

# Loopholes to Circumvent the Constitution

## Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad

Axel Arnbak<sup>1</sup>   Sharon Goldberg<sup>2</sup>

<sup>1</sup>Institute for Information Law (IViR, University of Amsterdam);  
Harvard University - Berkman Center for Internet & Society

<sup>2</sup>Computer Science, Boston University

HotPETS'14, Amsterdam, NL.  
July 18, 2014

<http://ssrn.com/abstract=2460462>

By ZACK WHITTAKER / CBS NEWS / June 30, 2014, 4:02 PM

# Legal loopholes could allow wider NSA surveillance, researchers say



# Outline

## **Legal Analysis**

Three Legal Regimes: When EO 12333 Applies  
American Internet Traffic Hardly Protected Under EO 12333  
Policies and Operations

## **Technical Analysis**

American traffic can naturally flow abroad  
Protocol manipulations can divert traffic abroad

## **NSA Response**

# Outline

## Legal Analysis

Three Legal Regimes: When EO 12333 Applies  
American Internet Traffic Hardly Protected Under EO 12333  
Policies and Operations

## Technical Analysis

American traffic can naturally flow abroad  
Protocol manipulations can divert traffic abroad

## NSA Response

# Three Legal Regimes for Network Surveillance

## Legal Protection Decreases Significantly

- ▶ Patriot Act s. 215
  - ▶ Domestic Communications
  - ▶ Surveillance Conducted on U.S. Soil
  - ▶ Example: 'The Verizon Metadata Program'

# Three Legal Regimes for Network Surveillance

## Legal Protection Decreases Significantly

- ▶ Patriot Act s. 215
  - ▶ Domestic Communications
  - ▶ Surveillance Conducted on U.S. Soil
  - ▶ Example: 'The Verizon Metadata Program'
  
- ▶ Foreign Intelligence Surveillance Act, notably s. 702
  - ▶ Foreign Communications
  - ▶ Surveillance Conducted on U.S. Soil
  - ▶ Examples: 'PRISM', 'UPSTREAM'

# Three Legal Regimes for Network Surveillance

## Legal Protection Decreases Significantly

- ▶ Patriot Act s. 215
  - ▶ Domestic Communications
  - ▶ Surveillance Conducted on U.S. Soil
  - ▶ Example: 'The Verizon Metadata Program'
- ▶ Foreign Intelligence Surveillance Act, notably s. 702
  - ▶ Foreign Communications
  - ▶ Surveillance Conducted on U.S. Soil
  - ▶ Examples: 'PRISM', 'UPSTREAM'
- ▶ Executive Order 12333.
  - ▶ Surveillance Conducted on Foreign Soil.
  - ▶ 'Primary legal authority' according to the NSA.
  - ▶ Little media attention so far, but the focus of our paper.
  - ▶ Example: 'MUSCULAR'.

## Two Criteria for EO 12333 Application: Surveillance Location and 'Target'

- ▶ EO 12333 applies to network surveillance when the operation
  - ▶ does not 'intentionally target a U.S. person', AND
  - ▶ is conducted abroad.

may also apply domestically, under partly classified circumstances.



## Two Criteria for EO 12333 Application: Surveillance Location and 'Target'

- ▶ EO 12333 applies to network surveillance when the operation
  - ▶ does not 'intentionally target a U.S. person', AND
  - ▶ is conducted abroad.

may also apply domestically, under partly classified circumstances.

- ▶ Internet traffic is **presumed** 'foreign' when these **legal criteria** are met
  - ▶ Presumed 'foreign' entities (*i.e.*, persons, organizations, etc.) receive no constitutional protection in the U.S.
  - ▶ US Supreme Court [1990], *United States v. Verdugo-Urquidez*

# Antiquated Legal Definitions Create Network Surveillance Loopholes

- ▶ Key surveillance definitions are over three decades old
  - ▶ 'Electronic surveillance' in s. 1801(f) FISA  
hardly changed since 1978
  - ▶ 'Collection of information' in s. 2.3 EO 12333 and  
'collection techniques' in s. 2.4 EO 12333  
hardly changed since 1981

# Antiquated Legal Definitions Create Network Surveillance Loopholes

- ▶ Key surveillance definitions are over three decades old
  - ▶ 'Electronic surveillance' in s. 1801(f) FISA  
hardly changed since 1978
  - ▶ 'Collection of information' in s. 2.3 EO 12333 and  
'collection techniques' in s. 2.4 EO 12333  
hardly changed since 1981
- ▶ Antiquated laws fail to capture new technologies:
  - ▶ Bulk surveillance does not 'intentionally target a U.S. person';
  - ▶ 'Installing a device' for surveillance only covers 'radio'  
technology;

# Antiquated Legal Definitions Create Network Surveillance Loopholes

- ▶ Key surveillance definitions are over three decades old
  - ▶ 'Electronic surveillance' in s. 1801(f) FISA hardly changed since 1978
  - ▶ 'Collection of information' in s. 2.3 EO 12333 and 'collection techniques' in s. 2.4 EO 12333 hardly changed since 1981
- ▶ Antiquated laws fail to capture new technologies:
  - ▶ Bulk surveillance does not 'intentionally target a U.S. person';
  - ▶ 'Installing a device' for surveillance only covers 'radio' technology;
- ▶ Network protocol manipulations for untargeted surveillance are regulated by the permissive EO 12333 regime

# Antiquated Legal Definitions Create Network Surveillance Loopholes

- ▶ Key surveillance definitions are over three decades old
  - ▶ 'Electronic surveillance' in s. 1801(f) FISA hardly changed since 1978
  - ▶ 'Collection of information' in s. 2.3 EO 12333 and 'collection techniques' in s. 2.4 EO 12333 hardly changed since 1981
- ▶ Antiquated laws fail to capture new technologies:
  - ▶ Bulk surveillance does not 'intentionally target a U.S. person';
  - ▶ 'Installing a device' for surveillance only covers 'radio' technology;
- ▶ Network protocol manipulations for untargeted surveillance are regulated by the permissive EO 12333 regime
- ▶ Disclaimer:  
Arriving at a definite legal conclusion is difficult from the 'outside' because many interpretations remain classified.

# EO 12333 is more permissive than FISA

- ▶ Example: USSID 18 'intentional targeting of U.S. persons'
  - ▶ Already a very narrow legal definition
  - ▶ But, as a general rule, requires warrant from FISA Court
  - ▶ However, 'foreignness presumed' when conducted abroad under USSID 18,
  - ▶ USSID 18 sec. 4: wide exceptions overruling the warrant requirement

(U) Collection

4.1. ~~(S//SI//REL)~~ Communications which are known to be to, from or about a U.S. PERSON  not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances:

(b)(1)

a. (U//~~FOUO~~) With the approval of the United States Foreign Intelligence Surveillance Court either under the conditions outlined in Annex A of this USSID or as permitted by other FISA authorities.

b. (U) With the approval of the Attorney General of the United States, if:

(1) (U) The COLLECTION is directed against the following:

(a) (U//~~FOUO~~) Communications to or from U.S. PERSONS outside the UNITED STATES if such persons have been approved for targeting in accordance with the terms of FISA (e.g., the targeted U.S. PERSON is the subject of an order or authorization issued pursuant to Sections 105, 703, 704, or 705(b) of FISA), or

(b) ~~(S//SI//REL)~~ International communications to, from,

(b)(1)

# EO 12333 is more permissive than FISA

- ▶ Redacted exceptions go on for four pages in USSID 18 sec. 4

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(1) (U//~~FOUO~~) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

(2) (U//~~FOUO~~) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) (S//~~REL~~) The TARGETED [REDACTED] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(b)(1)

(4) (S//~~SI/REL~~) The COLLECTION is directed against [REDACTED] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(5) (S//~~SI/REL~~) Technical devices (e.g., [REDACTED]) are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [REDACTED]) and the COLLECTION is directed against [REDACTED] voice and facsimile communications with one COMMICANT in the UNITED STATES, and the TARGET of the COLLECTION is [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)  
(b)(3)-18 USC 798

(b)(1)

(a) A non-U.S. PERSON located outside the UNITED STATES [REDACTED]

(b) [REDACTED]

# EO 12333 is More Permissive than FISA

- ▶ An entire paragraph of USSID 18 s. 4.2. is redacted
  - ▶ This could overrule an entire regime of legal safeguards.
  - ▶ But it's impossible to tell.

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(U) [redacted] 4.2. (S//SI//REL) [redacted]

[redacted] [redacted] (b)(1)

a. (S//SI//REL) [redacted]

[redacted]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)  
(b)(3)-18 USC 798

b. (S//SI//REL) [redacted]

[redacted]

The diagram shows a document with several redacted sections. At the top, the text "(U)" is followed by a redacted box, then "4.2. (S//SI//REL)" followed by another redacted box. Below this is a large redacted block with a line pointing to it from the label "(b)(1)" on the right. Underneath is "a. (S//SI//REL)" followed by a redacted box. Below that is another redacted block with a line pointing to it from a list of labels on the left: "(b)(1)", "(b)(3)-P.L. 86-36", "(b)(3)-50 USC 3024(i)", and "(b)(3)-18 USC 798". At the bottom is "b. (S//SI//REL)" followed by a redacted box, and another redacted box below it.

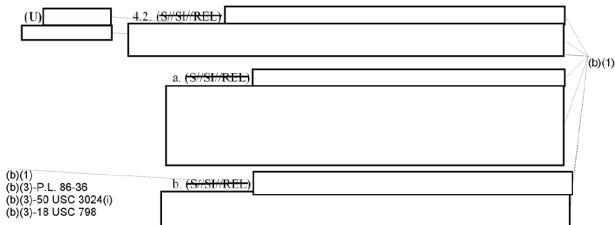


# EO 12333 is More Permissive than FISA

- ▶ An entire paragraph of USSID 18 s. 4.2. is redacted
  - ▶ This could overrule an entire regime of legal safeguards.
  - ▶ But it's impossible to tell.

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~



- ▶ These are only a few of many examples we could give.

# Bleak Long Term Outlook for EO 12333 Surveillance and Reform

- ▶ Fundamental problem:  
EO 12333 is under the Executive Branch.
  - ▶ Wide Executive authorities for overseas national security operations, art. II U.S. Constitution
  - ▶ Little authority nor interest in U.S. Congress & Judiciary

# Bleak Long Term Outlook for EO 12333 Surveillance and Reform

- ▶ Fundamental problem:  
EO 12333 is under the Executive Branch.
  - ▶ Wide Executive authorities for overseas national security operations, art. II U.S. Constitution
  - ▶ Little authority nor interest in U.S. Congress & Judiciary
- ▶ Several real and long-term consequences:
  - ▶ USSID 18 still heavily redacted (unlike FISA targeting and minimization procedures).
  - ▶ Under EO 12333, other critical surveillance guidelines and policy directives remain classified.
  - ▶ No court review of surveillance operations, little legislative review policies.
  - ▶ Sometimes, mere N.S.A. Director approval suffices.

**Even if s.215 and s.702 loopholes are closed,  
major EO 12333 loopholes remain.**

# A Few Days After We Released Our Paper...

The Washington Post

National Security

## In NSA-intercepted data, those not targeted far outnumber the foreigners who are

Files provided by Snowden show extent to which ordinary Web users are caught in the net

The screenshot shows a document titled "Overview (U)" with a redaction bar at the top. It contains several sections of text, many of which are redacted with black boxes. Two photographs of a man with a beard and mustache are visible at the bottom of the document. The text includes names like "Muhammad Fakir (Makad)", "Abu Hamza, 'al'", and "Abu-Hamza, user of". It also mentions "AFRICAN, SOUTH AMERICAN, ASIAN, AUSTRALIAN, EUROPEAN, ISRAELI, JAPANESE, KOREAN, MEXICAN, MIDDLE EASTERN, NORTH AMERICAN, PACIFIC ISLANDER, SOUTH AMERICAN, SOUTH ASIAN, SOUTH EAST ASIAN, WESTERN EUROPEAN, AND WESTERN AFRICAN" and "COMMUNIST, SOCIALIST, AND OTHER LEFT-WING IDEOLOGUES".

Target package prepared by the National Security Agency prior to the capture of Abu Hamza in January 2011

By [Barton Gellman](#), [Julie Tate](#) and [Ashkan Soltani](#) July 5

Ordinary Internet users, American and non-American alike, far outnumber legally targeted foreigners in the communications intercepted by the National Security Agency from U.S. digital networks, according to a four-month investigation by The Washington Post.

### Most Read World

- 1 Iron Dome, Israel's antimissile system, changes calculus of fig...
- 2 MAP: How Asia is scared of China
- 3 Bride school: Where South Korea's mail-order wives learn their trade
- 4 Hamas rejects Egypt proposal for truce with Israel
- 5 Video: This is what an Israeli 'roof knock' looks like

washingtonpost.com  
© 1996-2014 The Washington Post

Help and Contact Us  
Terms of Service

Source: <http://wapo.st/1mVEPXG>

# A Few Days After We Released Our Paper...

The Washington Post

National Security

## In NSA-intercepted data, those not targeted far outnumber the foreigners who are

Files provided by Snowden show extent to which ordinary Web users are caught in the net

Overview (U)

Target package prepared by the National Security Agency prior to the capture of Abu Hamza in January 2011

By Barton Gellman, Julie Tate and Ashkan Soltani July 5

Ordinary Internet users, American and non-American alike, far outnumber legally targeted foreigners in the communications intercepted by the National Security Agency from U.S. digital networks, according to a four-month investigation by The Washington Post.

### Most Read World

- 1 Iron Dome, Israel's antimissile system, changes calculus of fig...
- 2 MAP: How Asia is scared of China
- 3 Bride school: Where South Korea's mail-order wives learn their trade
- 4 Hamas rejects Egypt proposal for truce with Israel
- 5 Video: This is what an Israeli 'roof knock' looks like

washingtonpost.com

© 1996-2014 The Washington Post

Help and Contact Us

Terms of Service

Source: <http://wapo.st/1mVEPXG>

Disturbing, but covers s.702 surveillance, not even EO 12333.

# Outline

## Legal Analysis

Three Legal Regimes: When EO 12333 Applies

American Internet Traffic Hardly Protected Under EO 12333

Policies and Operations

## Technical Analysis

American traffic can naturally flow abroad

Protocol manipulations can divert traffic abroad

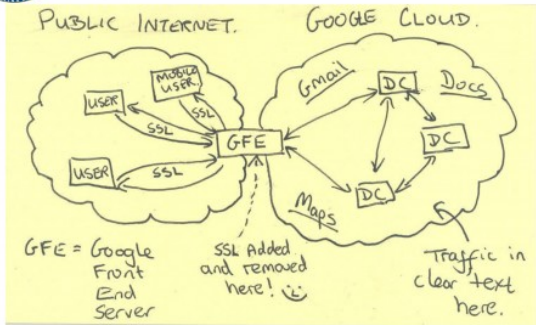
## NSA Response

# Data Can be Stored Abroad

TOP SECRET//SI//NOFORN



## Current Efforts - Google

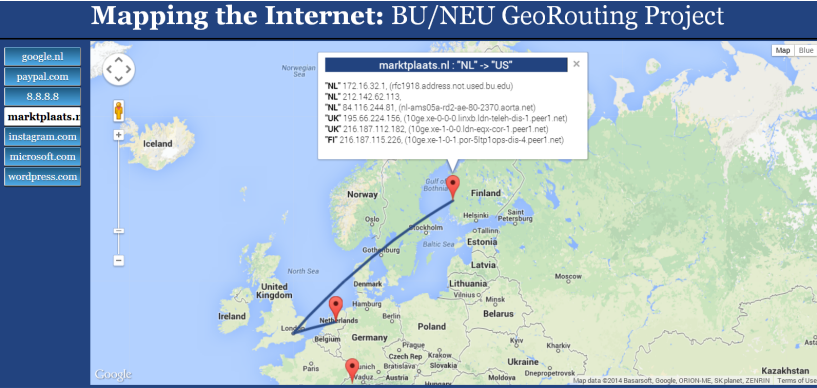


TOP SECRET//SI//NOFORN

"Such large-scale collection of Internet content would be illegal in the United States, but the operations take place overseas, where the NSA is allowed to presume that anyone using a foreign data link is a foreigner. ... Outside U.S. territory, statutory restrictions on surveillance seldom apply and the FISC has no jurisdiction."

Source: <http://wapo.st/1bCL7HK>

# Routing Can Naturally Divert Traffic Abroad

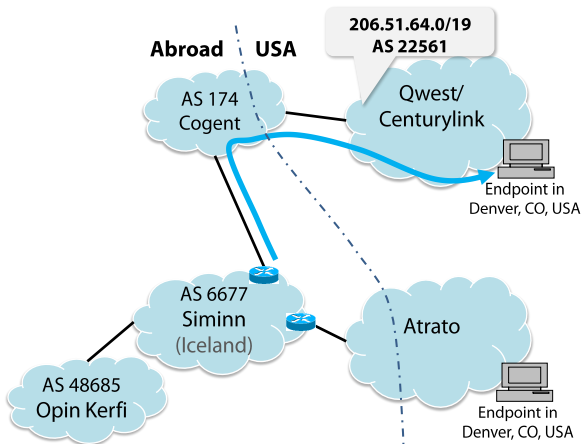


BU/NEU Georoute Project AJ Trainor, George Hongkai Sun, Anthony Faraco-Hadlock, Sharon Goldberg and David Choffnes  
<http://georoute.bu.edu/demo/>



# BGP Manipulations Can Divert Traffic Abroad

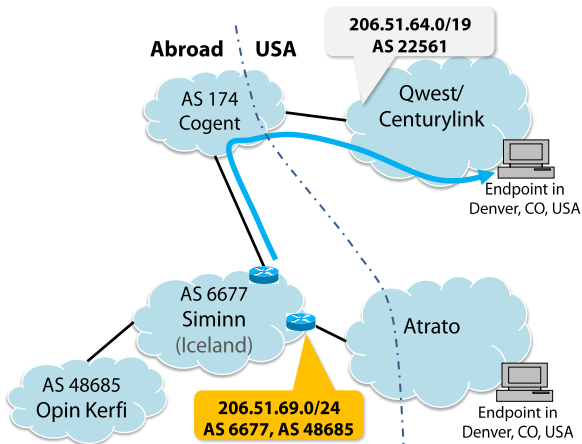
This happened on June 31, 2013; Siminn claimed it was a misconfiguration.



Source: <http://www.renesys.com/2013/11/mitm-internet-hijacking/>

# BGP Manipulations Can Divert Traffic Abroad

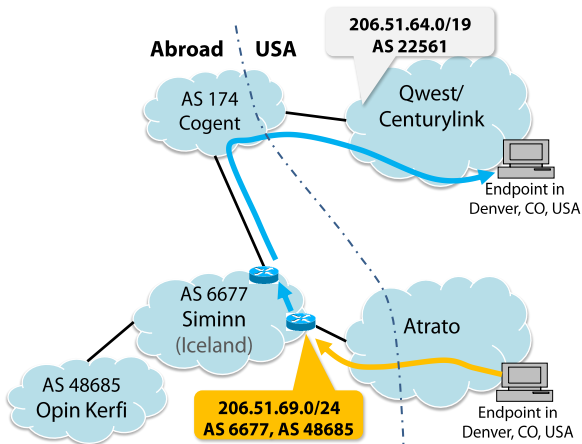
This happened on June 31, 2013; Siminn claimed it was a misconfiguration.



Source: <http://www.renesys.com/2013/11/mitm-internet-hijacking/>

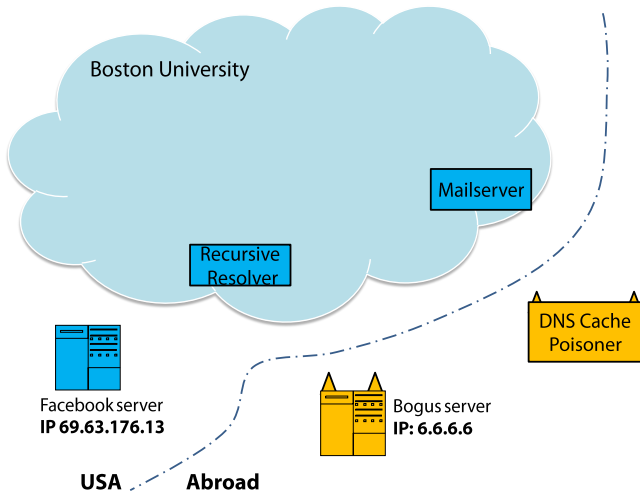
# BGP Manipulations Can Divert Traffic Abroad

This happened on June 31, 2013; Siminn claimed it was a misconfiguration.



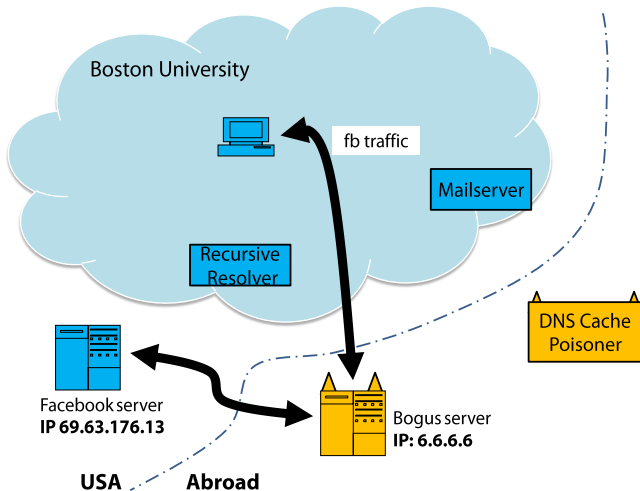
Source: <http://www.renesys.com/2013/11/mitm-internet-hijacking/>

# DNS Manipulations Can Divert Traffic Abroad



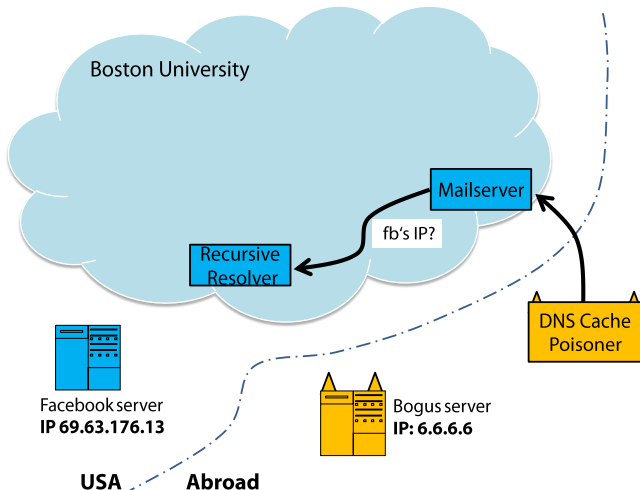
A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

# DNS Manipulations Can Divert Traffic Abroad



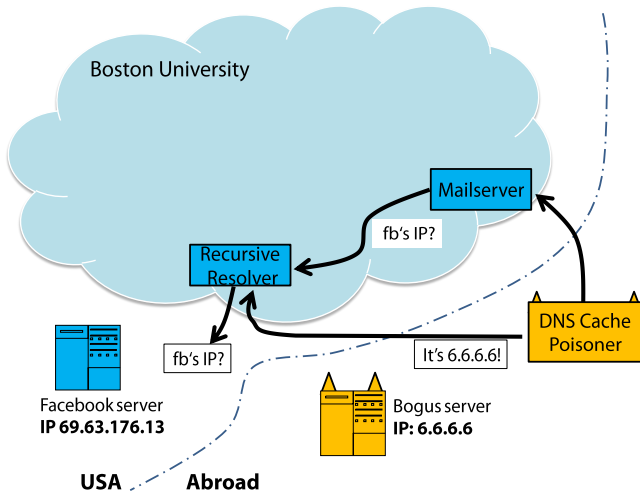
A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

# DNS Manipulations Can Divert Traffic Abroad



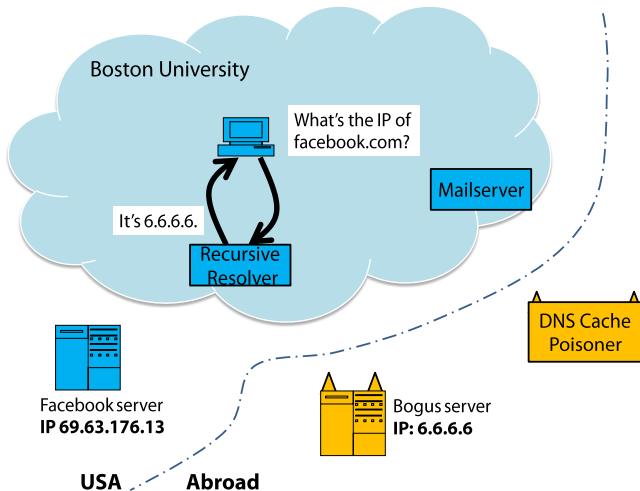
A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

# DNS Manipulations Can Divert Traffic Abroad



A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

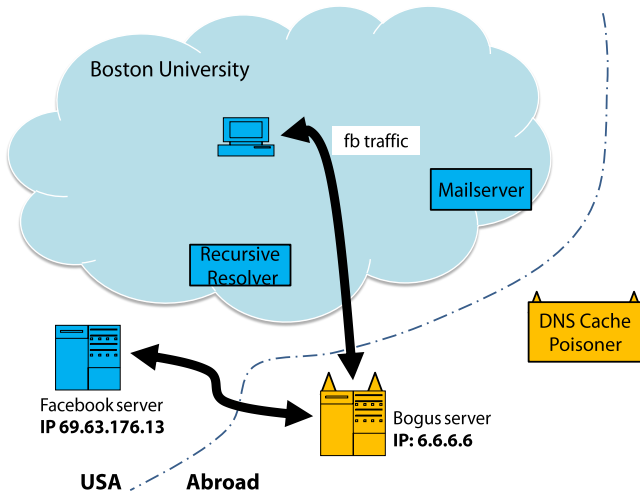
# DNS Manipulations Can Divert Traffic Abroad



A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.



# DNS Manipulations Can Divert Traffic Abroad



A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

# Outline

## Legal Analysis

Three Legal Regimes: When EO 12333 Applies  
American Internet Traffic Hardly Protected Under EO 12333  
Policies and Operations

## Technical Analysis

American traffic can naturally flow abroad  
Protocol manipulations can divert traffic abroad

## NSA Response

## NSA Response

However, an NSA spokesperson denied that either EO 12333 or USSID 18 “authorizes **targeting** of U.S. persons for electronic surveillance by routing their communications outside of the U.S.” in an emailed statement to CBS News.

“**Absent limited exception** (for example, in an emergency), the Foreign Intelligence Surveillance Act requires that we get a court order to **target** any U.S. person anywhere in the world for electronic surveillance. In order to get such an order, we have to establish, to the satisfaction of a federal judge, probable cause to believe that the U.S. person is an agent of a foreign power,” the spokesperson said.

Emphasis ours.

# Our Reaction to the NSA Response

<http://is.gd/5S9L1x>

## FREEDOM TO TINKER

research and expert commentary on digital technologies in public life



### “Loopholes for Circumventing the Constitution”, the NSA Statement, and Our Response

JULY 11, 2014 BY AXEL ARNBAK 1 COMMENT

CBS News and a host of other outlets have covered my [new paper with Sharon Goldberg](#), *Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad*. We'll present the paper on July 18 at [HotPETS](#), right after a keynote by Bill Binney (the NSA whistleblower), and at TPRC in September. Meanwhile, the NSA has responded to our paper in a clever way that avoids addressing what our paper is actually about.

In the paper, we reveal known and new legal and technical loopholes that enable internet traffic shaping by intelligence authorities to circumvent constitutional safeguards for Americans. The paper is in some ways a classic exercise in threat modeling, but what's rather new is our combination of descriptive legal analysis with methods from computer science. Thus, we're able to identify interdependent legal and technical loopholes, mostly in internet routing. We'll definitely be pursuing similar projects in the future and hope we get other folks to adopt such multidisciplinary methods too.

As to the media coverage, the CBS News [piece](#) contains some outstanding reporting and an official NSA statement that seeks – but fails – to debunk our analysis:

However, an NSA spokesperson denied that either EO 12333 or USSID 18 “authorizes targeting of U.S. persons for electronic surveillance by routing their communications outside of the U.S.,” in an emailed statement to CBS News.

“Absent limited exception (for example, in an emergency), the Foreign Intelligence Surveillance Act requires that we get a court order to target any U.S. person anywhere in the world for electronic surveillance. In order to get such an order, we have to establish, to the satisfaction of a federal judge, probable cause to believe that

## Summary & Discussion

- ▶ A surveillance operation falls in the permissive EO 12333 regime when it *presumes* two connected criteria:
  - ▶ it does not *intentionally target a U.S. person*
  - ▶ and is *conducted abroad*.
- ▶ For example, bulk collection of American traffic abroad.
- ▶ Traffic can also be deliberately diverted abroad.
- ▶ Many legal interpretations remain classified.

## Summary & Discussion

- ▶ A surveillance operation falls in the permissive EO 12333 regime when it *presumes* two connected criteria:
  - ▶ it does not *intentionally target a U.S. person*
  - ▶ and is *conducted abroad*.
- ▶ For example, bulk collection of American traffic abroad.
- ▶ Traffic can also be deliberately diverted abroad.
- ▶ Many legal interpretations remain classified.
  
- ▶ Discussion
  - ▶ What attacks on Tor fall under the two criteria?
  - ▶ Morality aside: is there a more robust way of distinguishing US persons and foreigners?

## Summary & Discussion

- ▶ A surveillance operation falls in the permissive EO 12333 regime when it *presumes* two connected criteria:
  - ▶ it does not *intentionally target a U.S. person*
  - ▶ and is *conducted abroad*.
- ▶ For example, bulk collection of American traffic abroad.
- ▶ Traffic can also be deliberately diverted abroad.
- ▶ Many legal interpretations remain classified.
  
- ▶ Discussion
  - ▶ What attacks on Tor fall under the two criteria?
  - ▶ Morality aside: is there a more robust way of distinguishing US persons and foreigners?

**Even if s.215 and s.702 loopholes are closed,  
major EO 12333 legal & technical loopholes remain.**