

Exhibit 7

Exhibit 7

LIBERTY AND SECURITY IN A CHANGING WORLD

12 December 2013

**Report and Recommendations of
The President's Review Group on Intelligence
and Communications Technologies**

This page has been intentionally left blank.

Transmittal Letter

Dear Mr. President:

We are honored to present you with the Final Report of the Review Group on Intelligence and Communications Technologies. Consistent with your memorandum of August 27, 2013, our recommendations are designed to protect our national security and advance our foreign policy while also respecting our longstanding commitment to privacy and civil liberties, recognizing our need to maintain the public trust (including the trust of our friends and allies abroad), and reducing the risk of unauthorized disclosures.

We have emphasized the need to develop principles designed to create strong foundations for the future. Although we have explored past and current practices, and while that exploration has informed our recommendations, this Report should not be taken as a general review of, or as an attempt to provide a detailed assessment of, those practices. Nor have we generally engaged budgetary questions (although some of our recommendations would have budgetary implications).

We recognize that our forty-six recommendations, developed over a relatively short period of time, will require careful assessment by a wide range of relevant officials, with close reference to the likely consequences. Our goal has been to establish broad understandings and principles that

can provide helpful orientation during the coming months, years, and decades.

We are hopeful that this Final Report might prove helpful to you, to Congress, to the American people, and to leaders and citizens of diverse nations during continuing explorations of these important questions.

Richard A. Clarke

Michael J. Morell

Geoffrey R. Stone

Cass R. Sunstein

Peter Swire

Acknowledgements

The Review Group would like to thank the many people who supported our efforts in preparing this Report. A number of people were formally assigned to assist the Group, and all performed with professionalism, hard work, and good cheer. These included Brett Freedman, Kenneth Gould, and other personnel from throughout the government. We thank as well the many other people both inside and outside of the government who have contributed their time and energy to assisting in our work.

This page has been intentionally left blank.

Table of Contents

Preface

Executive Summary

Recommendations

Chapter I: Principles

Chapter II: Lessons of History

- A. The Continuing Challenge
- B. The Legal Framework as of September 11, 2001
- C. September 11 and its Aftermath
- D. The Intelligence Community

Chapter III: Reforming Foreign Intelligence Surveillance Directed at United States Persons

- A. Introduction
- B. Section 215: Background
- C. Section 215 and “Ordinary” Business Records

- D. National Security Letters
- E. Section 215 and the Bulk Collection of Telephony Meta-data
 - 1. The Program
 - 2. The Mass Collection of Personal Information
 - 3. Is Meta-data Different?
- F. Secrecy and Transparency

Chapter IV: Reforming Foreign Intelligence Surveillance Directed at Non-United States Persons

- A. Introduction
- B. Foreign Intelligence Surveillance and Section 702
- C. Privacy Protections for United States Persons Whose Communications are Intercepted Under Section 702
- D. Privacy Protections for Non-United States Persons

Chapter V: Determining What Intelligence Should Be Collected and How

- A. Priorities and Appropriateness
- B. Monitoring Sensitive Collection
- C. Leadership Intentions

D. Cooperation with Our Allies

Chapter VI: Organizational Reform in Light of Changing Communications Technology

A. Introduction

B. The National Security Agency

1. “Dual-Use” Technologies: The Convergence of Civilian Communications and Intelligence Collection
2. Specific Organizational Reforms

C. Reforming Organizations Dedicated to the Protection of Privacy and Civil Liberties

D. Reforming the FISA Court

Chapter VII: Global Communications Technology: Promoting Prosperity, Security, and Openness in a Networked World

A. Introduction

B. Background: Trade, Internet Freedom, and Other Goals

1. International Trade and Economic Growth
2. Internet Freedom

judicial approval would not be required under standard and well-established principles.

E. Section 215 and the Bulk Collection of Telephony Meta-data

1. The Program

One reading of section 215 is that the phrase “reasonable grounds to believe that the tangible things sought are *relevant* to an authorized investigation” means that the order must specify with reasonable particularity the records or other things that must be turned over to the government. For example, the order might specify that a credit card company must turn over the credit records of a particular individual who is reasonably suspected of planning or participating in terrorist activities, or that a telephone company must turn over to the government the call records of any person who called an individual suspected of carrying out a terrorist act within a reasonable period of time preceding the terrorist act. This interpretation of “relevant” would be consistent with the traditional understanding of “relevance” in the subpoena context.

In May 2006, however, the FISC adopted a much broader understanding of the word “relevant.”⁸⁴ It was that decision that led to the collection of bulk telephony meta-data under section 215. In that decision, and in thirty-five decisions since, fifteen different FISC judges have issued orders under section 215 directing specified United States telecommunications providers to turn over to the FBI and NSA, “on an

⁸⁴ See *In re Application of the Federal Bureau of Investigation for an Order Requiring the Prod. Of Tangible Things from [Telecommunications Providers] Relating to [Redacted version]*, Order No. BR-05 (FISC May 24, 2006).

ongoing daily basis,” for a period of approximately 90 days, “all call detail records or ‘telephony meta-data’ created by [the provider] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.”⁸⁵

The “telephony meta-data” that must be produced 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) number, International Mobile Station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.”⁸⁶ The orders expressly provide that the meta-data to be produced “does not include the substantive content of any communication . . . or the name, address, or financial information of a subscriber or customer,” nor does it include “cell site location information.”⁸⁷ The orders also contain a nondisclosure provision directing that, with certain exceptions, “no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order.”⁸⁸

The FISC authorized the collection of bulk telephony meta-data under section 215 in reliance “on the assertion of the [NSA] that having access to all the call records ‘is vital to NSA’s counterterrorism intelligence’ because ‘the only effective means by which NSA analysts are able

⁸⁵ *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-109 (FISC Oct. 11, 2013) (hereinafter FISC order 10/11/2013).

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

continuously to keep track of” the activities, operatives, and plans of specific foreign terrorist organizations who “disguise and obscure their communications and identities” is “to obtain and maintain an archive of meta-data that will permit these tactics to be uncovered.”⁸⁹ The government has explained the rationale of the program as follows:

One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort. It is imperative that we have the capability to rapidly identify any terrorist threat inside the United States. . . .

. . . By analyzing telephony meta-data based on telephone numbers or other identifiers associated with terrorist activity, trained expert analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. . . . In this respect, the program helps to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks.⁹⁰

⁸⁹ *In Re Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR-08-13 (FISC Dec. 12, 2008), quoting Application Exhibit A, Declaration of [Redacted version] (Dec. 11, 2008).

⁹⁰ Administration White Paper, *Bulk Collection of Telephony Meta-data Under Section 215 of the USA PATRIOT Act*, at 3-4 (August 9, 2013).

What this means, in effect, is that specified service providers must turn over to the government on an ongoing basis call records for every telephone call made in, to, or from the United States through their respective systems. NSA retains the bulk telephony meta-data for a period of five years. The meta-data are then purged automatically from NSA's systems on a rolling basis. As it currently exists, the section 215 program acquires a very large amount of telephony meta-data each day, but what it collects represents only a small percentage of the total telephony meta-data held by service providers. Importantly, in 2011 NSA abandoned a similar meta-data program for Internet communications.⁹¹

According to the terms of the FISC orders, the following restrictions govern the use of this telephony meta-data:

1. "NSA shall store and process the . . . meta-data in repositories with secure networks under NSA's control. The . . . meta-data shall carry unique markings such that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training," and

⁹¹ For several years, NSA used a similar meta-data program for Internet communications under the authority of FISA's pen register and trap-and-trace provisions rather than under the authority of section 215. NSA suspended this e-mail meta-data program in 2009 because of compliance issues (it came to light that NSA had inadvertently been collecting certain types of information that were not consistent with the FISC's authorization orders). After re-starting it in 2010, NSA Director General Keith Alexander decided to let the program expire at the end of 2011 because, for operational and technical reasons, the program was insufficiently productive to justify the cost. The possibility of revising and reinstating such a program was left open, however. This program posed problems similar to those posed by the section 215 program, and any effort to re-initiate such a program should be governed by the same recommendations we make with respect to the section 215 program.

“NSA shall restrict access to the . . . meta-data to authorized personnel who have received” such training.

2. “The government is . . . prohibited from accessing” the meta-data “for any purpose” other than to obtain “foreign intelligence information.”⁹²
3. “NSA shall access the . . . meta-data for purposes of obtaining foreign intelligence only through queries of the . . . meta-data to obtain contact chaining information . . . using selection terms approved as ‘seeds’ pursuant to the RAS approval process.” What this means is that NSA can access the meta-data only when “there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried,” that is, the specific phone number, “is associated with” a specific foreign terrorist organization. The government submits and the FISC approves a list of specific foreign terrorist organizations to which all queries must relate.
4. The finding that there is a reasonable, articulable suspicion that any particular identifier is associated with a foreign terrorist organization can be made initially by only one of 22 specially trained persons at NSA (20 line personnel and two supervisors). All RAS determinations must be made

⁹² Appropriately trained and authorized technical personnel may also access the meta-data “to perform those processes needed to make it usable for intelligence analysis,” and for related technical purposes, according to the FISC orders.

independently by at least two of these personnel and then approved by one of the two supervisors before any query may be made.

5. Before any selection term may be queried, NSA's Office of General Counsel (OGC) "must first determine" whether it is "reasonably believed to be used by a United States person."⁹³ If so, then the selection term may not be queried if the OGC finds that the United States person was found to be "associated with" a specific foreign terrorist organization "solely on the basis of activities that are protected by the First Amendment to the Constitution."
6. "NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the . . . meta-data for intelligence analysis purposes will be initiated using only selection terms that have been RAS-approved. Whenever the . . . meta-data is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis tools, an auditable record of the activity shall be generated."
7. The determination that a particular selection term may be queried remains in effect for 180 days if the selection term is reasonably believed to be used by a United States person, and otherwise for one year.

⁹³ 50 U.S.C. 1801(i). A "United States person" is either a citizen of the United States or a non-citizen who is a legal permanent resident of the United States.

8. Before any of the results from queries may be shared outside NSA (typically with the FBI), NSA must comply with minimization and dissemination requirements, and before NSA may share any results from queries that reveal information about a United States person, a high-level official must additionally determine that the information “is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.”
9. The FISA court does not review or approve individual queries either in advance or after the fact. It does set the criteria for queries, however, and it receives reports every 30 days from NSA on the number of identifiers used to query the meta-data and on the results of those queries. The Department of Justice and the Senate and House Intelligence Committees also receive regular briefings on the program.
10. Both NSA and the National Security Division of the Department of Justice (NSD/DOJ) conduct regular and rigorous oversight of this program. For example:
 - NSA’s OGC and Office of the Director of Compliance (ODOC) “shall ensure that personnel with access to the . . . meta-data receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and

retention of the . . . meta-data and the results of queries of the . . . meta-data.”⁹⁴

- NSD/DOJ receives “all formal briefing and/or training materials.” NSA’s ODOC “shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information.”⁹⁵
- NSA’s OGC “shall consult with NSD/DOJ “on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority,” and at least once every ninety days NSA’s OGC, ODOC and NSD/DOJ “shall meet for the purpose of assessing compliance” with the FISC’s orders. The results of that meeting “shall be reduced to writing and submitted” to the FISC “as part of any application to renew or reinstate the authority.”⁹⁶
- At least once every 90 days “NSD/DOJ shall meet with NSA’s Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA’s compliance” with the FISC’s orders, and at least once every 90 days NSA’s OGC and NSD/DOJ “shall review a

⁹⁴ *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-158 (FISC, Dec. 2011).

⁹⁵ *Id.*, at 14.

⁹⁶ *Id.*, at 14-15.

sample of the justifications for RAS approvals for selection terms used to query the . . . meta-data.”⁹⁷

- Approximately every 30 days, NSA must file with the FISC “a report that includes a discussion of NSA’s application of the RAS standard,” “a statement of the number of instances . . . in which NSA has shared, in any form, results from queries of the . . . meta-data that contain United States person information, in any form, with anyone outside NSA,” and an attestation for each instance in which United States information has been shared that “the information was related to counterterrorism information and necessary to understand counterterrorism or to assess its importance.”⁹⁸

How does the section 215 bulk telephony meta-data program work in practice? In 2012, NSA queried 288 unique identifiers, each of which was certified by NSA analysts to meet the RAS standard. When an identifier, or “seed” phone number, is queried, NSA receives a list of every telephone number that either called or was called by the seed phone number in the past five years. This is known as the “first hop.” For example, if the seed phone number was in contact with 100 different phone numbers in the past five years, NSA would have a list of those phone numbers. Given that NSA

⁹⁷ *Id.*, at 15.

⁹⁸ *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-109 (FISC Oct. 11, 2013) (hereinafter FISC order 10/11/2013).

has reasonable articulable suspicion to believe that the seed phone number is associated with a foreign terrorist organization, it then seeks to determine whether there is any reason to believe that any of the 100 numbers are *also* associated with a foreign terrorist organization. If so, the query has uncovered possible connections to a potential terrorist network that merits further investigation. Conversely, if none of the 100 numbers in the above hypothetical is believed to be associated with possible terrorist activity, there is less reason to be concerned that the potential terrorist is in contact with co-conspirators in the United States.

In most cases, NSA makes a second “hop.” That is, it queries the database to obtain a list of every phone number that called or was called by the 100 numbers it obtained in the first hop. To continue with the hypothetical: If we assume that the average telephone number called or was called by 100 phone numbers over the course of the five-year period, the query will produce a list of 10,000 phone numbers (100 x 100) that are two “hops” away from the person reasonably believed to be associated with a foreign terrorist organization. If one of those 10,000 phone numbers is thought to be associated with a terrorist organization, that is potentially useful information not only with respect to the individuals related to the first and third hops, but also with respect to individuals related to the second hop (the middleman). In a very few instances, NSA makes a third “hop,” which would expand the list of numbers to approximately one million (100 x 100 x 100).

In 2012, NSA's 288 queries resulted in a total of twelve "tips" to the FBI that called for further investigation. If the FBI investigates a telephone number or other identifier tipped to it through the section 215 program, it must rely on other information to identify the individual subscribers of any of the numbers retrieved. If, through further investigation, the FBI is able to develop probable cause to believe that an identifier in the United States is conspiring with a person engaged in terrorist activity, it can then seek an order from the FISC authorizing it to intercept the *contents* of future communications to and from that telephone number.

NSA believes that on at least a few occasions, information derived from the section 215 bulk telephony meta-data program has contributed to its efforts to prevent possible terrorist attacks, either in the United States or somewhere else in the world. More often, negative results from section 215 queries have helped to alleviate concern that particular terrorist suspects are in contact with co-conspirators in the United States. Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders. Moreover, there is reason for caution about the view that the program is efficacious in alleviating concern about possible terrorist connections, given the fact that the meta-data captured by the program covers only a portion of the records of only a few telephone service providers.

* * * * *