg.harvard.edu/publication/19163/usapatriot_act.html last visited July 20, 2014
[112] http://www.commondreams.org/newswire/2009/09/23-8 last visited July 20, 2014

ment[113]

- Ron Wyden Senator for Oregon Press Release of a speech in the U.S. Senate on the PATRIOT Reauthorization, May 26, 2011, on the secret interpretation of the PATRIOT Act by the US Government[114]
- ACLU – Surveillance Under the PATRIOT Act, October 24, 2011, giving information about the collection of phone and computer records and the "gag orders" that prevents recipients of orders to reveal them[115]

5.4.3 Conclusion

It is difficult to say to what extent the constitutional implications of the business record provision were raised within Congress, as not all the Congressional Research Service's documents are available on the Internet, and a lot of the discussion most likely is classified.

Still, the existence of a program like the MAINWAY database should not have come as a complete surprise, and it is astounding that somebody as fervently opposed to the Obama administration as Mr. Klayman, and an organization as diligent as the ACLU, did not find any legal means to address the subject at an earlier date.

With regard to the legal substance of the claims, without the FBI's application it is almost impossible to assess, whether the statutory requirements for a positive decision by the FISA were actually met, or whether the bulk collection of the metadata was unjustifiable.

But there are several arguments against the claims that need to be further explored. According to the court order the data requested by the FBI are comprehensive routing information, but material that could reveal the identity of a customer is expressively excluded. So without additional proceedings the identification of individuals is impossible. Also, according to the report to the House Permanent Select Committee on Intelligence, even the query for a specific number or address that raised suspicion within the stored data is subject to additional limitations and procedures.

As, according to the Attorney General's Guidelines for Domestic FBI Operations, the guidelines for the program in question here are classified, any assertion on the minimization procedures apart from what is included in the court order is mere speculation.

[113] https://www.aclu.org/national-security/surveillance-under-usa-patriot-act last visited July 20, 2014
[114] http://www.wyden.senate.gov/news/press-releases/in-speech-wyden-says-official-interpretations-of-patriot-act-must-be-made-public last visited July 20, 2014
[115] https://www.aclu.org/national-security/surveillance-under-patriot-act last visited July 20, 2014

And while there have been reported cases of employee misuse of data or non-compliance to the minimization procedures, the numerous built in safeguards should help to dissuade operatives from using the program for anything other than legitimate reasons.

All this raises the question of how the privacy of a person can be invaded, or his or her constitutional rights be infringed, as long as the identity of a person is not disclosed?

Also, all the information obtained by the NSA under this program is a copy of some of the information already stored by the communication companies for internal, mostly accounting purposes, with the significant distinction that these companies dispose of all the information necessary to identify the "owner" of a specific telephone number, device or email-address.

§ 50 U.S.C. 1861 (c)(2)(D) clearly states that, under an order based on this section, only material can be obtained that could also be obtained by a *subpoena duces tecum*. Solove and Schwartz maintain[116] that the Fifth Amendment does not protect information held by a third party. Their argument is backed by two Supreme Court decisions[117], when an attorney and an accountant were subpoenaed to produce their client's documents. And in 1979, the Supreme Court emphasized its recurring view that, as soon as information is voluntarily given to a third party, there can be no expectancy privacy with regard to that information[118], when dismissing a claim that the installation of a pen register at a telephone company would violate the Fourth Amendment[119] with a very interesting argument: "*When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. .... The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate*".

One could argue that the same argument is applicable here, as telephone and Internet users have a fairly good impression on what data the telephone/Internet company is col-

[116] Solove, Daniel J., and Paul M. Schwartz. *Information Privacy Law* – p 251
[117] ibidem Couch v. United States, 409 U.S. 322 (1973) and Fisher v. United States, 425 U.S. 391 (1976) – p 250
[118] ibidem Smith v. Maryland, 442 U.S. 735 (1979) – p 276
[119] a pen register is used to register all numbers dialed from a certain telephone connection

lecting, and have a tendency to volunteer more and more information for the benefit of the additional services modern technology offers.

It has to be mentioned though that three Judges were dissenting from the court's findings. One of the arguments was that, while people have no problem with their telephone number listed in a telephone directory, they would have a problem with public listing of their placed and received calls, mostly because this "*easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's live*"[120].

Also, Justice Marshall and Justice Brennan wrote that the use of a telephone is an unavoidable prerequisite of today's life, and privacy should only depend on the risks one "should be forced to assume in a free and open society".[121] It does not go without irony, that the judges in 1979 predicted that unlimited governmental access to phone records would be unsettling to the general public, and that "*many individuals including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts*".

Crucial is that all the arguments, in favor as well as against the third party doctrine, relate to cases where no warrant was obtained. The decisive factor, as said before, will be, if the process outlined by 50 U.S.C § 1861 is sufficient to provide the level of "*detached scrutiny by a neutral magistrate*" the Supreme Court missed in Katz v. United States[122].

6. Additional (Legal) Arguments[123]

6.1 ACLU et al. v. Clapper et al. – Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction

6.1.1 Plaintiffs' Memorandum

On August 26, 2013, the ACLU filed a "Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction"[124]. To prove that their claims are "more likely than not to succeed on the merits", and that "they are likely to suffer irreparable injury", plaintiffs maintain that the data collection, as operated by defendants, is not authorized

[120] Solove, Daniel J., and Paul M. Schwartz. *Information Privacy* – p 280 Smith v. Maryland, Justices Steward and Brennan dissenting opinion
[121] ibidem – p 280
[122] ibidem – p 265; Katz v. United States 389 U.S. 347 (1967)
[123] throughout this chapter "defendant" or "plaintiff" refers to the parties named in the Complaints, the term "respondents" is used as a synonym for "defendants"
[124] ACLU et al. v. Clapper et al. Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction. 13-cv-03994 (United States District Court Southern District of New York, August 26, 2013)

by statue, and violates plaintiffs' First and Fourth Amendment rights.

6.1.1.1 No authorization by statute

To succeed with an application for a primary order in accordance with 50 U.S.C. § 1861, the applicant agency needs to demonstrate that there are "*reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment)*". The ACLU argues, that "*the notion that detailed information about every phone call made by a resident of the United States over a seven-year period could be "relevant to an authorized investigation" finds no support in precedent or common sense*"[125]. With this plaintiffs challenge that the government's and the FISC's interpretation of relevance is covered by the statute. According to the ACLU, the statute's text compels to link the entirety of the collected data to (a) specific investigation(s) – a requirement the government cannot fulfill. And though the courts on various occasions have attributed a broad compass to the term, still they found that there are boundaries for its interpretation[126].

A very interesting citation is "In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993"[127], where the court instructed the government to use keyword searches to identify relevant documents, so that there would be no need to *subpoena* the delivery of documents irrelevant to the cause and stated that even an "*expanded investigation does not justify a subpoena which encompasses documents completely irrelevant to its scope"*[128].

Plaintiffs also try to quash the argument that, owing to the possible future relevance of the data, the bulk collection is required, as according to this interpretation of "relevance" essentially everything could become relevant at a later date, and thus subject to a retention under section 215 of the USA PATRIOT Act.

The second factor that yields exceeding statutory authorization is the approval of collecting records not in existence at the date of the issuance of the order. According to the ACLU the government itself has acknowledged that section 215 of the USA PATRIOT

[125] ACLU et al. v. Clapper et al. Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction – p 9
[126] ibidem – p 11 citing inter alia Bowman Dairy Co. v. United States, 341 U.S. 214, 221 (1951), In re Horowitz, 482 F.2d 72, (2d Cir. 1973), Cheney v. U.S. Dist. Court, 542 U.S. 367, 287-88 (2004) and In re Six Grand Jury Witnesses, 979 F.2d 939, 943 (2d Cir. 1992)
[127] ibidem – p 12
[128] ibidem – p 12 citing In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 G. Supp. 11, 12 (S.D.N.Y. 1994)

Act relates to existing records[129].

Eventually the third argument for a lack of statutory authority is, that the way the process for the issuance of a court order is designed today negates the way Congress intended it to be. From the ACLUs' point of view, the task to determine, whether data is closely connected to an investigation, should rest with the FISC, while at the moment that function has been taken over by the government.

6.1.1.2 Violation of the Fourth Amendment

The arguments for a violation of the Fourth Amendment are the same as brought forward in the complaint: the data collection constitutes a warrantless search and lacks probable cause, individualized suspicion, and reasonableness. The plaintiffs detail their assumption of how the government can use the data to aggregate detailed knowledge on every US resident ever making a telephone call, and cite an abundance of authorities to circumstantiate their arguments[130]. In an effort to counter the government's use of Smith v. Maryland[131], the ACLU cites the declaration of Prof. Felten, who argues that since the time of the decision in 1979 "*technological advances ... in computing, electronic data storage, and digital data mining ... have radically increased our ability to collect, store, and analyze personal communications, including metadata*"[132].

The authority plaintiffs rely on is United States v. Jones, 132 S. Ct. 945 (2012), where the Supreme Court found the installation of a GPS device to constitute a search. Justice Sotomayor in her concurring opinion stated "*GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future*"[133].

6.1.1.3 Violation of the First Amendment

Plaintiffs discuss the court's subjecting of surveillance tools, potentially damaging First Amendment rights, to "exacting scrutiny" with regard to being the "*least restrictive*

[129] ibidem – p 14 citing Robert Litt, the General Counsel, Office of the Director of National Intelligence at a House Judiciary Committee Hearing "*It's important to remember that 215 authority allows you to acquire existing records and documents and it's limited to that*"
[130] *ACLU et al. v. Clapper et al. Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction* – p 16-29 citing inter alia Kyllo v. United States, 533 U.S. 27, 33 (2001(, United States v. Gordon, 236 F.2d 916, 919 (2d Cir. 1956), United States v. Knotts, 460 U.S. 276, 284-85 (1983)
[131] supra 5.4.2 – p 38
[132] *ACLU et al. v. Clapper et al. Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction* – p 22
[133] ibidem – p 20 citing the concurring opinion by Justice Sotomayor in United States v. Jones

means of pursuing a compelling state interest"[134]. And while plaintiffs have no doubt that defendants' actions "*significantly burden their First Amendment rights*[135]", they are equally confident that the program "*cannot withstand exacting scrutiny*"[136].

6.1.2 Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction

On October 1, 2013, defendants in ACLU et al. v. Clapper et al. filed a "Memorandum of Law in Opposition of Plaintiffs' Motion for a Preliminary Injunction"[137]. Respondents reject the claims of plaintiffs, as they are "*based entirely on conjecture as to how the Government might misuse telephony metadata collected under the program, and consequences that might ensue*"[138]. They maintain that the claim is not supported by evidence, but rather constructed around public statements by the government taken out of context, while disregarding those parts of the statements that might be harmful to the claim.

Before responding to the legal arguments of the motion, defendants dispute plaintiffs' standing on the grounds that the asserted damages are not supported by evidence, and therefore lack substance. The government denies that the metadata collected would reveal the kind of information the ACLU's motion implies, that it is not used to collect "*a rich profile of every citizen as well as a comprehensive record of citizens' associations with one another*"[139], and they point to the fact that plaintiffs were not able to offer any evidence to support their allegations.

6.1.2.1 No exceeding of Statutory Limits

Respondents also reach the conclusion that plaintiffs failed to demonstrate that they are likely to succeed on the merits with regards to their allegation, that the program exceeds statutory authority under section 215. They emphasize that with regard to relevance, the FBI's applications were satisfactory for the FISC on 34 occasions. And, elaborating on the standard of review courts apply when enforcing grand jury or administrative subpoenas, defendants argue that "*when courts are called on to enforce grand jury or administrative subpoenas – instruments that informed Congress's understanding of Sec-*

[134] ibidem – p 30 citing Clark v. Library of Congress, 750 F.2d at 95
[135] *ACLU et al. v. Clapper et al. Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction* – p 30
[136] ibidem – p 34
[137] *ACLU et al. v. Clapper et al. - Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction.* 13-cv-3994 (United States District Court for the Southern District of New York, October 1, 2013)
[138] ibidem – p 1
[139] ibidem - p 13 citing ACLU

tion 215, ... the Government's determination that records are "relevant" to its investigation is subject only to the most deferential review"[140].

Furthermore, respondents dispute plaintiffs' allegation that the interpretation of the concept of relevance, as applied by the government, would allow for a collection of "*virtually any record on the theory that it may become relevant later*", by stating that the program gathers the metadata "*not because they may become relevant, but because reason and experience teach that they are relevant*"[141].

6.1.2.2 No violation of Fourth Amendment

Defendants reject plaintiffs' argument of a violation of the Fourth Amendment, as the program collects only numerical information, and not information that could identify the subscriber or customer. Citing Smith v. Maryland, respondents argue that a collection of metadata does not constitute a search, and that there is no reasonable expectancy of privacy with regard to telephone metadata, as this is information voluntarily disclosed to a third party[142]. Also the reasoning of plaintiffs that their expectation of privacy is reasonable and Smith not applicable is challenged. The government states that the conception of the NSA assembling "*a richly detailed profile of every person living in the United States*" is completely unfounded for the following reasons: the NSA does not receive information identifying subscribers, the NSA's access to the data is limited to queries based on authorized "*identifiers that are reasonably suspected of being associated with foreign terrorist organizations*", "*the NSA applies signals intelligence analysis to identify and alert the FBI to those communications that may be indicative of contacts between known or suspected terrorist*", and "*any subscriber-identifying information must be obtained from other sources, if necessary pursuant to other legal authorities*"[143].

Additionally defendants carve out the substantive differences between the telephone metadata collection and the GPS monitoring in United States v. Jones[144], where a GPS was mounted to the car of a person whose identity was known to the officers in charge of the surveillance.

With regard to reasonableness respondents reiterate that the metadata collection does

[140] *ACLU et al. v. Clapper et al. - Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction – p 17*
[141] ibidem – p 21 internal quotations omitted
[142] supra p 35 and infra p 55
[143] all quotes in this paragraph *ACLU et al. v. Clapper et al. - Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction – p* 27-28
[144] supra p 41

not constitute a search under the Fourth Amendment, as it is reasonable, constitutes only a minimal invasion on privacy if any, and also does not "*even involve electronic surveillance, as that term is defined by FISA*"[145].

6.1.2.3 No violation of First Amendment

In their motion for preliminary injunction plaintiffs reasoned that the "exacting scrutiny test" should be applied to the metadata collection, as it poses a "significant burden" on their First Amendment rights. Unsurprisingly, defendants feel that as "*good-faith governmental investigations conducted in observance of the Fourth Amendment, without the purpose of deterring or penalizing protected speech or association, do not violate the First Amendment*"[146], the same can be said of the bulk metadata collection. Respondents argue that plaintiffs have neither offered any evidence that their data has been reviewed, nor that the knowledge of the existence of the program had influenced their or their clients' behavior with regard to telephone calls or personal contact. And when explaining the fundamental differences between the cases, the ACLU cites in support of their legal position, and the situation in question here, defendants' arguments by and large can be summarized as follows: the metadata collection per se does not allow the identification of an individual, thus the collection does not constitute a Fourth Amendment search.

6.2 Klayman et al. v. Obama et al. – Plaintiffs' Memorandum of Points and Authorities in Support of their Motion for Preliminary Injunction

6.2.1 Plaintiffs' Memorandum

In the weeks following the claims a lot of procedural back and forth was going on in the Klayman case, partly caused by the looming government shutdown. On October 28, 2013, Mr. Klayman filed "Plaintiffs' Memorandum of Points and Authorities in Support of their Motion for Preliminary Injunction"[147]. Here, for the first time, also Mr. Klayman argues a violation of section 215 of the USA PATRIOT Act, but does not elaborate on the subject.

However he cites an "Amended Memorandum Opinion" dated August 29, 2013, signed

[145] *ACLU et al. v. Clapper et al. - Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction – p* 31
[146] ibidem – p 33
[147] *Klayman et al. v. Obama et al. - Memorandum of Points and Authorities in Support of their Motion for Preliminary Injunction.* 13-civ-0851 (United States District Court for the District of Columbia, October 28, 2013)

by Judge Eagan, where supposedly is stated that "*the Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information*"[148].

The document in question is Docket Number: BR 13-109[149]. The text cited by Klayman can be found on page 5, n.8, and not at n.9 as the motion states. It is staggering that plaintiffs cite this document[150], because the Judge's arguments why she is granting the Order, while fully aware of the controversy the program has caused, are well founded, and anything but in the Plaintiffs' favor. Inter alia

- the original footnote's full text reads: "*The Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information. Through oversight by this Court over a period of months, those issues were resolved*". Moreover, the text the footnote is attached to, expressly states, that during the last authorization period there have been no such incidents.
- on p3 of the document the court states: "*In conducting its review of the government's application, the Court considered whether the Fourth Amendment to the U.S. Constitution imposed any impediment to the government's proposed collection. Having found none in accord with U.S. Supreme Court precedent, the Court turned to Section 215 to determine if the proposed collection was lawful and that Orders requested from this Court should issue. The Court found that under the terms of Section 215 and under operation of the canons of statutory construction such orders were lawful and required, and the requested Orders were therefore issued*".
- on p4 the court specifies: "*Those telephone company business records consist of a very large volume of each company's call detail records or telephony metadata, but expressly exclude the contents of any communication; the name, address, or financial information of any subscriber or customer; or any cell site location information (CSLI)*". And a footnote explains that "*In the event that the government seeks the production of CSLI as part of the bulk production of call detail records in the future, the government would be required to provide notice and briefing to*

[148] *Klayman et al. v. Obama et al. - Memorandum of Points and Authorities in Support of their Motion for Preliminary Injunction – p 8*
[149] the declassified copy is available on http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.
[150] *In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Amended Memorandum Opinion.* BR 13-109 (U.S. Foreign Intelligence Surveillance Court, August 29, 2013)

this Court pursuant to FISC Rule 11[151]*. The production of all call detail records of all persons in the United States has never occurred under this program*".

- the amended Memorandum Opinion discusses Fourth Amendment implications and, citing Smith v. Maryland, comes to the same conclusion as drawn in 5.4.2 of this thesis, namely that the same type of data as in Smith are in question here. Also, on p 6 n.11, the court explains that it is aware of the additional data required here, but that "[o]*ther courts have had the opportunity to review whether there is a Fourth Amendment expectation of privacy in call detail records similar to the data sought in this matter and have found that there is none*".

The court also discussed the large number of persons affected by the order and came to the conclusion, as Fourth Amendment rights are "*personal and individual*", that "*where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence ex nihilo*"[152].

Also the court explains at length the difference between 18 U.S.C § 2703 and 50 U.S. C. § 1861, elaborates on the "*specific and complex statutory scheme for judicial review of an Order*", and states that up to now no recipient of an order, though entitled to do so, ever challenged the legality of such an order[153].

With regard to the question of relevance, the court acknowledges that in this context the concept is not only broad, but also "*amounts to a relatively low standard*". Unfortunately parts of the text are redacted, which makes the understanding of the reasoning a bit difficult. But the court details that "*the Section 215 provisions are designed to permit the government wide latitude to seek the information it needs….but only in combination with specific procedures for the protection of U.S. Person information that are tailored to the production and with an opportunity for the authorization to be challenged*"[154].

The most interesting argument concerns the reauthorization process in 2011. The court argues that, while in spite of the high classification level of the program and the authorization orders, Members of Congress were well aware of the nature and scope of the interpretation of section 215 (50 U.S.C. § 1861), displayed not only by the government,

[151] see Annex 3 FISC Rule 11
[152] *In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Amended Memorandum Opinion* – p 9
[153] ibidem – p16
[154] ibidem – pp 18-23

but also by the FISA, when they reauthorized the USA PATRIOT Act in 2011[155]. Therefor the court considers the SCOTUS's re-enactment doctrine that "*Congress is presumed to be aware of an administrative or judicial interpretation of a statue and to adopt that interpretation when it re-enacts a statute without change*"[156] to be applicable, and that the presumption "*that in 2011 Congress intended to ratify Section 215 as applied by this Court is well supported*".

The rest of the Klayman paper, apart from the same arguments the ACLU brought forward in their motion[157] with regard to relevance and the collection of future records, is full of citations from various news articles by more or less reputable media sources, or arguments from *Amici* Briefs taken from the ACLU lawsuit, together with allegations that Mr. Klayman is the prime target of the NSA, and rather irrational accusations of intrusive and highly secretive surveillance of Plaintiffs by the government[158]

6.2.2 Government's Opposition to Plaintiffs' Motion for Preliminary Injunctions

The government filed their Opposition[159] on November 12, 2013. It contains inter alia the FISA Memorandum Opinions dated August 29, 2013[160], as well as declarations by the Signals Intelligence Director NSA Teresa H. Shea, and the Acting Assistant Director, Counterterrorism Division of the FBI Robert J. Holley.

6.2.2.1 Defendants' Opposition – Introduction

Unsurprisingly, the defendants reject the claims on the grounds that the program itself is not infringing any of plaintiffs Constitutional Rights, as their account of the program is erroneous. Most importantly the minimization procedures, in combination with the regular revision of the used identifiers, impede the creation of comprehensive profiles of US persons.

Defendants also argue that plaintiffs have not been able to prove that their data has ever been reviewed or disseminated, nor that any of them had suffered irreparable damage.

---

[155] Supra pp 26-31
[156] *In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Amended Memorandum Opinion* – p 23
[157] *ACLU et al. v. Clapper et al. - Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction*
[158] *Klayman et al. v. Obama et al. - Memorandum of Points and Authorities in Support of their Motion for Preliminary Injunction* – p 16 „*Mary Ann Strange was on the computer when it abruptly photographed her (through some form of abusive surveillance since her computer does not have a built-in camera)...*"
[159] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction.* 13-civ-0851 (United States District Court for the District of Columbia, November 12, 2013)
[160] supra p 34-36

6.2.2.2 Defendants' Opposition – Statement of Facts

While describing the statutory background of three programs[161] plaintiffs challenge in various lawsuits, the main arguments for the legality and constitutionality of the collection of telephony metadata as pursued by the government are the judicial oversight, the judicial review, the strict minimizing procedures, the possibility to challenge the legality of a court order under 50 U.S.C. § 1861, and the fact "*that the Government may not intentionally target any person known at the time of acquisition to be located in the United States, may not intentionally target a person reasonably believed to be outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States, and may not intentionally target a United States person reasonably believed to be located outside the United States*"[162].

The brief details how the data collection is facilitated. In particular, it is argued that only data already collected by the service providers receiving an FISC order is turned over to the NSA, where the data is stored, and only in "*limited circumstances*" is subject to a query and a subsequent analysis of the results. It is pointed out that with respect to telephony metadata, only numerical information is gathered, and neither name or address, nor financial information of any party to a call is stored. It is also reiterated that the order does not allow monitoring or recording the call itself. The opposition also elaborates on the minimization procedures and on the process of accessing the data. The access is effected "*only through "contact-chaining" queries (electronic term searches) of the metadata using identifiers (typically telephone numbers) approved as "seeds" by one of twenty-two designated officials in NSA's Signals Intelligence Directorate*"[163]. A precondition for the use of an identifier is a "*reasonable, articulable suspicion that a selection term used to query the database is associated with one or more foreign terrorist organizations previously identified to and approved for targeting by the FISC*"[164]. NSA analysts will only review data responsive to such a probe, but the assessment is limited to "*records of communication within three "hops" from the seed*"[165], the first hop being the seed itself, the second hop a direct contact of the seed and the third hop a direct contact of the second hop.

---

[161] Collection of Bulk Telephony Metadata Under Section 215, Targeted Collection of Communications Content Pursuant to Section 702, Bulk Collection of Internet Metadata
[162] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 7; internal quotations omitted
[163] ibidem – p 10
[164] ibidem
[165] ibidem p 11

Defendants state that through creating a "*historical repository*", the program as it is operational to date, is the only viable possibility to identify terrorist networks also in retrospect every time "*new terrorist-associated telephone identifiers come to light*", but they strongly repudiate the idea that, through the database, "*rich comprehensive profiles of every citizen, including intimate details about their lives and personal associations*" can be accumulated.

They also acknowledge to violations of procedures as claimed by plaintiffs, leading to a suspension of the authorization to access the accumulated data in 2009, and, after resolving the problems, a subsequent reauthorization[166].

Also the program collecting Internet metadata is addressed, but only briefly, as it was abandoned in 2011 for "*operational and resource reasons*". In this program routing, addressing, and signaling information was collected but not the "*subject line of an email*". What was collected though was the "*"to" and "from" lines in an email*" – information that gives much more information about who is a partner in the email conversation as a purely numerical information and therefore would be of an even more sensitive nature than the telephone number.

With respect to the alleged collection of communication content, respondents assert that a program with that function is authorized under 50 U.S.C. § 1881a, but is only targeting non-US persons, who are "reasonably believed to be located outside the United States[167]. The procedures to gather the information through this program are also specified in the opposition: the collection is facilitated either directly through internet providers located within the United States, or as the communications "*transit internet "backbone" facilities within the United States*"[168]. If the communication identifies a US person, "*the information must reasonably appear to be foreign intelligence or evidence of a crime, or necessary to understand or assess foreign intelligence information*" before it can be disseminated by the collecting agency.

[166] for further details see *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 13
[167] ibidem – p 14
[168] ibidem

6.2.2.3 Defendants' Opposition – Arguments

In the third part of the brief defendants try to demonstrate in seven arguments[169] why the motion should be denied, five of which are of interest here.

6.2.2.3.1 Lack of standing

The first argument is plaintiffs' lack of standing as they, according to respondents, could not offer proof of suffered injury by any of the three data collection programs. No evidence was introduced to show that the NSA's PRISM program[170] "*targeted communications of [plaintiffs] (or of any non-U.S. persons with whom they communicate) for foreign intelligence purposes authorized under Section 702. Nor do they allege that communications of theirs have been or will be acquired incidental to the targeting of non-U.S. persons under section 702*"[171]. The same argument is applied *mutatis mutandis* for the discontinued program on Internet metadata collection.

As for the collection of telephony metadata, defendants' arguments do not lack a certain irony. It is maintained that plaintiffs cannot prove that the government ever collected data from Verizon Wireless, the company plaintiffs Klayman and Strange have a contract with, as the "*unlawfully disclosed Secondary Order of the FISC*[172]" was directed at Verizon Business Network Services Inc. (VBNS) – a completely different business entity.

Also "*the Government has not declassified any further information regarding VBNS's participation in this program or that of any other provider*" and "*plaintiffs' allegation do not indicate that they were subscribers of VBNS or that Verizon Wireless is subject to Section 215 collection*[173]". Respondents, citing Clapper v. Amnesty International USA 133 S.Ct. 1138 (2013)[174], explain that the "*burden to prove their standing by point-*

---

[169] these arguments are:
- plaintiffs have not demonstrated injury sufficient to establish their standing, nor shown any irreparable harm
- plaintiffs' claim that the alleged NSA activities exceed statutory authority is precluded by statute
- plaintiffs' claim that the alleged NSA intelligence-gathering programs exceeds the government's statutory authority is also unlikely to succeed on the merits
- plaintiffs cannot succeed on the merits of their fourth amendment claim because the challenged surveillance does not violate plaintiffs' fourth amendment rights
- plaintiffs cannot demonstrate that they are likely to succeed on their first amendment claim
- plaintiffs cannot demonstrate that they are likely to succeed on their fifth amendment claim
- The balance of equities and the public interest require that an injunction be denied

[170] Collection of Internet communications of non-US persons

[171] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 22

[172] ibidem – p 21

[173] ibidem

[174] for details see infra 6.2.2.3.2

ing to specific facts" lies with the plaintiffs and it is "*not the Government's burden to disprove standing by revealing details of its surveillance programs*"[175].

6.2.2.3.2 Clapper et al. v. Amnesty International et al.

This opinion of the Supreme Court[176], decided February 26, 2013 is certainly of interest here and therefor warrants a closer look at the opinion, as a lot of the arguments are valid for the question of Article III standing in both the Klayman and the ACLU proceedings.

On the same day the FISA was amended by the FISA Amendments Act of 2008 (FAA), adding 50 U.S.C. §1881a, the statutory basis for the PRISM program, Amnesty International USA and, among others, Global Fund for Women, Global Rights, Human Rights Watch, and the International Criminal Defense Attorneys Association challenged the constitutionality of this section, while defendants argued plaintiffs lacked standing, as they could not prove that conversations of either of them were actually subject of government surveillance. The District Court for the Southern District of New York followed defendants' argument, while the United States Court of Appeals for the Second Circuit, reversing the District Courts decision, ruled that plaintiffs had standing[177].

It is important to know that plaintiffs included inter alia the attorneys for several Guantanamo Bay detainees, and an individual, who faced criminal charges in connection with the September 11 terrorist attacks[178]. It is hard to believe, that the communications of these attorneys with or on behalf of their clients would not almost certainly trigger one if not several identifiers.

After the United States Court of Appeals for the Second Circuit denied a rehearing *en banc*, SCOTUS because "*of the importance of the issue*[179]" granted *certiorari*, and reversed the opinion. In its opinion, the court states that "*the law of Article III [of the Constitution] standing, which is built on separation-of-powers principles, serves to prevent the judicial process form being used to usurp the powers of the political branches*",

---

[175] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 21 – internal quotations omitted (the original citation in Clapper et al. v. Amnesty International USA et al. p 13 n.4 reads: "*As an initial matter, it is respondents' burden to prove their standing by pointing to specific facts, Lujan v. Defenders of Wildlife, 504 U. S. 555, 561 (1992), not the Government's burden to disprove standing by revealing details of its surveillance priorities*")

[176] *Clapper, Director of National Intelligence et al. v. Amnesty International USA et al.* 11-1025 (SCOTUS, February 26, 2013)

[177] *Clapper et al. v. Amnesty International et al.* 09-4112-cv (United States Court of Appeals for the Second Circuit, March 21, 2011)

[178] ibidem – p 17 n.11

[179] Clapper, Director of National Intelligence et al. v. Amnesty International USA et al. 11-1025 (SCOTUS, February 26, 2013) – p 8

that it's "*standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional*", and finally that the court has "*often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs*"[180]. The argument of the court, why the threatened injury is not certainly impending, is that five steps need to be fulfilled to "*constitute injury in fact*", and that this "*chain of possibilities*" is "*highly attenuated*"[181].

Also, the court finds the allegation that the government would actually target plaintiffs' communications "speculative", and that they could not produce any evidence for an actual monitoring of communications.

It is important to the court that plaintiffs "*do not even allege that the Government has sought the FISC's approval for surveillance of their communications*", but that their "*theory […] rests on their assertion that the Government will target other individuals– namely, their foreign contacts*", and that they "*have no actual knowledge of the Government's § 1881a targeting practices*"[182].

And when the court on p13, n.4, states that the government is not obliged to divulge surveillance details to disprove an opponent's standing, it explicates that such a "*hypothetical disclosure proceeding would allow a terrorist (or his attorney) to determine whether he is currently under U. S. surveillance simply by filing a lawsuit challenging the Government's surveillance program. Even if the terrorist's attorney were to comply with a protective order prohibiting him from sharing the Government's disclosures with his client, the court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets*".

Also, plaintiffs' allegation that without standing the constitutionality of the statute in discussion could not be challenged was dismissed by the court on the grounds, that not only is it wrong to assume, that just because plaintiffs do not have standing, no one else would have one either, but also could every affected person challenge the collection of

[180] all citations Clapper, Director of National Intelligence et al. v. Amnesty International USA et al. – p 9
[181] ibidem – p 11: "*the Government would have to decide to target a communication of non-US persons communicating with the Plaintiffs, decide to invoke authority under § 1881a, a FISC approval needs to be attained, the Government must be successful in intercepting a communication and the Plaintiffs must be part of that particular communication*"
[182] ibidem – p 12

the data if it were introduced as evidence in court by the government. And finally and most interestingly the court argued, "*any electronic communications service provider that the Government directs to assist in § 1881a surveillance may challenge the lawfulness of that directive before the FISC*".

It cannot go unmentioned that four Justices were dissenting, arguing that the harm is not speculative, but "*is as likely to take place as are most future events that commonsense interference and ordinary knowledge of human nature tell us will happen*"[183]. Obviously, the dissenting Justices attached more importance to who the clients of some of the plaintiffs were, and therefor find that in all likelihood at least part of the communication between the attorneys and their clients could be seen as related to terrorism and counter-terrorism.

6.2.2.3.3 No exceeding of Statutory Limits

The second argument of interest discusses plaintiffs' claim that the NSA programs exceed the government's statutory authority[184], disputing the relevance of the obtained data, as well as the FISC's authority to order the production of records not yet in existence.

Defendants, trying to refute the claim of irrelevance, argue that the term as well as the concept of relevance has a well-established meaning, not only in official investigations, but also in civil proceedings. They explore the broad relevance standard that is attributed in grand jury subpoenas, "*unless there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation*"[185]. Also administrative agencies can subpoena as evidence "*virtually any material that might cast light on the allegations at issue in an investigation*"[186]. And even when admitting that "*the case law in the contexts of civil discovery, grand jury subpoenas, and administrative investigation does not involve data acquisition on the scale of the telephony metadata collection",* defendants claim that *"relevance must be evaluated in light of the special nature, purpose, and scope of national security investigations*"[187]. When reflecting on the "relevance" of the data, it has to be taken into account that the nature of these investigations is entirely different to

[183] Clapper, Director of National Intelligence et al. v. Amnesty International USA et al. – dissenting opinion – p 1
[184] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 31
[185] ibidem – p 32; internal quotations and emphasis omitted
[186] ibidem – p 33; internal quotations omitted
[187] ibidem – p 34

ordinary procedures, as they are not looking retrospectively at already committed wrongdoings, but proactively try to inhibit terrorist activities from happening in the future. Therefore national security investigations have a much broader scope with respect to duration, geographical area, and involved persons and assets of interest, thus vindicating the wider connotation Congress obviously attributed to the relevance standard when enacting and reauthorizing the Statute in question here, while fully aware of the latitude of the programs proposed by the government and approved by the FISC. A more limited interpretation would bereave the Agencies involved in counterterrorism investigation of the one tool that allows for an early detection of attacks, and "*be contrary to the express understanding of the statue that Congress ratified on two separate occasions*"[188] (similar arguments by FISC supra p 45-47).

According to respondents, this meaning is also reflected in the different language of section 215(b)(2)(A), allowing to seek tangible things that are *"relevant to an authorized investigation*", as opposed to "*information relevant to the subject matter*" the wording usually used in civil discovery[189], asking to show "*reasonable grounds to believe*" that something is relevant rather than to demand a proof of relevance.

Further, defendants contest plaintiffs' claim that relevance cannot be attributed to the records collected, as only a fraction of the collected data can be attributed to persons subject to an authorized investigation, or suspected of terrorist activity, by pointing to the changes, the USA PATRIOT Act in 2001 entailed to previous provisions "*by eliminating the requirement in prior law of specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power*", thus considerably broadening the government's leeway in obtaining business records. Also, defendants' reason, Congress expressly refused to endorse a proposition to limit the collection of information to persons already under suspicion of terrorist activities.

Finally the wording of section 215 does not prevent the FISC from ordering to produce records not yet existing at the time of the order, as it refers to "any" tangible things, hence not limiting the records to be sought with the order in any kind. Apart from that, the production of future information has been considered appropriate on various occasions and defendants state, "*Courts have held that the Government may seek prospective*

[188] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 38
[189] ibidem – p 36 n.22; internal quotations omitted

disclosure of records .... because the prospective ... information sought by the Government ... becomes a historical record as soon as it is recorded by the provider"[190].

With regard to the collection of bulk Internet metadata, the respondents not only point to the fact that the program has been terminated in 2011, but also that plaintiffs simply are at fault when claiming that by implementing this program the government transgressed it's competence under section 215, as the collection of Internet metadata was authorized under 50 U.S.C. § 1842 and not 50 U.S.C. § 1861.

Equally, section 215 does not allow for the collection of content of electronic communication, so basing the claim on this statue is "*misguided as matter of fact and law*", moreover, the program plaintiffs mean to challenge, according to respondents, is based on § 702 of FISA (50 U.S.C. § 1881a).

6.2.2.3.4 No violation of Fourth Amendment Rights

The government's arguments against a violation of Fourth Amendment rights, as anticipated in the analysis of the complaints, are mostly based on the third-party-doctrine as laid out by the Supreme Court in Smith v. Maryland, 442 U.S. 735 (1979): all the data collected was voluntarily provided to a third party, no search of plaintiffs or their property was conducted to gather the data, there cannot be a "reasonable expectation of privacy" when telephone numbers are concerned, and all interested parties were well aware of the fact that all the records in question here are collected by phone companies for various business-related purposes. Moreover, the information obtained does not allow identifying the parties of a telephone call, much less drawing conclusions about their private lives.

So not only does the collection not constitute a search, but defendants argue it would additionally not represent a Fourth Amendment violation, as "*the collection of metadata at issue here is reasonable under the standard the Supreme Court applies to assess suspicionless searches that serve special government needs*"[191]

It goes without saying that the government finds the purpose for the data collection to be "*of overwhelming importance*", and its interest "*of the highest order of magnitude*".

[190] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 43; internal quotations omitted
[191] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 50

6.2.2.3.5 No violation of First Amendment Rights

According to respondents "*courts distinguish for purposes of First Amendment analysis between government investigation that may have the incidental effect of deterring First Amendment activity, and concrete government action of a regulatory, proscriptive, or compulsory nature that is directed against individuals based on their expressive or associational activities*"[192].

The overarching argument of the government is, that programs only collecting metadata cannot *per se* infringe First Amendment rights, as the purpose and the tools used are not intended to inhibit free speech or the right of free association. And, as plaintiffs' cannot show evidence that their metadata has ever been accessed or analyzed, they cannot claim a violation of their First Amendment rights.

The only program that could have a chilling effect on First Amendment rights, as it collects content, would be PRISM, a program directed solely at non-US persons. But, in defendants' view, plaintiffs could not show evidence that they ever communicated with targeted non-US persons, and that through this program any content of such an electronic conversation has been collected. Furthermore, as they did not assert that they have been unlawfully targeted by PRISM themselves, the First Amendment claim also must fail also with respect to this program.

6.2.2.3.6 No violation of Fifth Amendment Rights

The opposition does not really elaborate on plaintiffs' Fifth Amendment claim with regard to substantive due process, rather defendants restrict themselves to the argument that "*because Plaintiffs ground their substantive due process claim on privacy interests allegedly protected by the Fourth Amendment, that claim cannot serve as an independent basis for issuing a preliminary injunction*[193]". This is astounding as there seems to be a risk that an assertion of the Fifth Amendment may induce a strict scrutiny review of the statute itself, and one would have assumed that the government would not let an opportunity pass to argue the constitutionality of the statute in question.

Also, the arguments to dismiss the procedural due process claim are limited to the fact that plaintiffs have not been able to substantiate their allegation, that the government would be obliged to give prior notice to plaintiffs before starting collecting metadata relating to them.

---

[192] *Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction* – p 56

[193] ibidem – p 61

6.3 Comments

It comes as no surprise that the texts reveal a completely different understanding of the significance of the data collected, thus resulting in an equally different legal reasoning. While plaintiffs allege that the metadata divulges, "*whom they call, precisely when they call them, and for precisely how long they speak*[194]", the government completely rejects such an interpretation. In their reading, the data they collect is mere numerical data that does not support the conclusion, who was placing the call, and who was receiving it. Only when responding to a query, the data is analyzed. It has not been discussed in the briefs, whether this analysis includes substantiation with respect to who the "owners" of the telephone numbers are, and from where the call was placed (or where it was received).

Also, the parties differ in their conclusion on how many people would be affected by the three-hop concept. On the basis of 40 non-overlapping telephone numbers used, plaintiffs calculate that a three hop query would return the metadata of over two million telephone numbers, while Ms. Shea in her declaration[195] states that this would require a fourth hop, but that such a fourth hop is not authorized by the FISC. It should not go unmentioned, that the numbers presented by the Government on page 8, n.3, of the "Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction" and those presented by Ms Shea in her Declaration on page 9, n.1, are not identical[196].

7. Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint in ACLU et al. v. Clapper et al.

On August 26, 2013, Defendants in ACLU et al. v. Clapper et al. filed their Memorandum of Law in Support of Motion to Dismiss the Complaint[197].

Already the preliminary statement as well as the statement of facts shows that the mo-

[194] *ACLU et al. v. Clapper et al. - Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction* – p 17
[195] *ACLU et al. v. Clapper et al. - Declaration of Teresa H. Shea, Signals Intelligence Director, National Security Agency.* 13-cv-3994 (United States District Court for the Southern District of New York, October 1, 2013)
[196] Government 65.640 (first hop: 1x40=40; second hop: 41x40=1640; third hop: 1641x40=65640) Shea 64000 (first hop: 1x40=40; second hop: 40x40= 1600; third hop: 1600x40=64000; forth hop 64000*40= 2560000)
[197] *ACLU et al. v. Clapper et al. - Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint.* 13-cv-3994 (United States District Court for the Southern District of New York, August 26, 2013)

tion to dismiss relies on the same arguments as discussed in the analysis of the memorandums filed in opposition of the motions for preliminary injunctions and in the FISC Court Order dated August 29, 2013, Docket Number BR 13/109. The government reiterates that the FISC authorized the program several times over the past six years, describes the kind of data collected, the limitations of the authorizations with regard to identifiers and queries, and that the program is well within the limits of the statutory authority of section 215 of the USA PATRIOT Act.

Defendants also use identical rationales and authorities to dispute plaintiffs' standing, and to reject the claims of Constitutional violations with regard to the Fourth Amendment (the collection of metadata does not constitute a search or seizure as held by the Supreme Court in Smith v. Maryland, this being said, even if an interest protected by the Fourth Amendment would be infringed, given the special interest the government has in fighting terrorism, the program is the least abrasive tool, guaranteeing only minimal intrusion of privacy, and therefore is reasonable and lawful), with regard to the First Amendment (the program is not directed at plaintiffs' First Amendment rights, no expectation of privacy for telephone metadata voluntarily offered to a third party, no proof of actual effect on plaintiffs' or their clients), as well as the claim of exceeding statutory authority (Congress, while fully aware of the range of the program, did not change the statute when reauthorizing Section 215 in 2010 and 2011).

Furthermore defendants, when discussing the relevance aspect of the data collected, make it very clear, that Congress due to the broad scope of the program "*built protections into the statutory scheme not found in the other legal contexts*"[198], and that the prerequisite of prior judicial authorization provides the review necessary to balance the exceptional authority granted to the government.

8. The Courts' Decisions

On December 16, 2013, the United District Court for the District of Columbia granted plaintiffs request for injunction in Klayman et al. v. Obama et al., while on December 27, 2013, the United States District Court Southern District of New York not only denied the ACLU's request for injunction, but also dismissed the claim altogether.

[198] *ACLU et al. v. Clapper et al. - Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint* – p 26, n.14

8.1 Klayman et al. v. Obama et al. Memorandum Opinion

8.1.1 Introduction and Statutory Background

In the introduction, the court finds that it only has jurisdiction with regard to the Constitutional claims, but lacks this jurisdiction with regard to the assertion that the government, when implementing the program, exceeded the statutory authority of section 215 of the USA PATRIOT Act. Also, the court not only affirms that plaintiffs have standing, but deems it likely that they will succeed on the merits with their claim that the bulk collection violated their Fourth Amendments right.

However, the court decided to stay the order pending appeal because of "*the significant national security interest at stake … and the novelty of the constitutional issues*[199]".

At the outset the court discusses the statutory background of the FISA and section 215 of the USA PATRIOT Act, and in particular the history of the Act as well as the changes made after the September 11 attacks, detailing the parts of the statute of interest for this case.

The composition of the FISC is equally mentioned, especially the fact that three of the FISC judges must reside within 20 miles of the District of Columbia[200], and that therefore "*a disproportionate number of the FISC judges are drawn from the district courts of the District of Columbia and the Eastern District of Virginia*"[201]. This seems to be a subject of concern to Judge Leon, as he keeps coming back to this argument when discussing the judicial review of FISC Court Orders[202].

Finally the court states, quipping that "*to say the least, plaintiffs' and the Government have portrayed the scope of the Government's surveillance activities very differently*"[203], that the reasoning of the opinion would be based on the government's description of the surveillance program. But relative to the government's interpretation what "only a small percentage of the collected data is responsive to a query" actually means, it becomes very clear that Judge Leon fundamentally disagrees with the government's position. His

[199] *Klayman et al. v. Obama et al. - Memorandum Opinion.* 13-civ-0851 (United States District Court for the District of Columbia, December 16, 2013) – p 6
[200] 50 U.S.C. § 1803(a)(1)
[201] *Klayman et al. v. Obama et al. - Memorandum Opinion* – p 10 n 13 citing Theodore W. Ruger, Chief Justice Rehnquist's "Appointments to the FISA Court: An Empirical Perspective"
[202] ibidem – p 13 n 14 "*The tree judges who reside within twenty miles of the District of Columbia comprise the petition review pool*"
[203] ibidem – p 14 with a reference to the plaintiffs allegations they were the NSA's primary target

very personal view of the implications the three-hop query might have is a good example of the fear, this program induces in many people, and why, together with the reported and acknowledged compliance errors and violations, it leaves them very uncomfortable:

"*Suppose, for instance, that there is a person living in New York City who has a phone number that meets the RAS [reasonable, articulable suspicion] standard and is approved as a "seed." And suppose this person, who may or may not actually be associated with any terrorist organization, calls or receives calls from 100 unique numbers, as in my example. But now suppose that one of the numbers he calls is his neighborhood Domino's Pizza shop. The Court won't hazard a guess as to how many different phone numbers might dial a given Domino's Pizza outlet in New York City in a five-year period, but to take a page from the Government's book of understatement, it's "substantially larger" than the 100 in the second hop of my example, and would therefore most likely result in exponential growth in the scope of the query and lead to millions of records being captured by the third hop."*[204]

8.1.2 Constitutional Claims

8.1.2.1 Standing

It does not come as a surprise that the government's argument for plaintiffs' lack of standing[205] did not go down well with the court. Judge Leon finds the government was "*straining mightily*" to find an argument to support that claim, and moreover that it contradicts the defendant's plea that only the broad nature of the program addressing numerous telecommunication service providers guarantees the success of the program. He repudiates the government's arguments and concludes, "*Candor of this type defies common sense and does not exactly inspire confidence!"*[206].

And while Judge Leon does not follow plaintiffs' arguments for proof of the NSA having queried their numbers, it still finds that they have standing challenging the NSA querying procedures, because in Judge Leon's understanding the search for a telephone number responsive to a "seed" will only be successful, if all the telephone numbers in the database have been looked at, thus making it very unlikely that not all the telephone numbers were "analyzed". The court also does not differ between analysis by an agent

[204] *Klayman et al. v. Obama et al. - Memorandum Opinion* – p 19, n.21
[205] supra p 50 plaintiffs are customers of Verizon Wireless while the Court Order was directed at Verizon Business Network Services
[206] *Klayman et al. v. Obama et al. - Memorandum Opinion* – p 38

or by analytical software[207], and in doing so turns the governments "Smith" argument ("*We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate*") against the defendants[208].

The court also dismisses Clapper et al. v. Amnesty International as a relevant authority, as the fundamental difference between Clapper and this case is, that plaintiffs in Clapper at the time of it's decision did not and could not have any evidence for a mass surveillance program, quite contrary to the position of the plaintiffs here after the publication of the FISC court order.

8.1.2.2 Fourth Amendment Violation – does the metadata collection constitute a search

The court then addresses the question of a violation of the Fourth Amendment by applying a two-step analysis where the court first establishes whether plaintiffs have a reasonable expectation of privacy, and if it finds such expectation exists, the collection of the metadata would constitute a search under the Fourth Amendment. In the second step the court then establishes, whether the government's arguments, that the collection of the metadata is reasonable and constitutes the least intrusive means are justified.

The government in it's motion always relied on Smith v. Maryland, when arguing that nobody would have a reasonable expectancy of privacy with regards to their telephone number, as this is information voluntarily entrusted to a third party. But Judge Leon profoundly disagrees. As he very pointedly remarks: "*Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances–the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies–become so thoroughly unlike those considered by the Supreme court thirty-four years ago that a precedent like Smith simply does not apply? The answer, unfortunately for the Government, is now*."[209].

He equally dismissed defendants' argument that United States v. Jones is not applicable, by contrasting it to another decision – United States v. Knotts, 460 U.S. 286 (1983) – and the technical advances between the time a tracking beeper was used in Knotts and a GPS device in Jones, leading to a significantly different outcome with regard to Fourth

[207] The courts reasoning for the question of standing shows a substantial difference in the interpretation of what is "analyzing" the metadata. The Government does not see the initial query as an analysis but merely an electronic filter to find responsive telephone numbers that then are analyzed in the sense of having an NSA analyst looking at them. In Contrast the Court obviously considers every handling of the data to be an analysis with Fourth Amendment implications.
[208] *Klayman et al. v. Obama et al. - Memorandum Opinion* – p 41
[209] ibidem – p 45

Amendment implications, though in both cases a car, moving on public streets, was being monitored.

Moreover Judge Leon specifically mentions several factors that for him distinguish Smith from the subject matter.

First he claims that the long period of time the program was running and that it could be running with no end in sight, as opposed to the few days the trap and trace was in place in Jones, and the entirely different kind of data repository the extensive "*historical content information*" provides demonstrates a significant dissimilarity between the two cases.

Furthermore, the long period of time the program is in place has helped to evolve a special relationship between the government and the telephone service providers, and that hinders the application of the third-party doctrine as demonstrated in Smith. While the court agrees that the general public is well aware that telephone companies provide information to the government, they were not anticipating a "*joint intelligence-gathering operation*" facilitated by "*Orwellian technology*"[210].

His biggest concern however was that the "nature and quantity of the information contained in people's telephony metadata is much greater" than anybody could have imagined in 1979, the year Smith was decided. Or as Judge Leon phrased it: "*Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago, none of those phones would have been there. Thirty-four years ago, city streets were lined with pay phones*". And as he was not sure whether telephony metadata also included routing information on text messages, he added: "*Thirty-four years ago, when people wanted to send "text messages", they wrote letters and attached postage stamps*.[211]"

And though he recognizes that the information that can be drawn from metadata is somewhat limited, his concern is "*the quantity of the information that is now available and, more importantly, what that information can tell the Government about people's lives*."[212]. He considers the assumption that the evolution of a "cell phone-centric" culture as we have it today has led people to accept less privacy is wrong, but that on the contrary "*these trends have resulted in a greater expectation of privacy and a recogni-*

[210] *Klayman et al. v. Obama et al. - Memorandum Opinion* – p 48-49
[211] ibidem – p 52
[212] ibidem – p 53

tion that society views that expectation as reasonable"[213].

8.1.2.3 Fourth Amendment Violation – is the metadata collection reasonable

When discussing the question of reasonableness the quotes Judge Leon uses to lead into the subject have the underlying notion, that only in some rare instances a search can be reasonable without either a warrant or a certain degree of individualized suspicion. The questions the Judge sees before him therefor are, whether the government's interest in the warrantless search outbalances plaintiffs' reasonable expectancy of privacy, or whether a less burdensome process could be established. For the court, the mere scope of the program precludes any comparison to previous unwarranted searches upheld by various courts.

And while the court agrees, that preventing terrorist attacks on American soil is of the utmost importance, it has grave doubts that this can only be achieved by the metadata collection. The court gives utterance to the impression that the main advantage of the metadata collection, as opposed to other investigative methods, is speed. An while Ms. Shea and Mr. Holley emphasized the significant benefit of the program in time-sensitive situations, the court could not help noticing that the government could not demonstrate a single incident where time was a decisive factor, Judge Leon even applauded Assistant Director Holley's concession that investigative methods used by the FBI's have sometimes proven to be successful even before information from the database was obtained.

As the government according to Judge Leon chose not to request an *in camera* presentation of additional classified evidence to support it's claim, that fifty-four terrorist attacks have been prevented only because of the metadata collection program, he voiced "*serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism*"[214], thus concluding that the search is not reasonable.

8.2. ACLU et al. v. Clapper et al. Memorandum and Order

8.2.1 introduction and Statutory Background

The United States District Court for the Southern District of New York delivered the Memorandum and Order in the ACLU case, not only denying the motion for preliminary injunction but also dismissing the lawsuit. Its two seats in New York City, where

[213] ibidem – *p 55*
[214] *Klayman et al. v. Obama et al. - Memorandum Opinion* – p 62

24 of its 28 judges have their place of duty[215], is located in the Civic Center, a 1.5 km walk from the World Trade Center. And in the introduction of his memorandum Judge Pauley voices his opinion, that while the conventional intelligence programs in place before 9/11 failed to help prevent the terrorist attacks, telephone metadata "*would have furnished the missing information and might have permitted the NSA to notify the Federal Bureau of Investigation ("FBI") of the fact that al-Mihdhar[216] was calling the Yemeni safe house from inside the United States*."[217].

Also in this order the historical backgrounds of the FISA and the FISC are discussed, and Judge Pauley concentrates on the aspect of secrecy under which the FISC operates. Citing Art. I § 5 of the Constitution he states that not only Congress, but also the Constitution allows for a certain amount of secrecy when national security is concerned. He also expressly points to the fact, that the USA PATRIOT Act of 2001, by removing the previous constraints on the categories of businesses that could be a subject to the business records provision, as well as eliminating "*the requirement that the target be a foreign power or their agent*"[218], considerably broadened the government's authority to collect information. The court also considers the supervision of the program to be "*extensive*", with oversight "*by all three branches of government*", and discusses the problems of compliance that have occurred as well as the remedies for these issues. In his believe, the FISC order by Judge Bates, cited by the court in Klayman[219] as an example for the concern the FISC voiced over compliance issues, demonstrates that the FISC routinely "*engaged in a protracted iterative process with the Government*" and by no means just "*rubberstampe[d] applications for section 215 orders*"[220].

Finally Judge Pauley indicates, that Congress had renewed the sunset clause seven times.

When discussing the metadata collection program, Judge Pauley's understanding of the process varies widely from the one Judge Leon demonstrated in his opinion. Citing the declaration by Ms. Shea, the SID of NSA, the court states that "*there are restrictions on how and when it [the collected metadata] may be accessed and reviewed*", that the NSA

[215] apart from the Thurgood Marshall United States Courthouse and the Daniel Patrick Moynihan United States Courthouse in New York City the Court has a third seat in White Plains with 4 Judges located there.
[216] one of the hijackers in the 9/11 attacks
[217] *ACLU et al. v. Clapper et al. - Memorandum & Order.* 13-civ-3994 (United States District Court for the Southern District of New York, December 27, 2013)– p 1-2
[218] ibidem – p 6
[219] *Klayman et al. v. Obama et al. - Memorandum Opinion* – p 22
[220] *ACLU et al. v. Clapper et al. - Memorandum & Order* – p 7

"*may access the metadata to further a terrorism investigation only by "querying" the database with a telephone number, or "identifier", that is associated with a foreign terrorist organization*", that there needs to be a "reasonable, articulable suspicion" that the identifier is connected to an international terrorist organization, and "*that the "reasonable articulable suspicion" requirement ensures an "ordered and controlled" query and prevents general data browsing*". And while Judge Leon concluded that such a query would need to check every single telephone number in the database, and thus constitute a Fourth Amendment search, the court in ACLU concentrates on the fact that the NSA, only after the query showed results, "*takes this information and determines which of the results are likely to contain foreign intelligence information, related to counter-terrorism, that would be of investigative value to FBI (or other intelligence agencies)*" [221]. Additionally Judge Pauley does not do the math on the "three hops" himself, but cites the Shea declaration that though "substantially larger than 300" the number of metadata records responsive to query was "*still a very small percentage of the total volume of metadata records*", and that in 3 years (2006-2009) the NSA provided "*277 reports containing approximately 2,900 telephone numbers*" to the FBI.

8.2.2 Standing and lack of subject matter jurisdiction

Also, the court in ACLU, relying on Amnesty International v. Clapper, discusses the standing extensively, and as Judge Leon did, considers it a fact that telephone metadata of the plaintiffs was collected, thus giving the plaintiffs standing.

Also, both courts in Klayman and ACLU agree that they lack subject matter jurisdiction with regard to the claim, that the government exceeds the statutory authority granted by section 215 of the USA PATRIOT Act with it's metadata collection program, following the government's argumentation that Congress, when enacting the statute, precluded a review under the Administrative Procedure Act. But unlike Judge Leon, who leaves it at that, Judge Pauley, stating that "*even if the statutory claim were not precluded, it would fail*"[222], discusses also the merit of that claim.

8.2.3 No exceeding of the statutory limits

Comparing 18 U.S.C. § 2703 to 50 U.S.C. § 1861, the court states that the latter's only limitation is, that the records sought might be obtainable with a grand jury *subpoena*, and that nothing in the statute supports the claim that it is limited by provisions from the

[221] all quotes in the paragraph *ACLU et al. v. Clapper et al. - Memorandum & Order* – p 10-11 (internal quotation marks partially omitted)
[222] *ACLU et al. v. Clapper et al. - Memorandum & Order* – p 25

Stored Communications Act[223]: "*Read in harmony, the Stored Communications Act does not limit the Government's ability to obtain information from communications providers under section 215 because section 215 orders are functionally equivalent to grand jury subpoenas. Section 215 authorizes the Government to seek records that may be obtained with a grand jury subpoena, such as telephony metadata under the Stored Communications Act*"[224].

The second argument, why the government acted within the limits Congress allocated to section 215, mirrors the arguments of FISC Judge Eagan, when she reauthorized the metadata collection in August 2013, namely that Congress was well aware of the government's interpretation of section 215. And though Judge Pauley considers it to be "problematic" that the House Intelligence Committee did not make a document, detailing the scope of the surveillance program, available to all members of the House, he still finds that "*Congress ratified section 215 as interpreted by the Executive Branch and the FISC, when it reauthorized FISA"*[225]. And n.13 on page 31 does not withhold criticism, when Judge Pauley finds Congressman Sensenbrenner's statement in his *Amicus* Brief, filed to support ACLU in this lawsuit, to be "*a curious statement*" considering the fact that he "*not only had access to the five-page report made available to all Congressmen, but he also, as "a long-serving member of the House Judiciary Committee" was briefed semi-annually by the Executive Branch*", concluding that through this briefings and the FISC documents he received, the Congressman was well aware of the government's legal interpretation and the scope of the metadata collection.

And finally addressing the issue of relevance, the court, with an interesting reasoning, finds that the ACLU's argument of the irrelevance of most of the data "*has no traction here*": the FISC order forbids that the NSA disseminates data before having identified the data suspected to be pertaining to (suspected) terrorists. And while section 215 "*contemplates that tangible items will be produced to the FBI, FISC orders require that bulk telephony metadata be produced directly–and only –to the NSA*".

---

[223] The Stored Communications Act (18 U.S.C. § 2701-2712) was enacted as Title II of the Electronic Communications Privacy Act of 1986. The Statutes were inserted to Title 18 of the United States Code by Section 201 the Electronic Communications Privacy Act of 1986 that was amended in 1988 by the Drug-Free Workplace Act of 1988, in 1994 by the Communications Assistance for Law Enforcement Act, in 1996 by the Intelligence Authorization Act for Fiscal Year 1997, in 1998 by the Telemarketing Fraud Prevention Act of 1998, in 2001 by the USA PATRIOT Act of 2001, in 2002 by the 21st Century Department of Justice Appropriations Authorization Act, in 2005 by the Violence Against Women and Department of Justice Reauthorization Act of 2005 and finally in Foreign Evidence Request Efficiency Act of 2009.

[224] *ACLU et al. v. Clapper et al. - Memorandum & Order* – p 27

[225] *ibidem* – p 31

By and large Judge Pauley follows the government's arguments that it takes all the information to isolate the significant ones, thus making all the information relevant in the broad sense of the meaning.

8.2.4 Constitutional claims

Finally, after having spent considerable time explaining, why a claim that was precluded in the first place also lacked substance on the merit, the Judge discusses the Constitutional questions.

The Judge turns to Smith[226] when contemplating the Forth Amendment claim and finds that "[*t]he privacy concerns at stake in Smith were far more individualized than those raised by the ACLU*". Furthermore, he does not agree with the ACLU's conclusion that the metadata collection allows "*the creation of a rich mosaic*" of information about individuals. For him, the "*rigorous minimization procedures*" in place, and the fact that the data do not include any information on who the subscriber is, precludes such an application. Apart from that he states, citing General Alexander's testimony, "*the Government repudiates any notion that it conducts the type of data mining the ACLU warns about in its parade of horrible*s"[227].

Also, the argument that the metadata collection is neither reasonable, nor the least intrusive means is dismissed. Neither could the ACLU produce any evidence that there are other possibilities to gather the information needed that would be less intrusive, nor does the Supreme Court conclude that "only the "*least intrusive" search practicable can be reasonable under the Fourth Amendment*"[228]. And, citing Quon, 130 S. Ct. at 2632, Judge Pauley states "*That judicial-Monday-morning-quarterbacking could raise insuperable barriers to the exercise of virtually all search-and-seizure powers because judges engaging in after-the-fact evaluations of government conduct can almost always imagine some alternative means by which the objectives might have been accomplished*"[229].

But the most interesting reasoning is that the court finds, the ACLU fundamentally misunderstood the nature of ownership with respect to telephone metadata, and that this question is critical to the claim, as a person voluntarily providing information to a third party cannot expect a right to privacy with respect to that information. And for the court

[226] Smith v. Maryland 442 U.S. 735 (1979)
[227] *ACLU et al. v. Clapper et al. - Memorandum & Order* – p 41
[228] ibidem
[229] ibidem – internal quotation marks omitted

it is no question that the metadata does not belong to the ACLU, but that the respective telephone company is the owner of the data, thus obliterating any Fourth Amendment claim.

Furthermore neither the fact that the data might be queried more than once, nor the vast amount of data collected can constitute such a claim, when there is none in the first place.

For the court Smith is applicable, and it follows the government that relying on the concurring opinion of Justice Sotomayor in Jones is "*misplaced*", pointing to the fact that apart from the data collection, placing a GPS device implicates a physical intrusion that would constitute as a Fourth Amendment search as such.

The court also rejects the idea that Smith would be rendered irrelevant by "*the ubiquity of cellular telephones and how subscribers' relationships with their telephones have evolved since Smith*", by stating that "[*w]hile people may have an entirely different relationship with telephones than they did thirty-four years ago … this Court observes that their relationship with their telecommunications providers has not changed*"[230]. That being said, the court concludes that the Smith precedent is still valid, as the content of metadata has not changed over the years, and therefore the bulk collection of metadata is not violating the Fourth Amendment.

The court's considerations on why to dismiss the Fourth Amendment claim only fill six pages; even less is spent on the First Amendment argumentation. Citing several authorities[231], it all boils down to the argument that when the court finds that the collection of telephone metadata is consistent with the protection given by the Fourth Amendment, it consequently cannot constitute a violation of the First Amendment. And as the Supreme Court in Amnesty International v. Clapper has concluded that "*the bulk metadata collection does not burden First Amendment rights substantially*" the court deems it "*unnecessary to decide whether there could be a First Amendment violation in absence of a Fourth Amendment violation*" [232].

The court, following the government's asseveration that the metadata cannot and will

[230] *ACLU et al. v. Clapper et al. - Memorandum & Order* – p 44
[231] Inter alia United States v. Alvarez, 132 S. Ct. 2537, 2548 (2012), Nat'l Commodity & and Barter Ass'n v. Archer, 31 F.3d 1521, 1531 n.4 (10th Cir. 1994), In re Grand Jury Proceedings, 776 F.2d 1099, 1102-03 (2d Cir. 1985), Gordon v. Warren Consol. Bd. Of Educ., 706 F.2d 778, 781 n.3 (6th Cir. 1983), United States v. Mayer, 503 F.3d 740, 747-48 (9th Cir. 2007), Anderson v. Davia, 125 F.3d 148, 160 (3d Cri. 1997), Phila. Yearly Meeting of Religious Soc. Of Friends v. Tate, 519 F.2d 1335, 1337-38 (3d Cir. 1975)
[232] both quotes *ACLU et al. v. Clapper et al. - Memorandum & Order* – p 46

not be used for another purpose than the one approved in the FISC's orders, finds the worries of the ACLU to be "*speculative*", "*insufficient to create standing*" and inadequate to "*establish a violation of an individual's First Amendment rights*".

9. Conclusion

The purpose of this thesis was to analyze what led two US District Courts to contradicting decisions on whether the bulk metadata collection program was lawful and constitutional. Pondering the same legal questions and citing the same authorities they came to conclusions that seem to be diametrically opposed.

The thing the Judges interpret differently is the nature of the data. This is the decisive factor. A different understanding of the nature must, without fail, lead to a different legal interpretation.

In the first query only abstract numerical data is matched. Only those numbers "connecting" are filtered out. Though all data are "looked at" as Judge Leon observed, still they are anonymous. The legal question is, whether this set of numbers at the time of their collection and at the time of the first query can be the subject of a Fourth Amendment search.

A lot speaks for the validity of Judge Pauley's and also the government's arguments that Smith is still valid:

- In Smith, one party of the calls registered was known from the very beginning; today the data collection is anonymous – thus much less "individualized" as the data collected in Smith.
- If one set of data does not enjoy Fourth Amendment protection – why should millions of the same kind suddenly be protected?
- The substance of the data collected with the pen register in Smith has not changed. It is the same numerical information and also 34 years ago in a second step, law enforcement could have identified all the owners of the numbers calling and being called from the original number.
- To find out, if the suspect in Smith called the number of the victim, it's very likely that more than one number created by the pen register had to be looked at. Today only a responsive number is "analyzed" – but if a number is responsive it definitely is relevant to an authorized investigation.
- When "innocuous documents" are subject to an examination, the government, as

observed by the Supreme Court in Andresen v. Maryland, has to "take care to assure" to conduct the query in a "manner that minimizes unwarranted intrusions of privacy"[233].

- A keyword search was specifically suggested by SCOTUS in "In re Grand Jury Subpoena Duces Tecum" as a remedy to preclude the delivery of irrelevant documents[234].

Also the arguments of the legal differences between the metadata collection and the GPS device in Jones, as presented by the government, are more convincing. It is definitely more intrusive, but probably less scary, to think of law enforcement placing a GPS transmitter to a person's car, than the government collecting data of every telephone number a person calls – especially if the government, contrary to the officer placing the device, does not know who that "person" actually is.

Several recent U.S. decisions suggest, that judges strive in aligning evolving technology with the legal means placed at their disposal. Judge Leon on page 55 of his opinion voiced this struggle by stating that he "*cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones*[235]". It was for a reason he pleaded the "*novelty of the constitutional issues*" as the motive for staying his order pending appeal.

This being said, contrary to expectations in the analysis, neither the plaintiffs[236] nor one of the Judges even posed the question if section 215 as a whole is constitutional, while a substantive due process argument was expected to be the decisive factor in the courts' decisions.

To this date Klayman et al. v. Obama et al. has not been decided, nor has there been a decision by an Appellate Court, neither on the Injunction granted in Klayman, nor on the dismissal in ACLU.

[233] supra p 26
[234] supra p 40
[235] referring to Smith v. Maryland
[236] Klayman did at least claim a Fifth Amendment violation, but never argued it thoroughly

In the end it will be the Supreme Court who decides on the interpretation of the metadata collection, and if Smith v. Maryland is still valid after more than thirty-four years, or if its findings needs to be reversed and adapted to todays technical possibilities. It will be interesting to see what part if any the political dimension of prohibiting the program and thus risking possible debilitating effects on fighting terrorism will have in this decision.

Bibliography

ACLU. *American Civil Liberties Union.* October 24, 2011. https://www.aclu.org/national-security/surveillance-under-patriot-act (accessed July 20, 2014).

—. *American Civil Liberties Union.* December 10, 2010. https://www.aclu.org/national-security/surveillance-under-usa-patriot-act (accessed July 20, 2014).

—. *American Civil Liberties Union.* October 27, 2006. https://www.aclu.org/national-security/citing-improvements-law-aclu-withdraws-section-215-case-vows-fight-individual-orde (accessed July 20, 2014).

ACLU et al. v. Clapper et al. - Brief of former members of the Church Committee and Law Professors as Amicus Curiae supporting Plaintiff. 13-cv-3994 (United States District Court for the Southern District of New York, August 30, 2013).

ACLU et al. v. Clapper et al. - Complaint. 13-cv-3994 (United States District Court for the Southern District of New York, June 11, 2013).

ACLU et al. v. Clapper et al. - Declaration of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation. 13-cv-3994 (United States District Court for the Southern District of New York, October 1, 2013).

ACLU et al. v. Clapper et al. - Declaration of Teresa H. Shea, Signals Intelligence Director, National Security Agency. 13-cv-3994 (United States District Court for the Southern District of New York, October 1, 2013).

ACLU et al. v. Clapper et al. - Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction. 13-cv-3994 (United States District Court for the Southern District of New York, October 1, 2013).

ACLU et al. v. Clapper et al. - Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint. 13-cv-3994 (United States District Court for the Southern District of New York, August 26, 2013).

ACLU et al. v. Clapper et al. - Memorandum & Order. 13-civ-3994 (United States District Court for the Southern District of New York, December 27, 2013).

ACLU et al. v. Clapper et al. - Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction. 13-cv-3994 (United States District Court for the Southern District of New York, August 26, 2013).

Bivens v. Six Unknown Federal Narcotics Agents. 403 U.S. 388 (1971) (SCOTUS, June 21, 1971).

Clapper et al. v. Amnesty International et al. 09-4112-cv (United States Court of Appeals for the Second Circuit, March 21, 2011).

Clapper, Director of National Intelligence et al. v. Amnesty International USA et al. 11-1025 (SCOTUS, February 26, 2013).

Congressional Research Service. *The Constitution of the United States of America - Analysis and Interpretation.* Washington, DC: US Government Printing Office, 2013.

Department of Justice - Director of Public Affairs. *Office of the Director of National Intelligence.* July 31, 2013. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/908-dni-clapper-declassifies-and-releases-telephone-metadata-collection-documents (accessed July 7, 2014).

Department of Justice - Office of Legislative Affairs. *Office of the Director of National Intelligence.* July 31, 2013. http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf (accessed July 28, 2014).

—. *Office of the Director of National Intelligence.* July 31, 2013. http://www.dni.gov/files/documents/2009_CoverLetter_Report_Collection.pdf (accessed July 28, 2014).

Federal Judicial Center. *Federal Judicial Center.* 1967. www.fjc.gov (accessed July 5, 2014).

Feingold, Sen. Russ. *Common Dreams.* September 09, 2009. http://www.commondreams.org/newswire/2009/09/23-8 (accessed July 20, 2014).

Gifis, Steven H. *Law Dictionary.* 6th edition. New York: Barron's Educational Series, Inc., 2010.

Henning, Anna C., Elisabeth B. Bazan, Charles Doyle, and Edward C. Liu. *Government Collection of Privat Information: Background and Issues Related to the USA PATRIOT Act Reauthorization - Kindle Edition.* Washington, DC: Congressional Research Service, 2009.

Ides, Allen, and Christopher N. May. *Constitutional Law - Individual Rights.* 6th Edition. New York: Wolters Kluwer Law & Business, 2013.

In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Amended Memorandum Opinion. BR 13-109 (U.S. Foreign Intelligence Surveillance Court, August 29, 2013).

In Re Application of the FBI for an Order Requiring the Production of Tangible Things - Primary Order. BR 13-80 (U.S. Foreign Intelligence Surveillance Court, April 25, 2013).

Klayman et al. v. Obama et al. - Class Action Amended Complaint. 13-civ-0851 (United States District Court for the District of Columbia, June 10, 2013).

Klayman et al. v. Obama et al. - Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunction. 13-civ-0851 (United States District Court for the District of Columbia, November 12, 2013).

Klayman et al. v. Obama et al. - Memorandum of Points and Authorities in Support of their Motion for Preliminary Injunction. 13-civ-0851 (United States District Court for the District of Columbia, October 28, 2013).

Klayman et al. v. Obama et al. - Memorandum Opinion. 13-civ-0851 (United States District Court for the District of Columbia, December 16, 2013).

Klayman et al. v. Obama et al. - Plaintiffs' Reply in Support of their Motions for Preliminary Injunction. 13-civ-0851 (United States District Court for the District of Columbia, November 14, 2013).

Klayman v. Obama et al. - Complaint. 13-cv-0851 (United States District Court for the District of Columbia, June 6, 2013).

Office of the Law Revision Counsel. *United States Code.* 2014. www.uscode.house.gov (accessed July 5, 2014).

PCLOB. "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court." 2014.

Rosenbach, Eric, and Aki J. Peritz. *Belfer Center for Science and International Affairs - John F. Kennedy School of Government - Harvard University.* July 2001. http://belfercenter.ksg.harvard.edu/publication/19163/usapatriot_act.html (accessed July 20, 2014).

Seifert, Jeffrey W. *Data Mining and Homeland Security: An Overview - Kindle Edition.* Washington, DC: Congressional Research Service, 2007.

Solove, Daniel J., and Paul M. Schwartz. *Information Privacy Law .* New York: Wolters Kluwer Law & Business, 2011.

The Declaration of Independence and The Constitution of the United States (Bantam Classic) [Kindle Edition]. Bantam Classics, 2008.

Under Secretary of Defense for Intelligence. "Manual - DoD Information Security Programm: Marking of Classified Information." *Defense Technical Information Center.* February 24, 2012. http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf (accessed July 7, 2014).

Wyden, Sen. Ron. *Ron Wyden Senator for Oregon.* May 26, 2011. http://www.wyden.senate.gov/news/press-releases/in-speech-wyden-says-official-interpretations-of-patriot-act-must-be-made-public (accessed July 20, 2014).

Yeh, Brian T., and Charles Doyle. *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis - Kindle Edition.* Washington D.C.: Congressional Research Service, 2006.

Annexes

Annex 1 – Summary in German – Zusammenfassung

Gegenstand der Masterthese ist die Analyse zweier sich widersprechender Urteile erstinstanzlicher US-Bundesgerichte über die Zulässigkeit des Sammelns von Telefonmetadaten in den USA, nicht jedoch die Sammlung von Internetdaten außerhalb der USA im Rahmen verschiedener Programme wie ua. „PRISM".

Im Juni 2013 wurden die geheimen Datensammlungsprogramme durch eine Serie von Artikeln im Guardian öffentlich gemacht. Ein Artikel am 5. Juni 2013 enthüllte, dass auf Grund einer richterlichen Verfügung des United States Foreign Intelligence Surveillance Court (FISC) in Washington, DC, auch innerhalb der Vereinigten Staaten Metadaten von Telefongesprächen von den Telefongesellschaften gesammelt und tagesaktuell an die National Security Agency (NSA) weitergeleitet wurden.

Bereits am folgenden Tag erhob L. Klayman, ein konservativer Aktivist und Anwalt, vor dem US District Court for the District of Columbia Klage gegen Präsident Barack Obama, Attorney General Eric H. Holder Jr., den Direktor der NSA Mr. Keith B. Alexander, den Chief Executive Officer von Verizon Communications Mr. Lowell C. McAdam und den Richter des FISC Roger Vinson wegen Verletzung seiner verfassungsmäßig gewährleisteten Rechte insbesondere des ersten (Recht auf freie Meinungsäußerung), des vierten (Schutz der Privatsphäre) und des fünften (due process) Verfassungszusatzartikels[237].

Am 11. Juni 2013 folgte eine Klage der American Civil Liberties Union[238] (ACLU), einer US-amerikanischen Bürgerrechtsgruppe, vor dem United States District Court Southern District of New York, welche sich gegen den Director of National Intelligence James R. Clapper, den Direktor der NSA Keith B Alexander, den US-Verteidigungsminister Charles T. Hagel, den Attorney General Eric H. Holder und den Direktor des FBI Robert S. Mueller III, richtet und sich auf die Verletzung des ersten und des vierten Verfassungszusatzartikels stützt.[239]

Schon bei der Klageerhebung zeigten sich erste Unterschiede. Während L. Klayman in seiner ersten Klage den 1., 4. und 5 Verfassungszusatzartikel verletzt sah, stützte die

[237] (Klayman v Obama et al. - Complaint 2013)
[238] Die ACLU setzt sich vor allem für die Meinungsfreiheit, den Schutz der Privatsphäre und die Trennung von Kirche und Staat ein
[239] ACLU et al v James R. Clapper et al - Complaint 2013

ACLU ihre Klage neben der behaupteten Verletzung des 1. und 4. Zusatzartikels vor allem auf eine nicht gesetzeskonforme Auslegung von 50 USC § 1861[240] und damit eine Verletzung von 5 USC § 706[241]. Die nicht-gesetzeskonforme Auslegung des FISA wurde nachträglich auch von Klayman vorgebracht.

Vergleicht man die Urteile, so stellt man fest, dass beide Gerichte ihre Zuständigkeit hinsichtlich des Klagsteils, welcher sich auf eine Überschreitung der Kompetenzen durch den FISC stützt, zurückweist und sich nur für die Klagsteile zuständig erklärt, welche sich auf eine Verletzung der verfassungsmäßigen Rechte gründen. In seinem Urteil vom 16. Dezember 2013 sieht das Gericht in Washington, DC auch ausreichende Argumente der Klagsseite, dass die Sammlung von Telefonmetadaten nicht verfassungskonform sei. Wegen der weitreichenden Fragen der Nationalen Sicherheit und der Neuheit der verfassungsrechtlichen Fragen wurde die Durchsetzung der „Preliminary Injunction" vom Ausgang eines allfälligen Berufungsverfahrens abhängig gemacht.[242]

Am 27. Dezember 2013 erklärte das New Yorker Gericht hingegen die Sammlung der Metadaten für zulässig. Begründet wird dies unter anderem damit, dass der Schutz des vierten Zusatzartikels kein grenzenloser wäre und die Beurteilung der Frage, ob die gegenständlichen Daten durch diesen Artikel geschützt werden, eine Frage der Verhältnismäßigkeit sei, welche laufend durch die Verwaltung, den Kongress und auch den FISC überprüft wird.

Die widersprüchlichen Urteile lassen sich auf eine unterschiedliche Auslegung der Frage zurück führen, ob die Sammlung der Daten und die erste, automatisierte Sichtung der Daten, welche zu diesem Zeitpunkt keinerlei Rückschlüsse auf Personen zulassen, eine „Search" im Sinne des 4. Verfassungszusatzartikels darstellen.

[240] 50 USC § 1861: War and National Defense – Chapter 36 Foreign Intelligence Surveillance – Subchapter IV – Access to certain business records for foreign intelligence purposes – Access to certain business records for foreign intelligence and international terrorism investigations
[241] 5 USC § 706: Government Organization and Employees – The Agencies Generally – Judicial Review – Scope of review
[242] in Klayman ist noch kein Urteil ergangen, gegen die Gewährung der "Preliminary Injunction" läuft derzeit eine Berufung; die Berufung in ACLU ist noch nicht entschieden.

Annex 2 – Cases

Andresen v Maryland, 427 U.S. 463 (1976)

Bland et al. v. Roberts Case 4:11-cv-00045-RAJ-TEM E.D.Va

Bland et al v. Roberts US Court of Appeals fort he Fourth Circuit No 12-1671

Bowles v. Willingham, 321 Z.S. 503, 521 (1944)

City of Ladue v. Gilleo, 512 U.S. 43 (1994)

Couch v. United States, 409 U.S. 322 (1973)

Country of Sacramento v. Lewis, 523 U.S. 833, 846 (1998)

DeShaney v. Winnebago County Dept. of Social Servs., 489 U.S. (1989)

Fisher v. United States, 425 U.S. 391 (1976)

Gouled v. United States 255 U.S. 298, (1921)

Katz v. United States 389 U.S. 347 (1967)

Murray's Lessee v. Hoboken Land & Improvement Co., 59 U.S. (18 How.) 272 (1856)

Reno v. ACLU, 521 U.S. 844 (1997)

Smith v. Maryland, 442 U.S. 735 (1979)

United States v. Jones, 132 S. Ct. 945 (2012)

United States v. Knotts, 460 U.S. 286 (1983)

United States v. U.S. District Court, 407 U.S. 297 (1972)

Wolff v. McDonnell, 418 U.S. 539, 558 (1974)

Annex 3 – List of Law Professors as Amici Curiae Supporting Plaintiff ACLU

- W. David Ball – Assistant Professor, Santa Clara Law
- William C. Banks – Board of Advisors Distinguished Professor and Professor of Law, Syracuse University College of Law
- Annemarie Bridy – Associate professor, University of Idaho
- Brian Carver – Assistant Professor, University of California, Berkley
- Fred H. Cate – Distinguished Professor and C. Ben Duton Professor of Law at Indiana University, Maurer School of Law
- Erwin Chemerinsky – founding Dean, Distinguished Professor of Law, and Raymond Pryke Professor of First Amendment Law, University of California, Irvine, School of Law
- Ralph D. Clifford – Professor of Law at the University of Massachusetts School of Law
- Julie Cohen – Professor of Law, Georgetown Law
- Laura K. Donohue – Professor of Law, Georgetown University Law Center
- Susan Freiwald – Professor of Law, University of San Francisco School of Law
- Michael Froomkin Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law, University of Miami School of Law
- Ahmed Ghappour – Clinical Instructor of Law in the Civil Rights Clinic and Director of National Security Defense Project, University of Texas School of Law
- Shubha Ghosh – Vilas Research Fellow & Professor of Law, University of Wisconsin Law School
- Jennifer Stisa Granick – Director of Civil Liberties at the Stanford Center for Internet and Society
- Robert A. Heverly – Associate Professor and Interim Director of the Government Law Center, Albany Law School of Union University
- Anne Klinefelter – Director of the Law Library and Associate Professor of Law, University of North Carolina
- Edward Lee – Professor of Law and Director of the Program in Intellectual Property Law, Norman and Edna Freehling Scholar, IIT Chicago-Kent College of Law
- Mark A. Lemley – William H. Neukom Professor, Stanford Law School
- David Levine – Associate Professor of Law, Elon University School of Law
- Karl Manheim – Professor of Law, Loyola Law School, Los Angeles
- Ranjana Natarajan – Clinical Professor at the University of Texas School of Law
- Ira Steven Nathenson – Associate Professor of Law, St. Thomas University School of Law
- David W. Opderbeck – Professor of Law, Seton Hall University Law School
- Peter Raven-Hansen – Glen Earl Westen Research Professor of Law, George Washington University Law School
- Kim Lane Scheppele – Rockefeller Professor of International Affairs, Woodrow Wilson School and Director of the Program in Law and Public Affairs, Princeton University
- Jessica Silbey – Professor of Law, Suffolk University Law School
- Katherine J. Strandburg – Alfred B. Engelberg Professor of Law, New York University School of Law

- Sephen I. Vladeck – Professor of Law and Associate Dean for Scholarship, American University Washington College of Law
- Jonathan Weinberg – Professor of Law, Wayne State University

Annex 4 – Development of 50 U.S.C § 1861

Original Text as of USA PATRIOT Act – black

Text as amended by the USA PATRIOT Improvement and Reauthorization Act of 2005 – red

Text as amended by the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 – green

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

''SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

''(a)(1) ~~The~~ Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

''(2) An investigation conducted under this section shall—

''(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

''(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

''(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.''

''(b) Each application under this section—

''(1) shall be made to—

''(A) a judge of the court established by section 103(a); or

''(B) a United States Magistrate Judge under chapter 43 of title 28, United

States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

''(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. shall include–

''(A) a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to—

''(i) a foreign power or an agent of a foreign power;

''(ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

''(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation; and

''(B) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.''.

''(c)(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b), the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) be followed ~~records if the judge finds that the application meets the requirements of this section~~.

''(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a). An order under this subsection— ''(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified;

''(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

''(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d);

''(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States

in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things; and

''(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a).''.

''(d) (1) No person shall disclose to any other person ~~(other than those persons necessary to produce the tangible things under this section)~~ that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section, other than to–

''(A) those persons to whom disclosure is necessary to comply with such order;

''(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the order; or

''(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

''(2)(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom an order is directed under this section in the same manner as such person.

''(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section shall notify such person of the nondisclosure requirements of this subsection.

''(C) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under ~~this section~~ subparagraph (A) or (C) of paragraph (1) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request~~, but in no circumstance shall a person be required to inform the Director or such designee that the person intends to consult an attorney to obtain legal advice or legal assistance~~.''

''(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

''(f)(1) In this subsection–

"(A) the term "production order" means an order to produce any tangible thing under this section; and

(B) the term "nondisclosure order" means an order imposed under subsection (d).

"(2)(A)(i) A person receiving a~~n~~ production order ~~to produce any tangible thing under this section~~ may challenge the legality of that order by filing a petition with the pool established by section 103(e)(1). Not less than 1 year after the date of the issuance of the production order, the recipient of a pro-

duction order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by section 103(e)(1).

"(ii) The presiding judge shall immediately assign ~~the~~ a petition under clause (i) to one of the judges serving in ~~such~~ the pool established by section 103(e)(1). Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the production order or nondisclosure order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established ~~pursuant to~~ under section 103(e)(2).

"(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

"(B) A ~~The~~ judge considering ~~the~~ a petition ~~may~~ to modify or set aside ~~the~~ a production order may grant such petition ~~order~~ only if the judge finds that ~~the~~ such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm ~~the~~ such order, and order the recipient to comply therewith. ~~The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this paragraph~~.

"(C)(i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

"(ii) If upon filing of such a petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive, unless the judge finds that the certification was made in bad faith.

(iii) If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing another such petition with respect to such nondisclosure order.

"(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect.

''(~~2~~3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the ~~United States~~ Government or any person receiving such order shall be made to the court of review established under sec-

tion 103(b), which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition of the ~~United States~~ Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

''(~~3~~4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the Director of National Intelligence.

''(45) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.''

''(g) MINIMIZATION PROCEDURES.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, the Attorney General shall adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this title.

''(2) DEFINED.—In this section, the term 'minimization procedures' means—

''(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

''(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 101(e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and

''(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

''(h) USE OF INFORMATION.—Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States

person only in accordance with the minimization procedures adopted pursuant to subsection (g). No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this title shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this title may be used or disclosed by Federal officers or employees except for lawful purposes.''

Annex 5 – Rule 11

Rule 11. Notice and Briefing of Novel Issues.

(a) Notice to the Court. If a submission by the government for Court action involves an issue not previously presented to the Court – including, but not limited to, a novel issue of technology or law – the government must inform the Court in writing of the nature and significance of that issue.

(b) Submission Relating to New Techniques. Prior to requesting authorization to use a new surveillance or search technique, the government must submit a memorandum to the Court that:

(1) explains the technique;

(2) describes the circumstances of the likely implementation of the technique;

(3) discusses any legal issues apparently raised; and

(4) describes the proposed minimization procedures to be applied.

At the latest, the memorandum must be submitted as part of the first proposed application or other submission that seeks to employ the new technique.

(c) Novel Implementation. When requesting authorization to use an existing surveillance or search technique in a novel context, the government must identify and address any new minimization or other issues in a written submission made, at the latest, as part of the application or other filing seeking such authorization.

(d) Legal Memorandum. If an application or other request for action raises an issue of law not previously considered by the Court, the government must file a memorandum of law in support of its position on each new issue. At the latest, the memorandum must be submitted as part of the first proposed application or other submission that raises the issue.

Appendices - Text of US Acts

all texts saved as pdf from the website www.uscode.house.gov, date of the download in upper right hand corner

5 U.S.C. § 706

5 USC 706: Scope of review
Text contains those laws in effect on August 12, 2014

From Title 5-GOVERNMENT ORGANIZATION AND EMPLOYEES
PART I-THE AGENCIES GENERALLY
CHAPTER 7-JUDICIAL REVIEW
Jump To:
Source Credit
Miscellaneous

§706. Scope of review

To the extent necessary to decision and when presented, the reviewing court shall decide all relevant questions of law, interpret constitutional and statutory provisions, and determine the meaning or applicability of the terms of an agency action. The reviewing court shall-

(1) compel agency action unlawfully withheld or unreasonably delayed; and
(2) hold unlawful and set aside agency action, findings, and conclusions found to be-
(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;
(B) contrary to constitutional right, power, privilege, or immunity;
(C) in excess of statutory jurisdiction, authority, or limitations, or short of statutory right;
(D) without observance of procedure required by law;
(E) unsupported by substantial evidence in a case subject to sections 556 and 557 of this title or otherwise reviewed on the record of an agency hearing provided by statute; or
(F) unwarranted by the facts to the extent that the facts are subject to trial de novo by the reviewing court.

In making the foregoing determinations, the court shall review the whole record or those parts of it cited by a party, and due account shall be taken of the rule of prejudicial error.

(Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 393 .)

HISTORICAL AND REVISION NOTES

Derivation	*U.S. Code*	*Revised Statutes and Statutes at Large*
	5 U.S.C. 1009(e).	June 11, 1946, ch. 324, §10(e), 60 Stat. 243.

Standard changes are made to conform with the definitions applicable and the style of this title as outlined in the preface of this report.

ABBREVIATION OF RECORD

Pub. L. 85–791, Aug. 28, 1958, 72 Stat. 941 , which authorized abbreviation of record on review or enforcement of orders of administrative agencies and review on the original papers, provided, in section 35 thereof, that: "This Act [see Tables for classification] shall not be construed to repeal or modify any provision of the Administrative Procedure Act [see Short Title note set out preceding section 551 of this title]."

18 U.S.C. § 2510

18 USC 2510: Definitions
Text contains those laws in effect on July 6, 2014

From Title 18-CRIMES AND CRIMINAL PROCEDURE
PART I-CRIMES
CHAPTER 119-WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Jump To:

§2510. Definitions

As used in this chapter-

(1) “wire communication” means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) “oral communication” means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.[1]

(5) “electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than-

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) “person” means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) “Investigative or law enforcement officer” means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) “Judge of competent jurisdiction” means-

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) “communication common carrier” has the meaning given that term in section 3 of the Communications Act of 1934;

(11) “aggrieved person” means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include-

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) “user” means any person or entity who-

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not-

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) “electronic storage” means-

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) “aural transfer” means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) “foreign intelligence information”, for purposes of section 2517(6) of this title, means-

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against-

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to-

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) “protected computer” has the meaning set forth in section 1030; and

(21) “computer trespasser”-

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or

part of the protected computer.

(Added Pub. L. 90–351, title III, §802, June 19, 1968, 82 Stat. 212; amended Pub. L. 99–508, title I, §101(a), (c)(1)(A), (4), Oct. 21, 1986, 100 Stat. 1848, 1851; Pub. L. 103–414, title II, §§202(a), 203, Oct. 25, 1994, 108 Stat. 4290, 4291; Pub. L. 104–132, title VII, §731, Apr. 24, 1996, 110 Stat. 1303; Pub. L. 107–56, title II, §§203(b)(2), 209(1), 217(1), Oct. 26, 2001, 115 Stat. 280, 283, 290; Pub. L. 107–108, title III, §314(b), Dec. 28, 2001, 115 Stat. 1402; Pub. L. 107–273, div. B, title IV, §4002(e)(10), Nov. 2, 2002, 116 Stat. 1810.)

References in Text

Section 3 of the Communications Act of 1934, referred to in par. (10), is classified to section 153 of Title 47, Telecommunications.

Amendments

2002-Par. (10). Pub. L. 107–273 substituted “has the meaning given that term in section 3 of the Communications Act of 1934;” for “shall have the same meaning which is given the term ‘common carrier’ by section 153(h) of title 47 of the United States Code;”.

2001-Par. (1). Pub. L. 107–56, §209(1)(A), struck out “and such term includes any electronic storage of such communication” before semicolon at end.

Par. (14). Pub. L. 107–56, §209(1)(B), inserted “wire or” after “transmission of”.

Par. (19). Pub. L. 107–108 inserted “, for purposes of section 2517(6) of this title,” before “means” in introductory provisions.

Pub. L. 107–56, §203(b)(2), added par. (19).

Pars. (20), (21). Pub. L. 107–56, §217(1), added pars. (20) and (21).

1996-Par. (12)(D). Pub. L. 104–132, §731(1), added subpar. (D).

Par. (16)(F). Pub. L. 104–132, §731(2), struck out subpar. (F) which read as follows: “an electronic communication;”.

1994-Par. (1). Pub. L. 103–414, §202(a)(1), struck out before semicolon at end “, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit”.

Par. (12). Pub. L. 103–414, §202(a)(2), redesignated subpars. (B) to (D) as (A) to (C), respectively, and struck out former subpar. (A) which read as follows: “the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;”.

Par. (16)(F). Pub. L. 103–414, §203, added subpar. (F).

1986-Par. (1). Pub. L. 99–508, §101(a)(1), substituted “any aural transfer” for “any communication”, inserted “(including the use of such connection in a switching station)” after “reception”, struck out “as a common carrier” after “person engaged”, and inserted “or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit” before the semicolon at end.

Par. (2). Pub. L. 99–508, §101(a)(2), inserted “, but such term does not include any electronic communication” before the semicolon at end.

Par. (4). Pub. L. 99–508, §101(a)(3), inserted “or other” after “aural” and “, electronic,” after “wire”.

Par. (5). Pub. L. 99–508, §101(a)(4), (c)(1)(A), (4), substituted “wire, oral, or electronic” for “wire or oral” in introductory provisions, substituted “provider of wire or electronic communication service” for “communications common carrier” in subpars. (a)(i) and (ii), and inserted “or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business” before the semicolon in subpar. (a)(i).

Par. (8). Pub. L. 99–508, §101(a)(5), (c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral” and struck out “identity of the parties to such communication or the existence,” after “concerning the”.

Pars. (9)(b), (11). Pub. L. 99–508, §101(c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral”.

Pars. (12) to (18). Pub. L. 99–508, §101(a)(6), added pars. (12) to (18).

Termination Date of 2001 Amendment

Pub. L. 107–56, title II, §224, Oct. 26, 2001, 115 Stat. 295, as amended by Pub. L. 109–160, §1, Dec. 30, 2005, 119 Stat. 2957; Pub. L. 109–170, §1, Feb. 3, 2006, 120 Stat. 3, which provided that title II of Pub. L. 107–56 and the amendments made by that title would cease to have effect on Mar. 10, 2006, with certain exceptions, was repealed by Pub. L. 109–177, title I, §102(a), Mar. 9, 2006, 120 Stat. 194.

Effective Date of 1986 Amendment

Pub. L. 99–508, title I, §111, Oct. 21, 1986, 100 Stat. 1859, provided that:

"(a) In General.-Except as provided in subsection (b) or (c), this title and the amendments made by this title [enacting sections 2521 and 3117 of this title, amending this section and sections 2232, 2511 to 2513, and 2516 to 2520 of this title, and enacting provisions set out as notes under this section] shall take effect 90 days after the date of the enactment of this Act [Oct. 21, 1986] and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

"(b) Special Rule for State Authorizations of Interceptions-Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of-

"(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended; or

"(2) the date two years after the date of the enactment of this Act [Oct. 21, 1986].

"(c) Effective Date for Certain Approvals by Justice Department Officials-Section 104 of this Act [amending section 2516 of this title] shall take effect on the date of enactment of this Act [Oct. 21, 1986]."

Short Title of 1997 Amendment

Pub. L. 105–112, §1, Nov. 21, 1997, 111 Stat. 2273, provided that: "This Act [amending section 2512 of this title] may be cited as the 'Law Enforcement Technology Advertisement Clarification Act of 1997'."

Short Title of 1986 Amendment

Pub. L. 99–508, §1, Oct. 21, 1986, 100 Stat. 1848, provided that: "This Act [enacting sections 1367, 2521, 2701 to 2710, 3117, and 3121 to 3126 of this title, amending sections 2232, 2511 to 2513, and 2516 to 2520 of this title, and enacting provisions set out as notes under this section and sections 2701 and 3121 of this title] may be cited as the 'Electronic Communications Privacy Act of 1986'."

Intelligence Activities

Pub. L. 99–508, title I, §107, Oct. 21, 1986, 100 Stat. 1858, provided that:

"(a) In General.-Nothing in this Act or the amendments made by this Act [see Short Title of 1986 Amendment note above] constitutes authority for the conduct of any intelligence activity.

"(b) Certain Activities Under Procedures Approved by the Attorney General.-Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to-

"(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

"(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. 1801 et seq.]; or

"(3) access an electronic communication system used exclusively by a foreign power or

agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978."

Congressional Findings

Pub. L. 90–351, title III, §801, June 19, 1968, 82 Stat. 211, provided that: "On the basis of its own investigations and of published studies, the Congress makes the following findings:

"(a) Wire communications are normally conducted through the use of facilities which form part of an interstate network. The same facilities are used for interstate and intrastate communications. There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. The contents of these communications and evidence derived therefrom are being used by public and private parties as evidence in court and administrative proceedings, and by persons whose activities affect interstate commerce. The possession, manufacture, distribution, advertising, and use of these devices are facilitated by interstate commerce.

"(b) In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

"(c) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

"(d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused."

National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance

Pub. L. 90–351, title III, §804, June 19, 1968, 82 Stat. 223, as amended by Pub. L. 91–452, title XII, §1212, Oct. 15, 1970, 84 Stat. 961; Pub. L. 91–644, title VI, §20, Jan. 2, 1971, 84 Stat. 1892; Pub. L. 93–609, §§1–4, Jan. 2, 1975, 88 Stat. 1972, 1973; Pub. L. 94–176, Dec. 23, 1975, 89 Stat. 1031, established a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, provided for its membership, Chairman, powers and functions, compensation and allowances, required the Commission to study and review the operation of the provisions of this chapter to determine their effectiveness and to submit interim reports and a final report to the President and to the Congress of its findings and recommendations on or before Apr. 30, 1976, and also provided for its termination sixty days after submission of the final report.

[1] *So in original. The period probably should be a semicolon.*

18 U.S.C. § 2702

18 USC 2702: Voluntary disclosure of customer communications or records
Text contains those laws in effect on July 4, 2014

From Title 18-CRIMES AND CRIMINAL PROCEDURE
PART I-CRIMES
CHAPTER 121-STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS
Jump To:

§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.

(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

[(B) Repealed. Pub. L. 108–21, title V, §508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(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 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; 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); and

(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.

(Added Pub. L. 99–508, title II, §201[(a)], Oct. 21, 1986, 100 Stat. 1860; amended Pub. L. 100–690, title VII, §7037, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 105–314, title VI, §604(b), Oct. 30, 1998, 112 Stat. 2984; Pub. L. 107–56, title II, §212(a)(1), Oct. 26, 2001, 115 Stat. 284; Pub. L. 107–296, title II, §225(d)(1), Nov. 25, 2002, 116 Stat. 2157; Pub. L. 108–21, title V, §508(b), Apr. 30, 2003, 117 Stat. 684; Pub. L. 109–177, title I, §107(a), (b)(1), (c), Mar. 9, 2006, 120 Stat. 202, 203; Pub. L. 110–401, title V, §501(b)(2), Oct. 13, 2008, 122 Stat. 4251.)

Amendments

2008-Subsecs. (b)(6), (c)(5). Pub. L. 110–401 substituted “section 2258A” for “section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032)”.

2006-Subsec. (a). Pub. L. 109–177, §107(c), inserted “or (c)” after “Except as provided in subsection (b)”.

Subsec. (b)(8). Pub. L. 109–177, §107(b)(1)(A), struck out “Federal, State, or local” before “governmental entity”.

Subsec. (c)(4). Pub. L. 109–177, §107(b)(1)(B), added par. (4) and struck out former par. (4) which read as follows: “to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;”.

Subsec. (d). Pub. L. 109–177, §107(a), added subsec. (d).

2003-Subsec. (b)(5). Pub. L. 108–21, §508(b)(1)(C), which directed amendment of par. (5) by striking “or” at the end, could not be executed because “or” did not appear at the end. See 2002 Amendment note below.

Subsec. (b)(6). Pub. L. 108–21, §508(b)(1)(D), added par. (6). Former par. (6) redesignated (7).

Subsec. (b)(6)(B). Pub. L. 108–21, §508(b)(1)(A), struck out subpar. (B) which read as follows: “if required by section 227 of the Crime Control Act of 1990; or”.

Subsec. (b)(7), (8). Pub. L. 108–21, §508(b)(1)(B), redesignated pars. (6) and (7) as (7) and (8), respectively.

Subsec. (c)(5), (6). Pub. L. 108–21, §508(b)(2), added par. (5) and redesignated former par. (5) as (6).

2002-Subsec. (b)(5). Pub. L. 107–296, §225(d)(1)(A), struck out “or” at end.

Subsec. (b)(6)(A). Pub. L. 107–296, §225(d)(1)(B), inserted “or” at end.

Subsec. (b)(6)(C). Pub. L. 107–296, §225(d)(1)(C), struck out subpar. (C) which read as follows: “if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.”

Subsec. (b)(7). Pub. L. 107–296, §225(d)(1)(D), added par. (7).

2001-Pub. L. 107–56, §212(a)(1)(A), substituted “Voluntary disclosure of customer communications or records” for “Disclosure of contents” in section catchline.

Subsec. (a)(3). Pub. L. 107–56, §212(a)(1)(B), added par. (3).

Subsec. (b). Pub. L. 107–56, §212(a)(1)(C), substituted “Exceptions for disclosure of communications” for “Exceptions” in heading and “A provider described in subsection (a)” for “A person or entity” in introductory provisions.

Subsec. (b)(6)(C). Pub. L. 107–56, §212(a)(1)(D), added subpar. (C).

Subsec. (c). Pub. L. 107–56, §212(a)(1)(E), added subsec. (c).

1998-Subsec. (b)(6). Pub. L. 105–314 amended par. (6) generally. Prior to amendment, par. (6) read as follows: “to a law enforcement agency, if such contents-

“(A) were inadvertently obtained by the service provider; and

“(B) appear to pertain to the commission of a crime.”

1988-Subsec. (b)(2). Pub. L. 100–690 substituted “2517” for “2516”.

Effective Date of 2002 Amendment

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

18 U.S.C. § 2703

18 USC 2703: Required disclosure of customer communications or records
Text contains those laws in effect on July 5, 2014

From Title 18-CRIMES AND CRIMINAL PROCEDURE
PART I-CRIMES
CHAPTER 121-STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Jump To:

§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.

(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.

(Added Pub. L. 99–508, title II, §201[(a)], Oct. 21, 1986, 100 Stat. 1861; amended Pub. L. 100–690, title VII, §§7038, 7039, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 103–322, title XXXIII, §330003(b), Sept. 13, 1994, 108 Stat. 2140; Pub. L. 103–414, title II, §207(a), Oct. 25, 1994, 108 Stat. 4292; Pub. L. 104–132, title VIII, §804, Apr. 24, 1996, 110 Stat. 1305; Pub. L. 104–293, title VI, §601(b), Oct. 11, 1996, 110 Stat. 3469; Pub. L. 104–294, title VI, §605(f), Oct. 11, 1996, 110 Stat. 3510; Pub. L. 105–184, §8, June 23, 1998, 112 Stat. 522; Pub. L. 107–56, title II, §§209(2), 210, 212(b)(1), 220(a)(1), (b), Oct. 26, 2001, 115 Stat. 283, 285, 291, 292; Pub. L. 107–273, div. B, title IV, §4005(a)(2), div. C, title I, §11010, Nov. 2, 2002, 116 Stat. 1812, 1822; Pub. L. 107–296, title II, §225(h)(1), Nov. 25, 2002, 116 Stat. 2158; Pub. L. 109–162, title XI, §1171(a)(1), Jan. 5, 2006, 119 Stat. 3123; Pub. L. 111–79, §2(1), Oct. 19, 2009, 123 Stat. 2086.)

References in Text

The Federal Rules of Criminal Procedure, referred to in subsecs. (a), (b)(1)(A), and (c)(1)(B)(i), are set out in the Appendix to this title.

Amendments

2009-Subsecs. (a), (b)(1)(A), (c)(1)(A). Pub. L. 111–79, which directed substitution of "(or, in the case of a State court, issued using State warrant procedures) by a court of competent

jurisdiction" for "by a court with jurisdiction over the offense under investigation or an equivalent State warrant", was executed by making the substitution for "by a court with jurisdiction over the offense under investigation or equivalent State warrant" to reflect the probable intent of Congress.

2006-Subsec. (c)(1)(C). Pub. L. 109–162 struck out "or" at end.

2002-Subsec. (c)(1)(E). Pub. L. 107–273, §4005(a)(2), realigned margins.

Subsec. (e). Pub. L. 107–296 inserted ", statutory authorization" after "subpoena".

Subsec. (g). Pub. L. 107–273, §11010, added subsec. (g).

2001-Pub. L. 107–56, §212(b)(1)(A), substituted "Required disclosure of customer communications or records" for "Requirements for governmental access" in section catchline.

Subsec. (a). Pub. L. 107–56, §§209(2)(A), (B), 220(a)(1), substituted "Contents of Wire or Electronic" for "Contents of Electronic" in heading and "contents of a wire or electronic" for "contents of an electronic" in two places and "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in text.

Subsec. (b). Pub. L. 107–56, §209(2)(A), substituted "Contents of Wire or Electronic" for "Contents of Electronic" in heading.

Subsec. (b)(1). Pub. L. 107–56, §§209(2)(C), 220(a)(1), substituted "any wire or electronic communication" for "any electronic communication" in introductory provisions and "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in subpar. (A).

Subsec. (b)(2). Pub. L. 107–56, §209(2)(C), substituted "any wire or electronic communication" for "any electronic communication" in introductory provisions.

Subsec. (c)(1). Pub. L. 107–56, §§212(b)(1)(C), 220(a)(1), designated subpar. (A) and introductory provisions of subpar. (B) as par. (1), substituted "A governmental entity may require a provider of electronic communication service or remote computing service to" for "(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may" and a closing parenthesis for provisions which began with "covered by subsection (a) or (b) of this section) to any person other than a governmental entity." in former subpar. (A) and ended with "(B) A provider of electronic communication service or remote computing service shall disclose 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) or (b) of this section) to a governmental entity", redesignated clauses (i) to (iv) of former subpar. (B) as subpars. (A) to (D), respectively, substituted "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in subpar. (A) and "; or" for period at end of subpar. (D), added subpar. (E), and redesignated former subpar. (C) as par. (2).

Subsec. (c)(2). Pub. L. 107–56, §210, amended par. (2), as redesignated by section 212 of Pub. L. 107–56, by substituting "entity the-" for "entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber" in introductory provisions, inserting subpars. (A) to (F), striking out "and the types of services the subscriber or customer utilized," before "when the governmental entity uses an administrative subpoena", inserting "of a subscriber" at beginning of concluding provisions and designating "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)." as remainder of concluding provisions.

Pub. L. 107–56, §212(b)(1)(C)(iii), (D), redesignated subpar. (C) of par. (1) as par. (2) and temporarily substituted "paragraph (1)" for "subparagraph (B)".

Pub. L. 107–56, §212(b)(1)(B), redesignated par. (2) as (3).

Subsec. (c)(3). Pub. L. 107–56, §212(b)(1)(B), redesignated par. (2) as (3).

Subsec. (d). Pub. L. 107–56, §220(b), struck out "described in section 3127(2)(A)" after "court of competent jurisdiction".

1998-Subsec. (c)(1)(B)(iv). Pub. L. 105–184 added cl. (iv).

1996-Subsec. (c)(1)(C). Pub. L. 104–293 inserted “local and long distance” after “address,”.

Subsec. (d). Pub. L. 104–294 substituted “in section 3127(2)(A)” for “in section 3126(2)(A)”.

Subsec. (f). Pub. L. 104–132 added subsec. (f).

1994-Subsec. (c)(1)(B). Pub. L. 103–414, §207(a)(1)(A), redesignated cls. (ii) to (iv) as (i) to (iii), respectively, and struck out former cl. (i) which read as follows: “uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury or trial subpoena;”.

Subsec. (c)(1)(C). Pub. L. 103–414, §207(a)(1)(B), added subpar. (C).

Subsec. (d). Pub. L. 103–414, §207(a)(2), amended first sentence generally. Prior to amendment, first sentence read as follows: “A court order for disclosure under subsection (b) or (c) of this section may be issued by any court that is a court of competent jurisdiction set forth in section 3127(2)(A) of this title and shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry.”

Pub. L. 103–322 substituted “section 3127(2)(A)” for “section 3126(2)(A)”.

1988-Subsecs. (b)(1)(B)(i), (c)(1)(B)(i). Pub. L. 100–690, §7038, inserted “or trial” after “grand jury”.

Subsec. (d). Pub. L. 100–690, §7039, inserted “may be issued by any court that is a court of competent jurisdiction set forth in section 3126(2)(A) of this title and” before “shall issue”.

Effective Date of 2002 Amendment

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

18 U.S.C § 2709

18 USC 2709: Counterintelligence access to telephone toll and transactional records
Text contains those laws in effect on July 5, 2014

From Title 18-CRIMES AND CRIMINAL PROCEDURE
PART I-CRIMES
CHAPTER 121-STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Jump To:
Source Credit
Amendments

§2709. Counterintelligence access to telephone toll and transactional records

(a) DUTY TO PROVIDE.-A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.-The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may-

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) PROHIBITION OF CERTAIN DISCLOSURE.-

(1) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such person of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).

(d) DISSEMINATION BY BUREAU.-The Federal Bureau of Investigation may disseminate information and records

obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.-On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(f) LIBRARIES.-A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title.

(Added Pub. L. 99–508, title II, §201[(a)], Oct. 21, 1986, 100 Stat. 1867; amended Pub. L. 103–142, Nov. 17, 1993, 107 Stat. 1491; Pub. L. 104–293, title VI, §601(a), Oct. 11, 1996, 110 Stat. 3469; Pub. L. 107–56, title V, §505(a), Oct. 26, 2001, 115 Stat. 365; Pub. L. 109–177, title I, §116(a), Mar. 9, 2006, 120 Stat. 213; Pub. L. 109–178, §§4(b), 5, Mar. 9, 2006, 120 Stat. 280, 281.)

AMENDMENTS

2006-Subsec. (c). Pub. L. 109–177 reenacted heading without change and amended text generally. Prior to amendment, text read as follows: "No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."

Subsec. (c)(4). Pub. L. 109–178, §4(b), amended par. (4) generally. Prior to amendment, par. (4) read as follows: "At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, but in no circumstance shall a person be required to inform the Director or such designee that the person intends to consult an attorney to obtain legal advice or legal assistance."

Subsec. (f). Pub. L. 109–178, §5, added subsec. (f).

2001-Subsec. (b). Pub. L. 107–56, §505(a)(1), inserted "at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director" after "Deputy Assistant Director" in introductory provisions.

Subsec. (b)(1). Pub. L. 107–56, §505(a)(2), struck out "in a position not lower than Deputy Assistant Director" after "(or his designee" and substituted "made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and" for "made that-

"(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

"(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and".

Subsec. (b)(2). Pub. L. 107–56, §505(a)(3), struck out "in a position not lower than Deputy Assistant Director" after "(or his designee" and substituted "made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States." for "made that-

"(A) the information sought is relevant to an authorized foreign counterintelligence

investigation; and

"(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with-

"(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

"(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States."

1996-Subsec. (b)(1). Pub. L. 104–293 inserted "local and long distance" before "toll billing records".

1993-Subsec. (b). Pub. L. 103–142, §1, amended subsec. (b) generally. Prior to amendment, subsec. (b) read as follows: "REQUIRED CERTIFICATION.-The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that-

"(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

"(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)."

Subsec. (e). Pub. L. 103–142, §2, inserted ", and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate," after "Senate".

50 U.S.C. § 1861

50 USC 1861: Access to certain business records for foreign intelligence and international terrorism investigations
Text contains those laws in effect on July 5, 2014

From Title 50-WAR AND NATIONAL DEFENSE
CHAPTER 36-FOREIGN INTELLIGENCE SURVEILLANCE
SUBCHAPTER IV-ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES

Jump To:

§1861. Access to certain business records for foreign intelligence and international terrorism investigations

(a) Application for order; conduct of investigation generally

(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall-

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Recipient and contents of application

Each application under this section-

(1) shall be made to-

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall include-

(A) a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to-

(i) a foreign power or an agent of a foreign power;

(ii) the activities of a suspected agent of a foreign power who is the subject of such authorized

investigation; or

(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation; and

(B) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

(c) Ex parte judicial order of approval

(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b), the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) be followed.

(2) An order under this subsection-

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified;

(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d);

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things; and

(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a).

(d) Nondisclosure

(1) No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section, other than to-

(A) those persons to whom disclosure is necessary to comply with such order;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the order; or

(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(2)(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom an order is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section shall notify such person of the nondisclosure requirements of this subsection.

(C) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under subparagraph (A) or (C) of paragraph (1) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(e) Liability for good faith disclosure; waiver

A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

(f) Judicial review of FISA orders

(1) In this subsection-

(A) the term “production order” means an order to produce any tangible thing under this section; and

(B) the term “nondisclosure order” means an order imposed under subsection (d).

(2)(A)(i) A person receiving a production order may challenge the legality of that order by filing a petition with the pool established by section 1803(e)(1) of this title. Not less than 1 year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by section 1803(e)(1) of this

title.

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by section 1803(e)(1) of this title. Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the production order or nondisclosure order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established under section 1803(e)(2) of this title.

(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

(B) A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm such order, and order the recipient to comply therewith.

(C)(i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

(ii) If, upon filing of such a petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive, unless the judge finds that the certification was made in bad faith.

(iii) If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing another such petition with respect to such nondisclosure order.

(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect.

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 1803(b) of this title, which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(5) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.

(g) Minimization procedures

(1) In general

Not later than 180 days after March 9, 2006, the Attorney General shall adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this subchapter.

(2) Defined

In this section, the term “minimization procedures” means-

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

(h) Use of information

Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (g). No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this subchapter shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(Pub. L. 95–511, title V, §501, as added Pub. L. 107–56, title II, §215, Oct. 26, 2001, 115 Stat. 287; amended Pub. L. 107–108, title III, §314(a)(6), Dec. 28, 2001, 115 Stat. 1402; Pub. L. 109–177, title I, §§102(b)(1), 106(a)–(e), (f)(2), (g), Mar. 9, 2006, 120 Stat. 195–198; Pub. L. 109–178, §§3, 4(a), Mar. 9, 2006, 120 Stat. 278, 280; Pub. L. 111–118, div. B, §1004(a), Dec. 19, 2009, 123 Stat. 3470; Pub. L. 111–141, §1(a), Feb. 27, 2010, 124 Stat. 37; Pub. L. 112–3, §2(a), Feb. 25, 2011, 125 Stat. 5; Pub. L. 112–14, §2(a), May 26, 2011, 125 Stat. 216.)

Amendment of Section

Pub. L. 109–177, title I, §102(b), Mar. 9, 2006, 120 Stat. 195, as amended by Pub. L. 111–118, div. B, §1004(a), Dec. 19, 2009, 123 Stat. 3470; Pub. L. 111–141, §1(a), Feb. 27, 2010, 124 Stat. 37; Pub. L. 112–3, §2(a), Feb. 25, 2011, 125 Stat. 5; Pub. L. 112–14, §2(a), May 26, 2011, 125 Stat. 216, provided that, effective June 1, 2015, with certain exceptions, this section is amended to read as it read on Oct. 25, 2001:

§1861. Definitions

As used in this subchapter:

(1) The terms "foreign power", "agent of a foreign power", "foreign intelligence information", "international terrorism", and "Attorney General" shall have the same meanings as in section 1801 of this title.

(2) The term "common carrier" means any person or entity transporting people or property by land, rail, water, or air for compensation.

(3) The term "physical storage facility" means any business or entity that provides space for the storage of goods or materials, or services related to the storage of goods or materials, to the public or any segment thereof.

(4) The term "public accommodation facility" means any inn, hotel, motel, or other establishment that provides lodging to transient guests.

(5) The term "vehicle rental facility" means any person or entity that provides vehicles for rent, lease, loan, or other similar use to the public or any segment thereof.

See 2006, 2009, 2010, and 2011 Amendment notes below.

References in Text

Executive Order No. 12333, referred to in subsec. (a)(2)(A), is set out as a note under section 3001 of this title.

Prior Provisions

A prior section 1861, Pub. L. 95–511, title V, §501, as added Pub. L. 105–272, title VI, §602, Oct. 20, 1998, 112 Stat. 2410, defined terms used in this subchapter, prior to repeal by Pub. L. 107–56, title II, §215, Oct. 26, 2001, 115 Stat. 287. See Amendment of Section note above.

Amendments

2011-Pub. L. 112–14 amended directory language of Pub. L. 109–177, §102(b)(1). See 2006 Amendment note below.

Pub. L. 112–3 amended directory language of Pub. L. 109–177, §102(b)(1). See 2006 Amendment note below.

2010-Pub. L. 111–141 amended directory language of Pub. L. 109–177, §102(b)(1). See 2006 Amendment note below.

2009-Pub. L. 111–118 amended directory language of Pub. L. 109–177, §102(b)(1). See 2006 Amendment note below.

2006-Pub. L. 109–177, §102(b)(1), as amended by Pub. L. 111–118, Pub. L. 111–141, Pub. L. 112–3, and Pub. L. 112–14, amended section effective June 1, 2015, so as to read as it read on Oct. 25, 2001. Prior to amendment, section related to access to certain business records for foreign

intelligence and international terrorism investigations.

Subsec. (a)(1). Pub. L. 109–177, §106(a)(1), substituted “Subject to paragraph (3), the Director” for “The Director”.

Subsec. (a)(3). Pub. L. 109–177, §106(a)(2), added par. (3).

Subsec. (b)(2). Pub. L. 109–177, §106(b), amended par. (2) generally. Prior to amendment, par. (2) read as follows: “shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.”

Subsec. (c). Pub. L. 109–177, §106(c), (d), amended subsec. (c) generally. Prior to amendment, text read as follows:

“(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

“(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a) of this section.”

Subsec. (d). Pub. L. 109–177, §106(e), amended subsec. (d) generally. Prior to amendment, text read as follows: “No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.”

Subsec. (d)(2)(C). Pub. L. 109–178, §4(a), amended subpar. (C) generally. Prior to amendment, subpar. (C) read as follows: “At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, but in no circumstance shall a person be required to inform the Director or such designee that the person intends to consult an attorney to obtain legal advice or legal assistance.”

Subsec. (f). Pub. L. 109–178, §3, amended subsec. (f) generally. Prior to amendment, subsec. (f) provided for judicial proceedings relating to challenging an order to produce tangible things.

Pub. L. 109–177, §106(f)(2), added subsec. (f).

Subsecs. (g), (h). Pub. L. 109–177, §106(g), added subsecs. (g) and (h).

2001-Subsec. (a)(1). Pub. L. 107–108 inserted “to obtain foreign intelligence information not concerning a United States person or” after “an investigation”.

Effective Date of 2006 Amendment

Amendment by section 102(b)(1) of Pub. L. 109–177 effective June 1, 2015, except that former provisions to continue in effect with respect to any particular foreign intelligence investigation that began before June 1, 2015, or with respect to any particular offense or potential offense that began or occurred before June 1, 2015, see section 102(b) of Pub. L. 109–177, set out as a note under section 1805 of this title.

50 U.S.C. § 1881a

50 USC 1881a: Procedures for targeting certain persons outside the United States other than United States persons
Text contains those laws in effect on August 12, 2014

From Title 50-WAR AND NATIONAL DEFENSE
CHAPTER 36-FOREIGN INTELLIGENCE SURVEILLANCE
SUBCHAPTER VI-ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

Jump To:

§1881a. Procedures for targeting certain persons outside the United States other than United States persons

(a) Authorization

Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) Limitations

An acquisition authorized under subsection (a)-

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(c) Conduct of acquisition

(1) In general

An acquisition authorized under subsection (a) shall be conducted only in accordance with-

(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

(B) upon submission of a certification in accordance with subsection (g), such certification.

(2) Determination

A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.

(3) Timing of determination

The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)-

(A) before the submission of a certification in accordance with subsection (g); or

(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

(4) Construction

Nothing in subchapter I shall be construed to require an application for a court order under such

subchapter for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

(d) Targeting procedures

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to-

(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(2) Judicial review

The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(e) Minimization procedures

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 1801(h) of this title or section 1821(4) of this title, as appropriate, for acquisitions authorized under subsection (a).

(2) Judicial review

The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(f) Guidelines for compliance with limitations

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure-

(A) compliance with the limitations in subsection (b); and

(B) that an application for a court order is filed as required by this chapter.

(2) Submission of guidelines

The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to-

(A) the congressional intelligence committees;

(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

(C) the Foreign Intelligence Surveillance Court.

(g) Certification

(1) In general

(A) Requirement

Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

(B) Exception

If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.

(2) Requirements

A certification made under this subsection shall-

(A) attest that-

(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to-

(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons

reasonably believed to be located outside the United States; and
(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

(ii) the minimization procedures to be used with respect to such acquisition-
(I) meet the definition of minimization procedures under section 1801(h) or 1821(4) of this title, as appropriate; and
(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;

(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this chapter;
(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;
(v) a significant purpose of the acquisition is to obtain foreign intelligence information;
(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
(vii) the acquisition complies with the limitations in subsection (b);

(B) include the procedures adopted in accordance with subsections (d) and (e);
(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is-
(i) appointed by the President, by and with the advice and consent of the Senate; or
(ii) the head of an element of the intelligence community;

(D) include-
(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or
(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

(3) Change in effective date

The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

(4) Limitation

A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

(5) Maintenance of certification

The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

(6) Review

A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).

(h) Directives and judicial review of directives

(1) Authority

With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to-
(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) Compensation

The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(3) Release from liability

No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(4) Challenging of directives

(A) Authority to challenge

An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) Assignment

The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 1803(e)(1) of this title not later than 24 hours after the filing of such petition.

(C) Standards for review

A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

(D) Procedures for initial review

A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

(E) Procedures for plenary review

If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

(F) Continued effect

Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

(G) Contempt of Court

Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(5) Enforcement of directives

(A) Order to compel

If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) Assignment

The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 1803(e)(1) of this title not later than 24 hours after the filing of such petition.

(C) Procedures for review

A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

(D) Contempt of Court

Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(E) Process

Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

(6) Appeal

(A) Appeal to the Court of Review

The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

(B) Certiorari to the Supreme Court

The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(i) Judicial review of certifications and procedures

(1) In general

(A) Review by the Foreign Intelligence Surveillance Court

The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.

(B) Time period for review

The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

(C) Amendments

The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

(2) Review

The Court shall review the following:

(A) Certification

A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements.

(B) Targeting procedures

The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures

are reasonably designed to-

(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(C) Minimization procedures

The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 1801(h) of this title or section 1821(4) of this title, as appropriate.

(3) Orders

(A) Approval

If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

(B) Correction of deficiencies

If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order-

(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or

(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

(C) Requirement for written statement

In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

(4) Appeal

(A) Appeal to the Court of Review

The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

(B) Continuation of acquisition pending rehearing or appeal

Any acquisition affected by an order under paragraph (3)(B) may continue-

(i) during the pendency of any rehearing of the order by the Court en banc; and

(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

(C) Implementation pending appeal

Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

(D) Certiorari to the Supreme Court

The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(5) Schedule

(A) Reauthorization of authorizations in effect

If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

(B) Reauthorization of orders, authorizations, and directives

If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

(j) Judicial proceedings

(1) Expedited judicial proceedings

Judicial proceedings under this section shall be conducted as expeditiously as possible.

(2) Time limits

A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

(k) Maintenance and security of records and proceedings

(1) Standards

The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(2) Filing and review

All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

(3) Retention of records

The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

(l) Assessments and reviews

(1) Semiannual assessment

Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to-

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution-

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

(2) Agency assessment

The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General-

(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(D) shall provide each such review to-

(i) the Attorney General;

(ii) the Director of National Intelligence; and

(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution-

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(3) Annual review

(A) Requirement to conduct

The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)-

(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

(B) Use of review

The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

(C) Provision of review

The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to-

(i) the Foreign Intelligence Surveillance Court;

(ii) the Attorney General;

(iii) the Director of National Intelligence; and

(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution-

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(Pub. L. 95–511, title VII, §702, as added Pub. L. 110–261, title I, §101(a)(2), July 10, 2008, 122 Stat. 2438 .)

Repeal of Section

Pub. L. 110–261, title IV, §403(b)(1), July 10, 2008, 122 Stat. 2474 , as amended by Pub. L. 112–238, §2(a)(1), Dec. 30, 2012, 126 Stat. 1631, provided that, except as provided in section 404 of Pub. L. 110–261, set out as a note under section 1801 of this title, effective Dec. 31, 2017, this section is repealed.

References in Text

This chapter, referred to in subsecs. (f)(1)(B) and (g)(2)(A)(iii), was in the original "this Act", meaning Pub. L. 95–511, Oct. 25, 1978, 92 Stat. 1783 , which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of this title and Tables.

Senate Resolution 400 of the 94th Congress, referred to in subsec. (l), was agreed to May 19, 1976, and was subsequently amended by both Senate resolution and public law. The Resolution,

which established the Senate Select Committee on Intelligence, is not classified to the Code.

Effective Date of Repeal

Pub. L. 110–261, title IV, §403(b)(1), July 10, 2008, 122 Stat. 2474 , as amended by Pub. L. 112–238, §2(a)(1), Dec. 30, 2012, 126 Stat. 1631, provided that, except as provided in section 404 of Pub. L. 110–261, set out as a Transition Procedures note under section 1801 of this title, the repeals made by section 403(b)(1) are effective Dec. 31, 2017.

Curriculum Vitae

Name	Brigitte Raicher-Siegl

Education

1982	Doctorate in Law, University of Vienna

Professional Experience

1983	Internship: District Court for Commercial Matters, Vienna
1983 – present	Ministry of Transport, Innovation and Technology, Legal Department since 1988 as head of Department (Legal Affairs, Legislative Affairs, Coordinating Department for Civil Emergency Planning and Critical Infrastructure Protection, Information and Data Security)
1999 – present	Representative at the 3 NATO Euro-Atlantic Partnership Council (EAPC) Transport Planning Boards (now NATO EAPC Transport Group [TG])
2005 – 2014	EAPC Planning Board for Inland Surface Transport Working-Group (PBIST-WG) (now TG(IST) WG) Vice Chair