Loopholes to Circumvent the Constitution

Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad

Axel Arnbak[1] Sharon Goldberg[2]

[1]Institute for Information Law (IViR, University of Amsterdam);
Harvard University - Berkman Center for Internet & Society

[2]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

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'.

DISCLAIMER: Please read the paper. FISA and EO 12333 are complicated, old and partly still classified law.

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 [redacted] 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, [redacted] (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] (b)(1)
[redacted] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(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 COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [redacted] (b)(1)

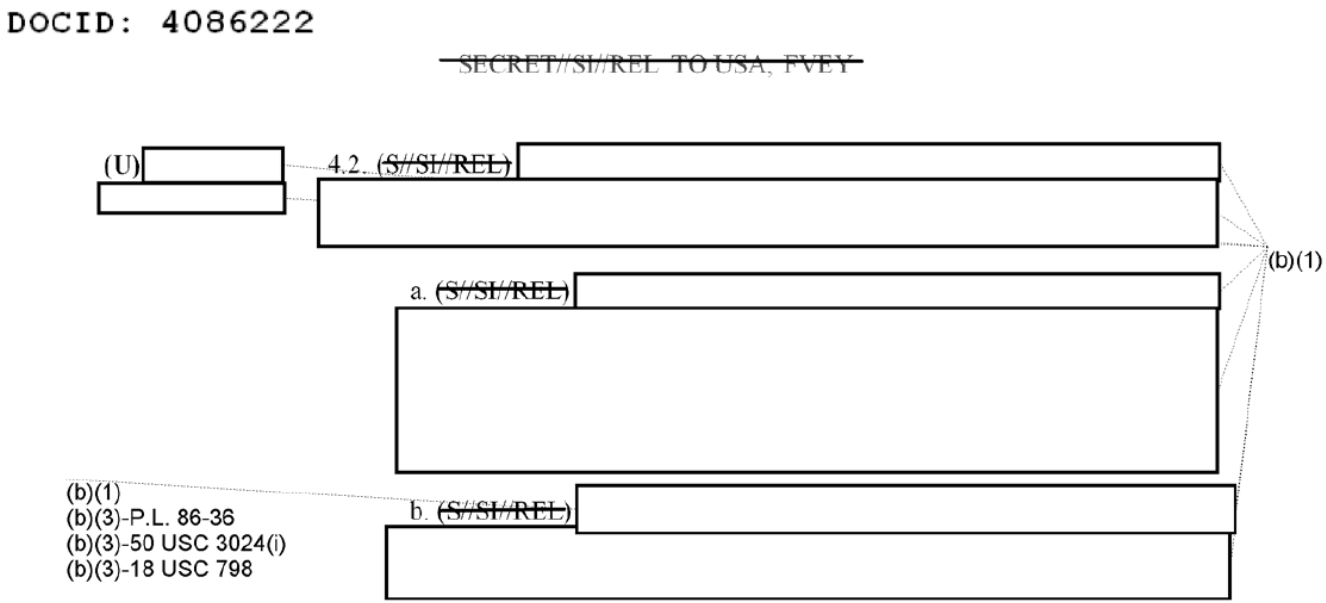
(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

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

(b) [redacted]

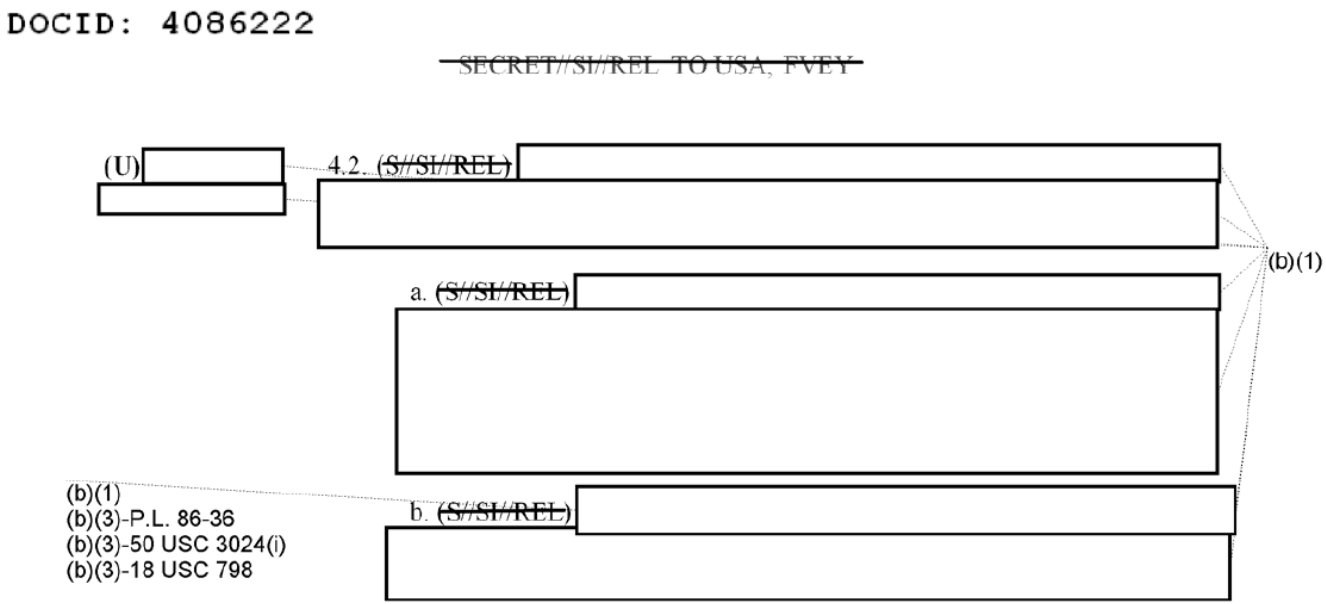
EO 12333 is More Permissive than FISA

- 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.



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.



- 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.

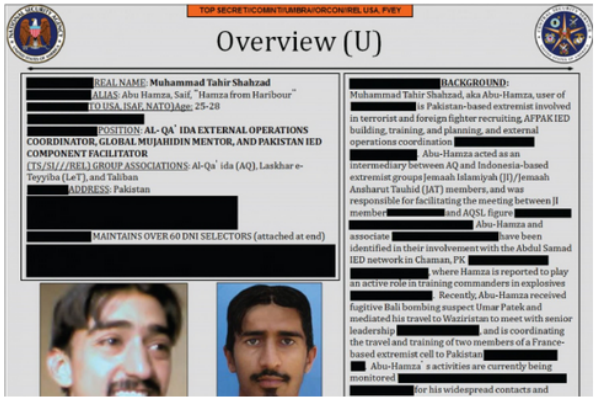
A Few Days After We Released Our Paper...

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



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

Source: `http://wapo.st/1mVEPXG`

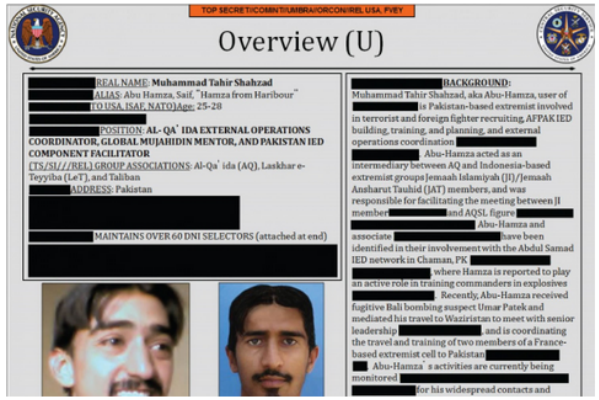
A Few Days After We Released Our Paper...

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


TOP SECRET//COMINT//NOFORN

Overview (U)

REAL NAME: Muhammad Tahir Shahzad
ALIAS: Abu Hamza, Saif, "Hamza from Haribour"
TO USA, ISAF, NATO)Age: 25-28
POSITION: AL- QA' IDA EXTERNAL OPERATIONS COORDINATOR, GLOBAL MUJAHIDIN MENTOR, AND PAKISTAN IED COMPONENT FACILITATOR
(TS//SI//REL) GROUP ASSOCIATIONS: Al-Qa' ida (AQ), Laskhar e-Teyyiba (LeT), and Taliban
ADDRESS: Pakistan
MAINTAINS OVER 60 DNI SELECTORS (attached at end)

BACKGROUND:
Muhammad Tahir Shahzad, aka Abu-Hamza, user of is Pakistan-based extremist involved in terrorist and foreign fighter recruiting, AFPAK IED building, training, and planning, and external operations coordination . Abu-Hamza acted as an intermediary between AQ and Indonesia-based extremist groups Jemaah Islamiyah (JI)/Jemaah Ansharut Tauhid (JAT) members, and was responsible for facilitating the meeting between JI member and AQSL figure . Abu-Hamza and associate have been identified in their involvement with the Abdul Samad IED network in Chaman, PK , where Hamza is reported to play an active role in training commanders in explosives . Recently, Abu-Hamza received fugitive Bali bombing suspect Umar Patek and mediated his travel to Waziristan to meet with senior leadership , and is coordinating the travel and training of two members of a France-based extremist cell to Pakistan. Abu-Hamza 's activities are currently being monitored for his widespread contacts and

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

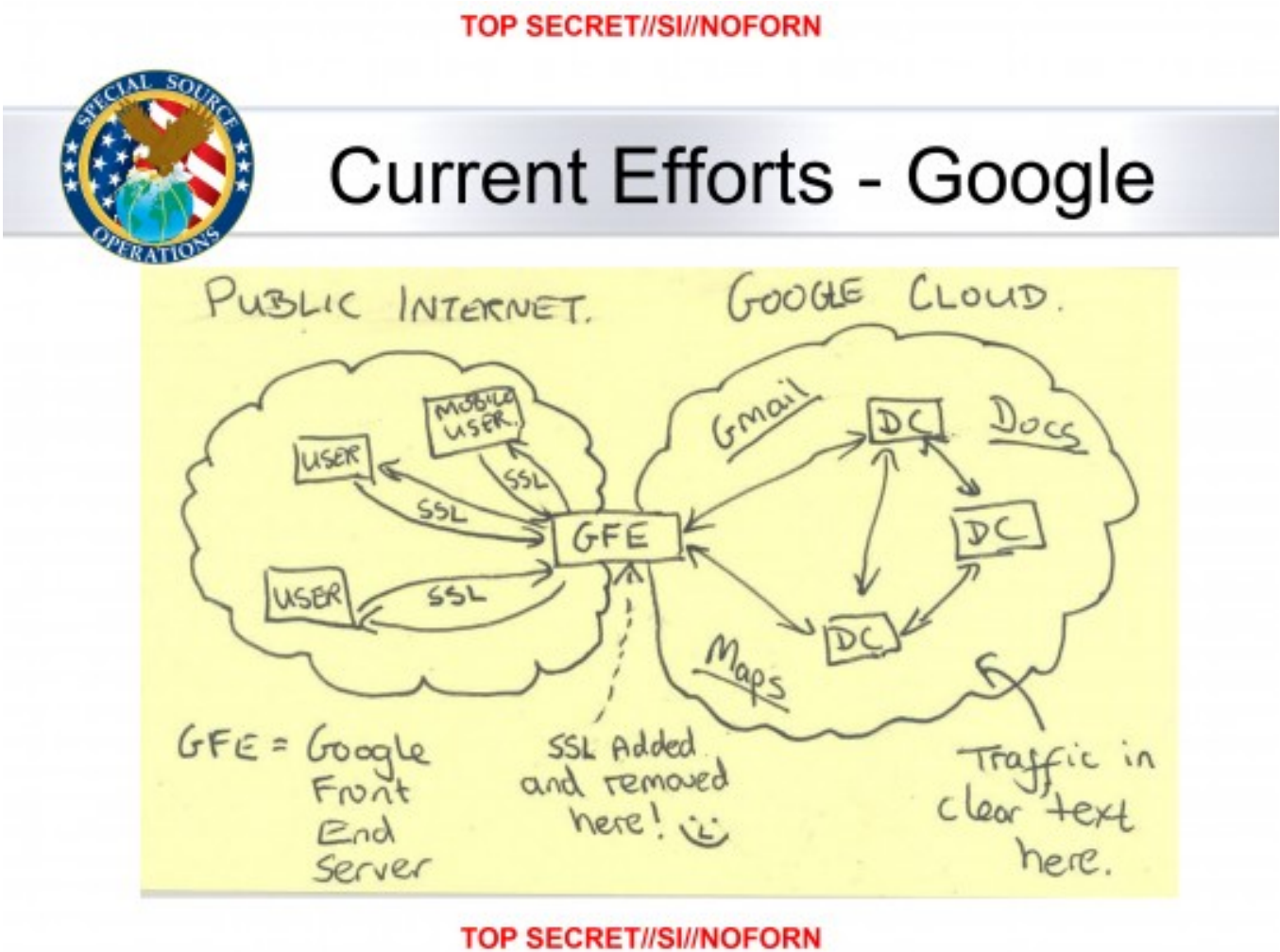
1 Iron Dome, Israel's antimissile system, changes calculus of fig...
2 MAP: How Asia is scared of China
3 Bride school: Where South Korea's mail-order wives learn their trade
4 Hamas rejects Egypt proposal for truce with Israel
5 Video: This is what an Israeli 'roof knock' looks like

Source: `http://wapo.st/1mVEPXG`

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

Outline

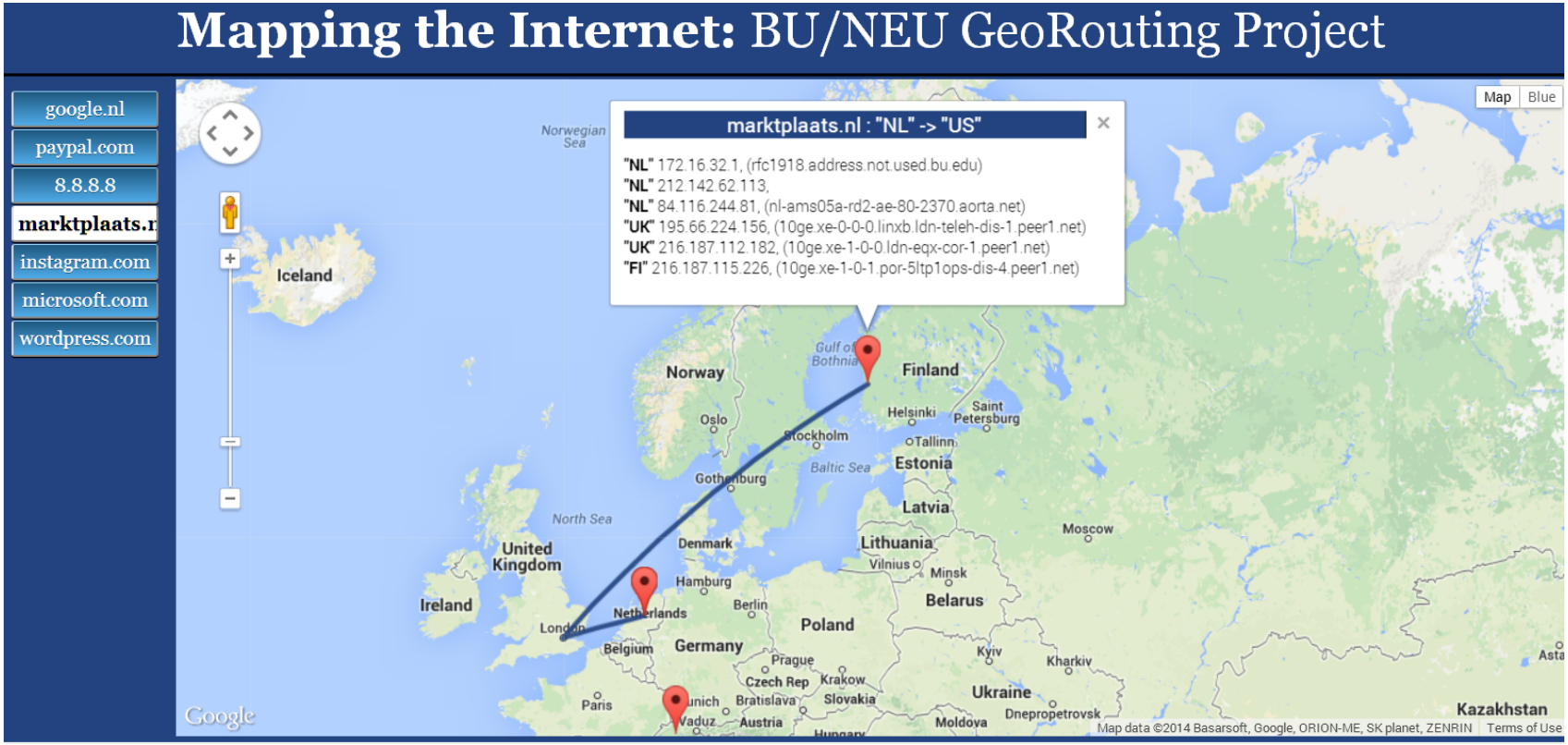
Data Can be Stored Abroad



"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

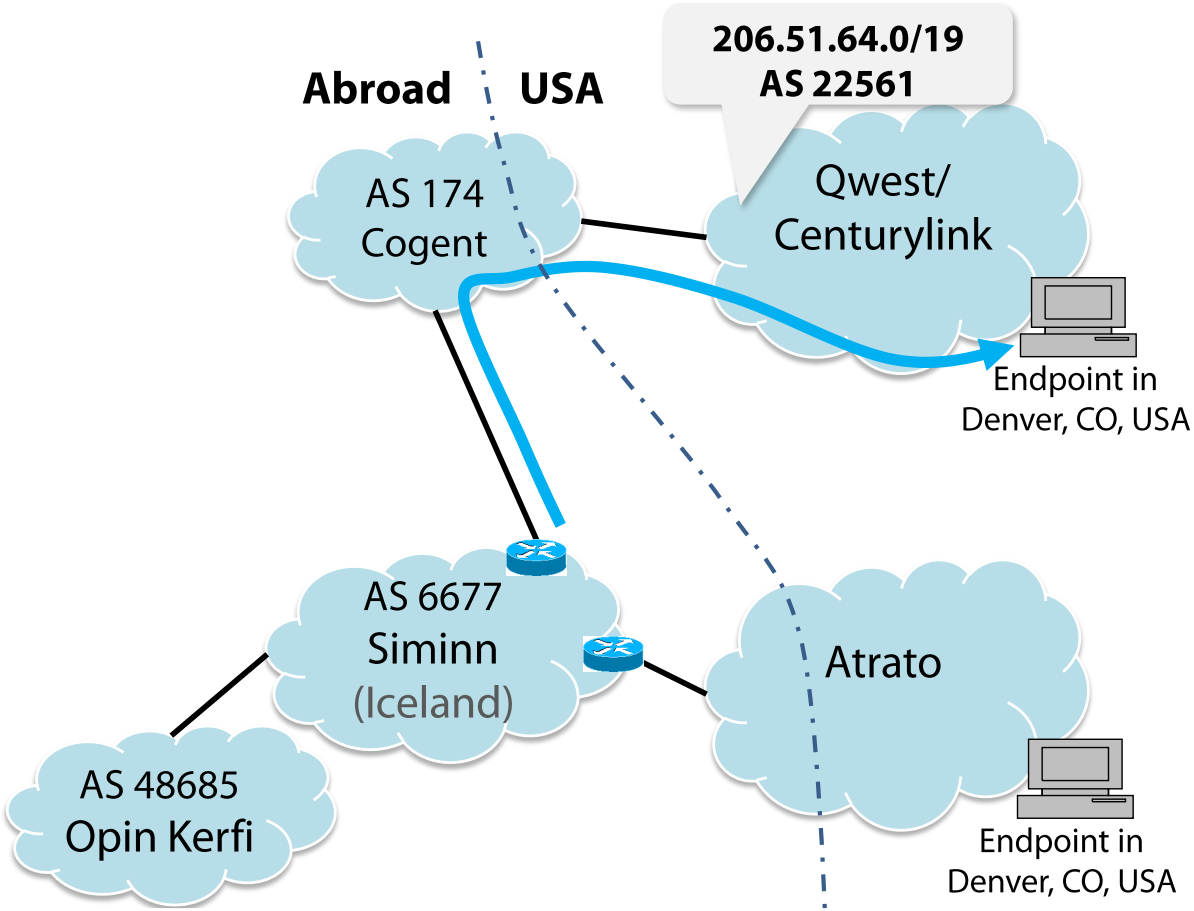


BU/NEU Georoute Project AJ Trainor, George Hongkai Sun, Anthony Faraco-Hadlock, Sharon Goldberg and David Choffnes

`http://georoute.bu.edu/demo/`

BGP Manipulations Can Divert Traffic Abroad

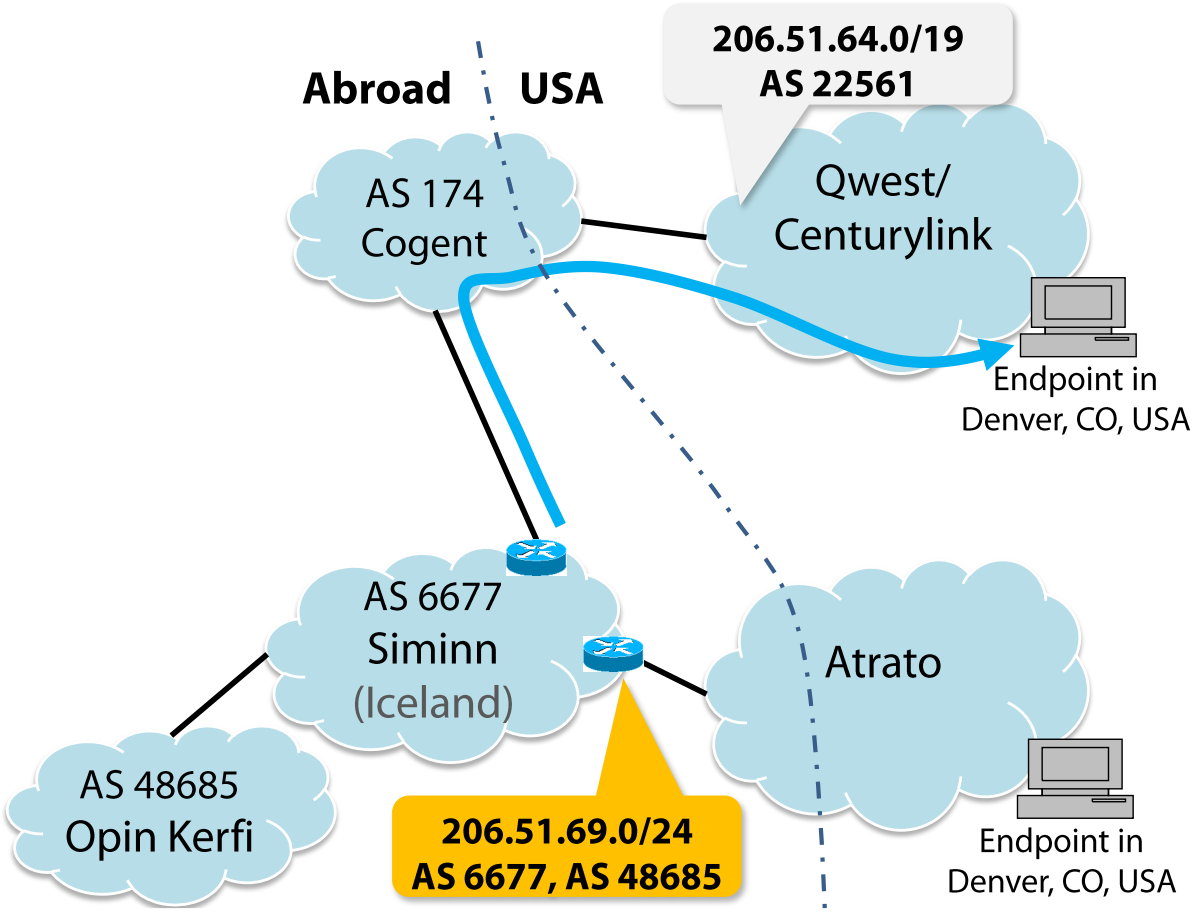
This happened on June 31, 2013; Siminn claimed it was a misconfiguration.



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

BGP Manipulations Can Divert Traffic Abroad

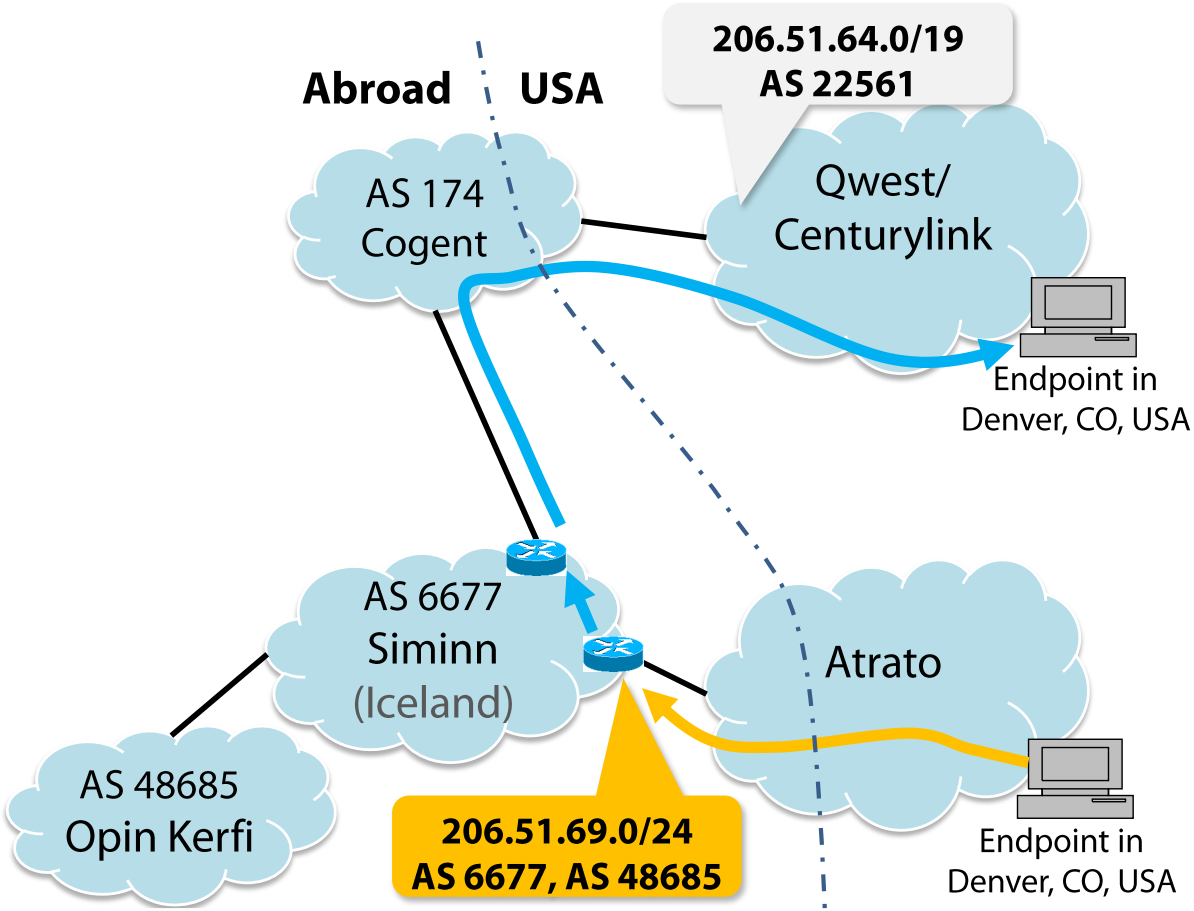
This happened on June 31, 2013; Siminn claimed it was a misconfiguration.



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

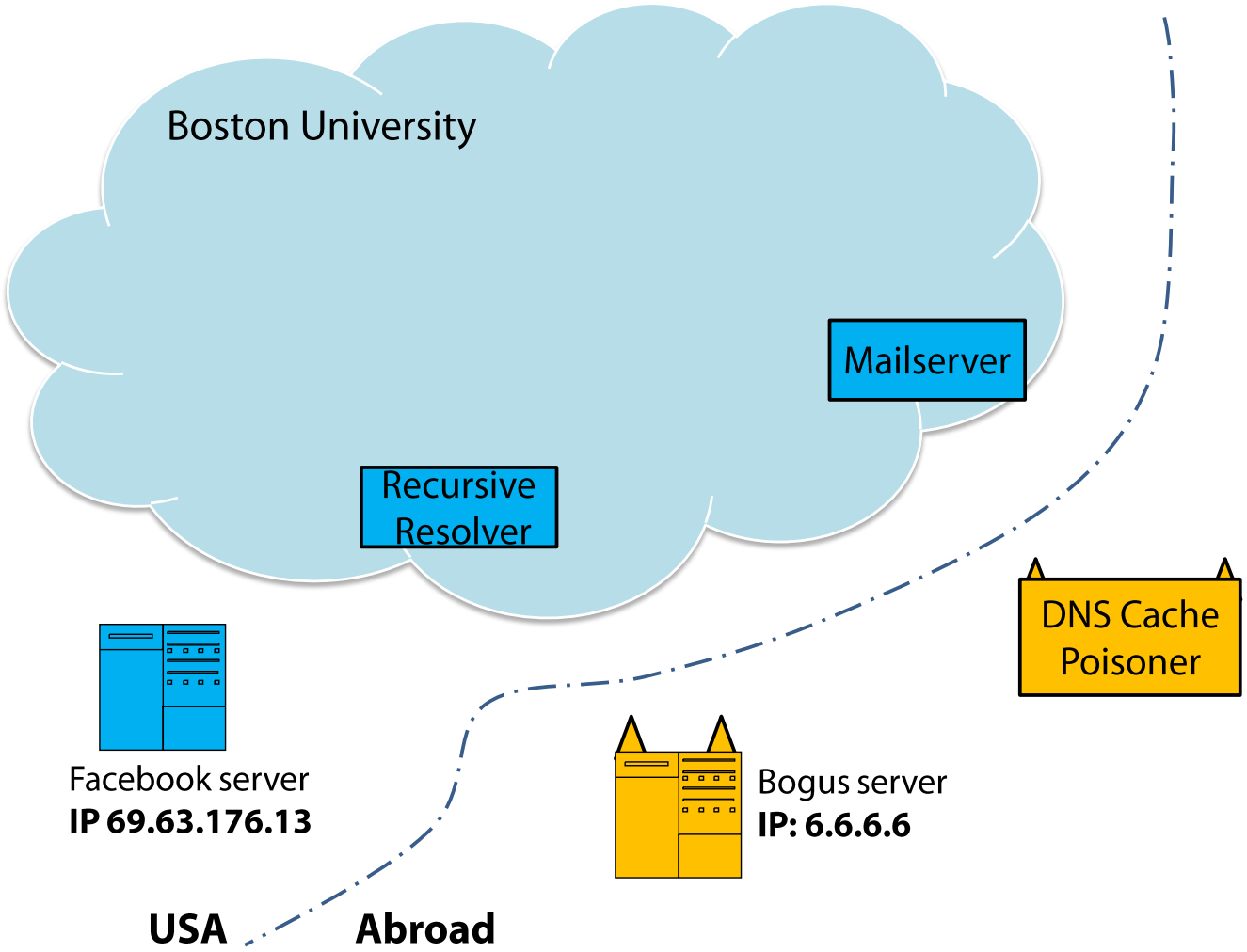
BGP Manipulations Can Divert Traffic Abroad

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



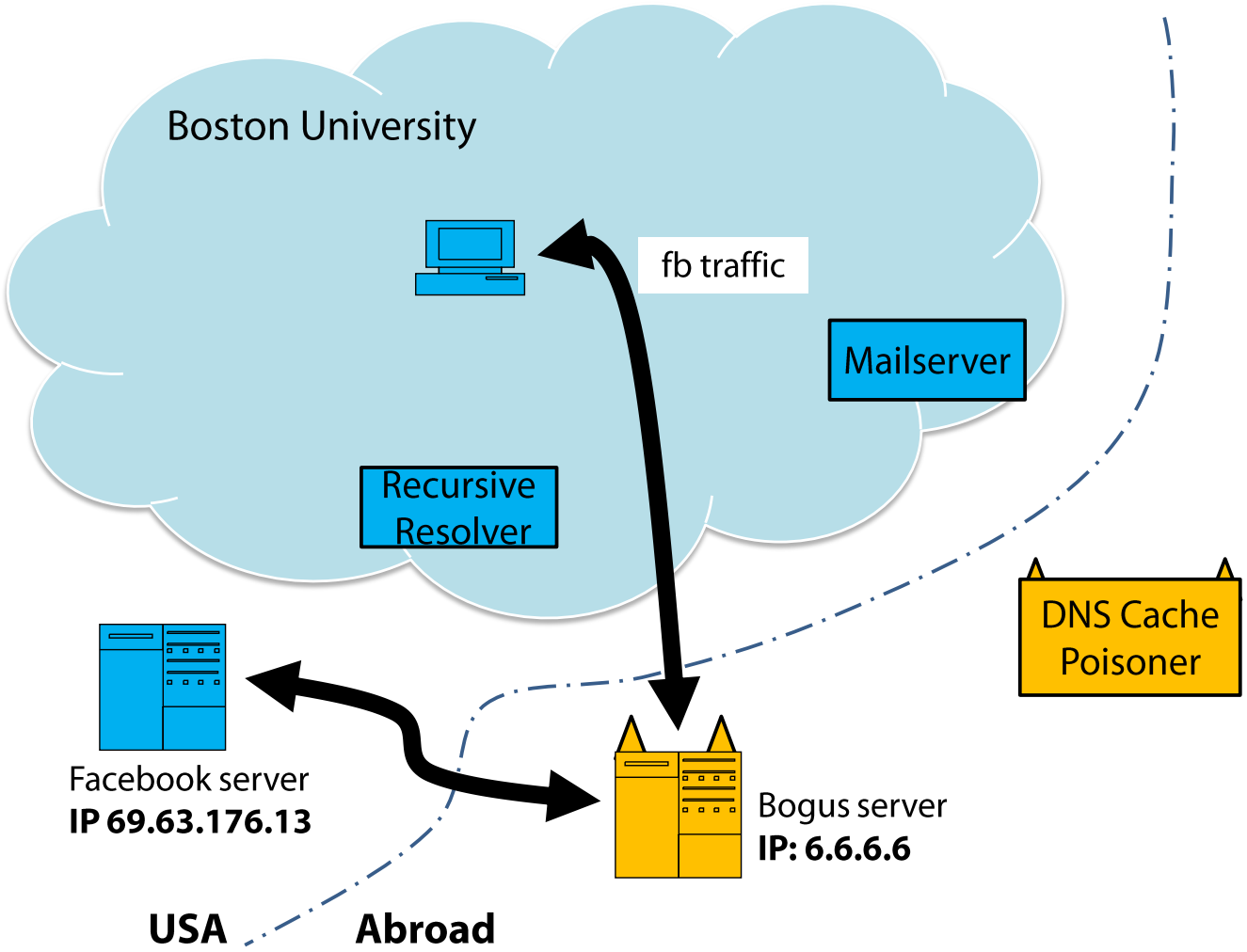
Source: `http://www.renesys.com/2013/11/mitm-internet-hijacking/`

DNS Manipulations Can Divert Traffic Abroad



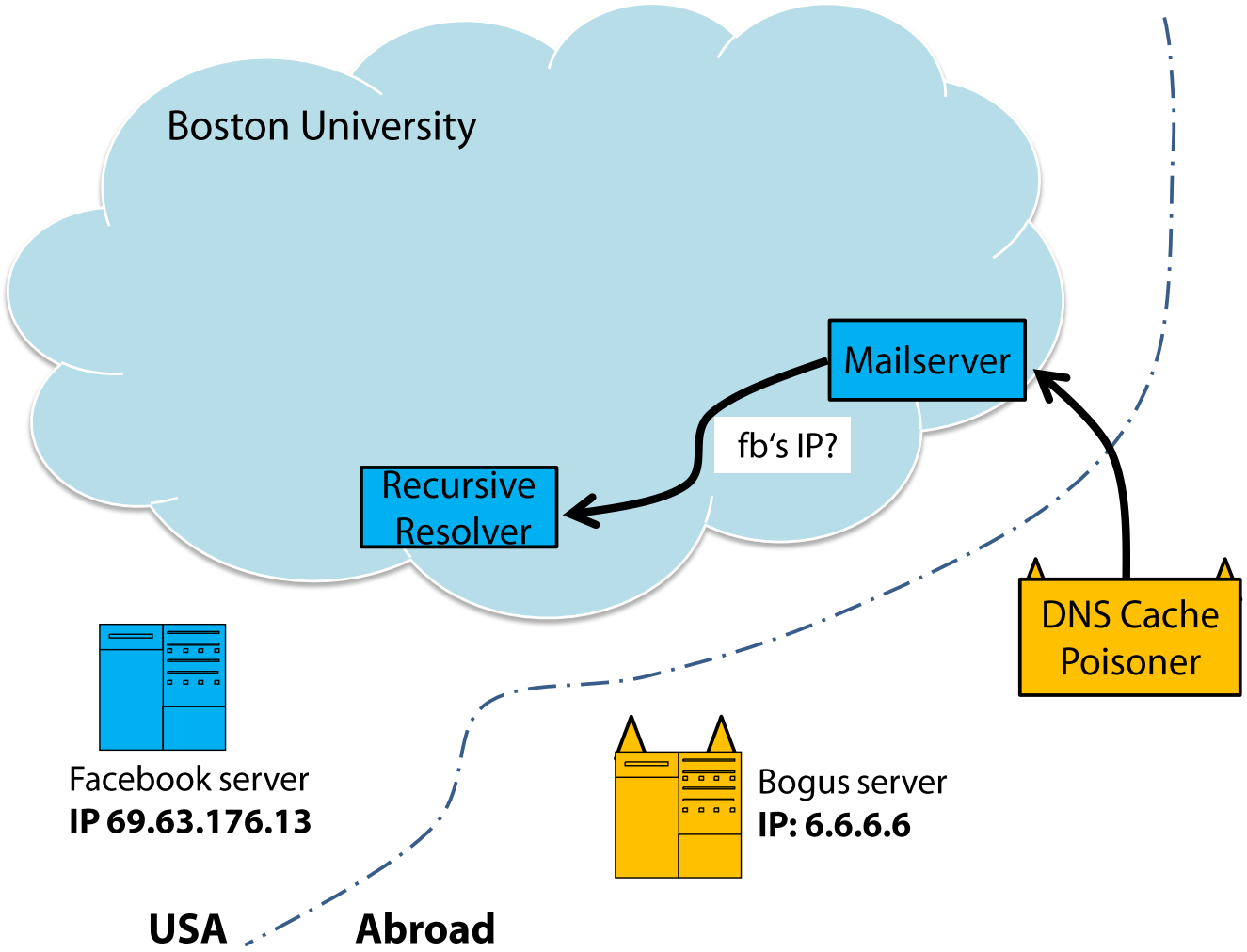
A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

DNS Manipulations Can Divert Traffic Abroad



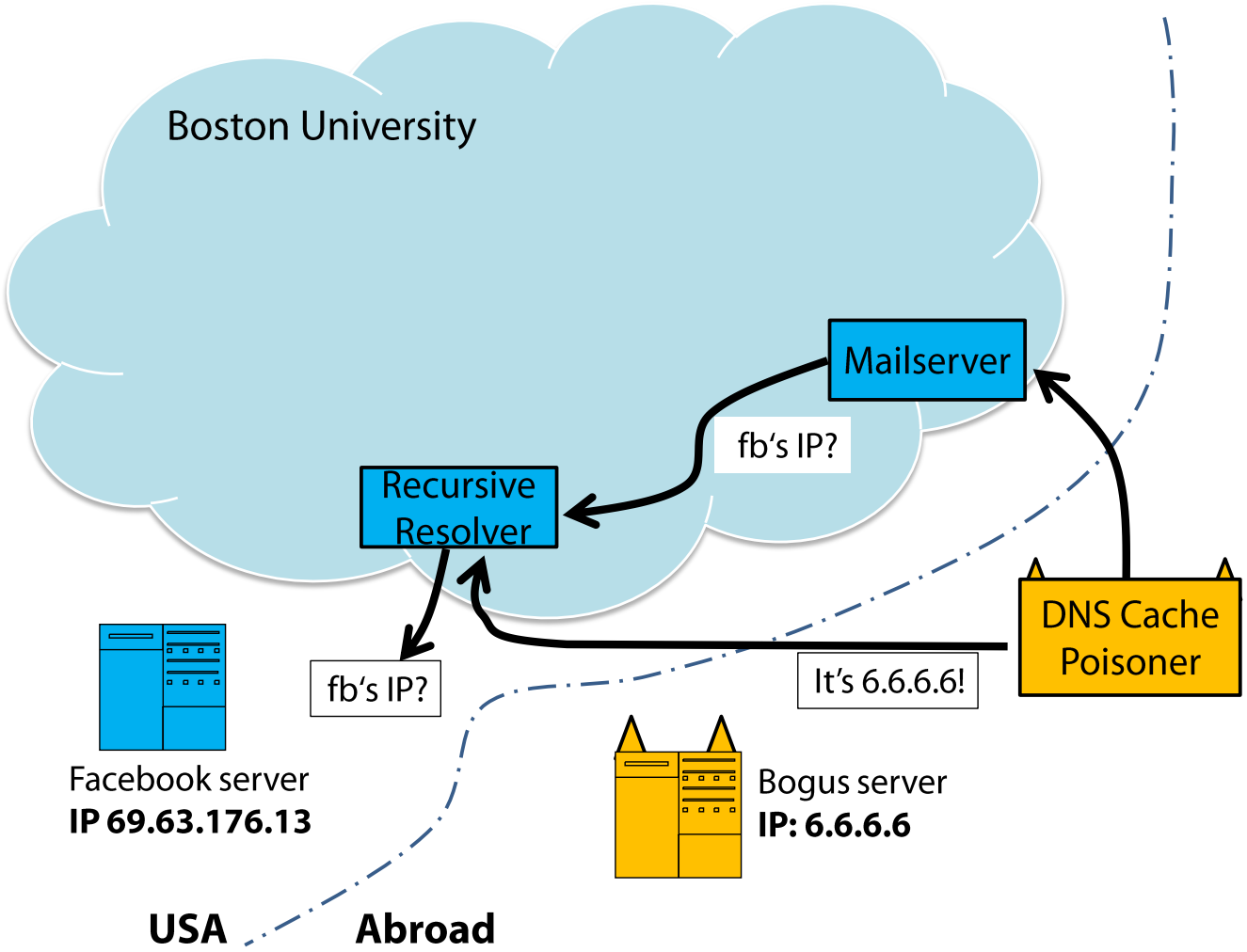
A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

DNS Manipulations Can Divert Traffic Abroad



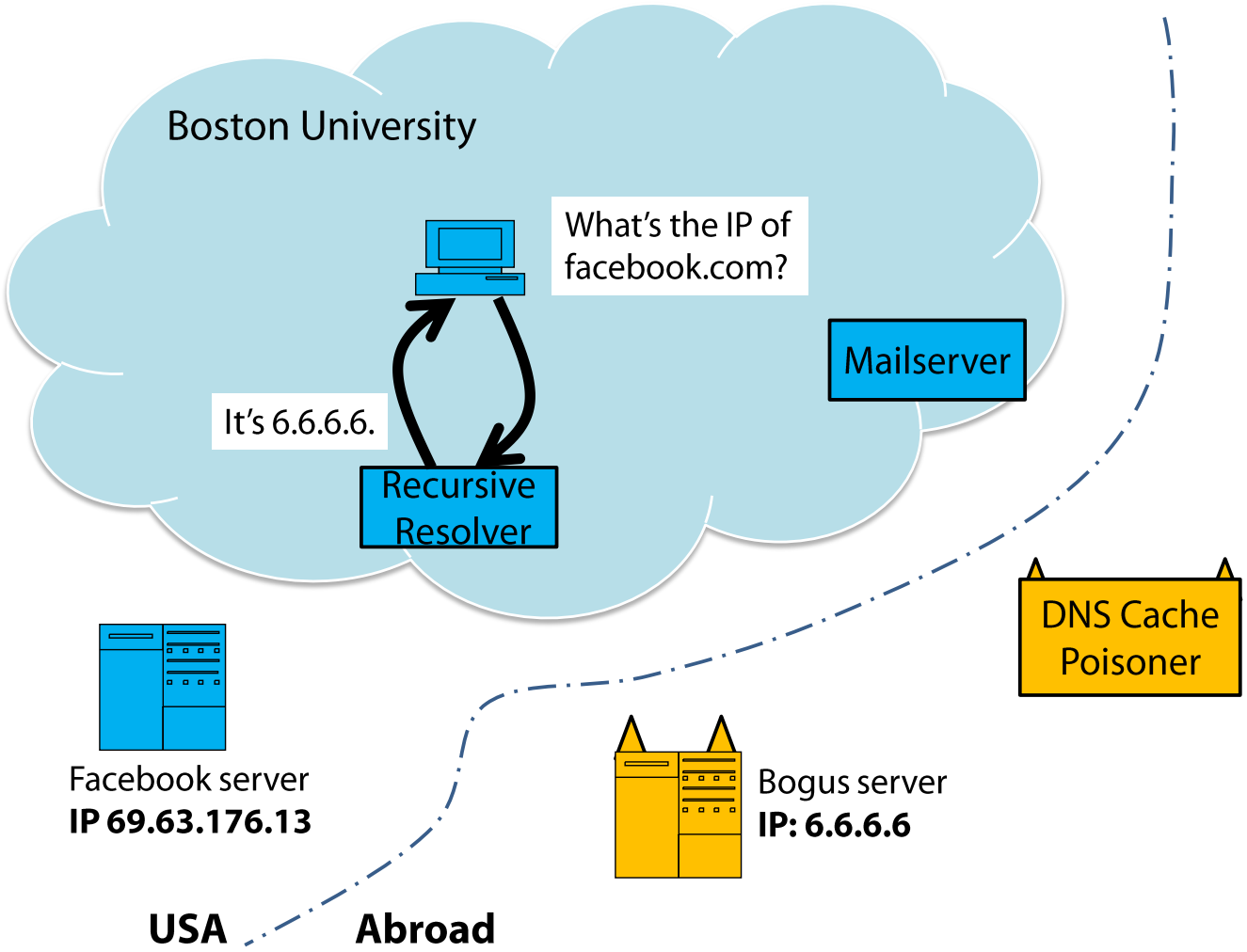
A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

DNS Manipulations Can Divert Traffic Abroad



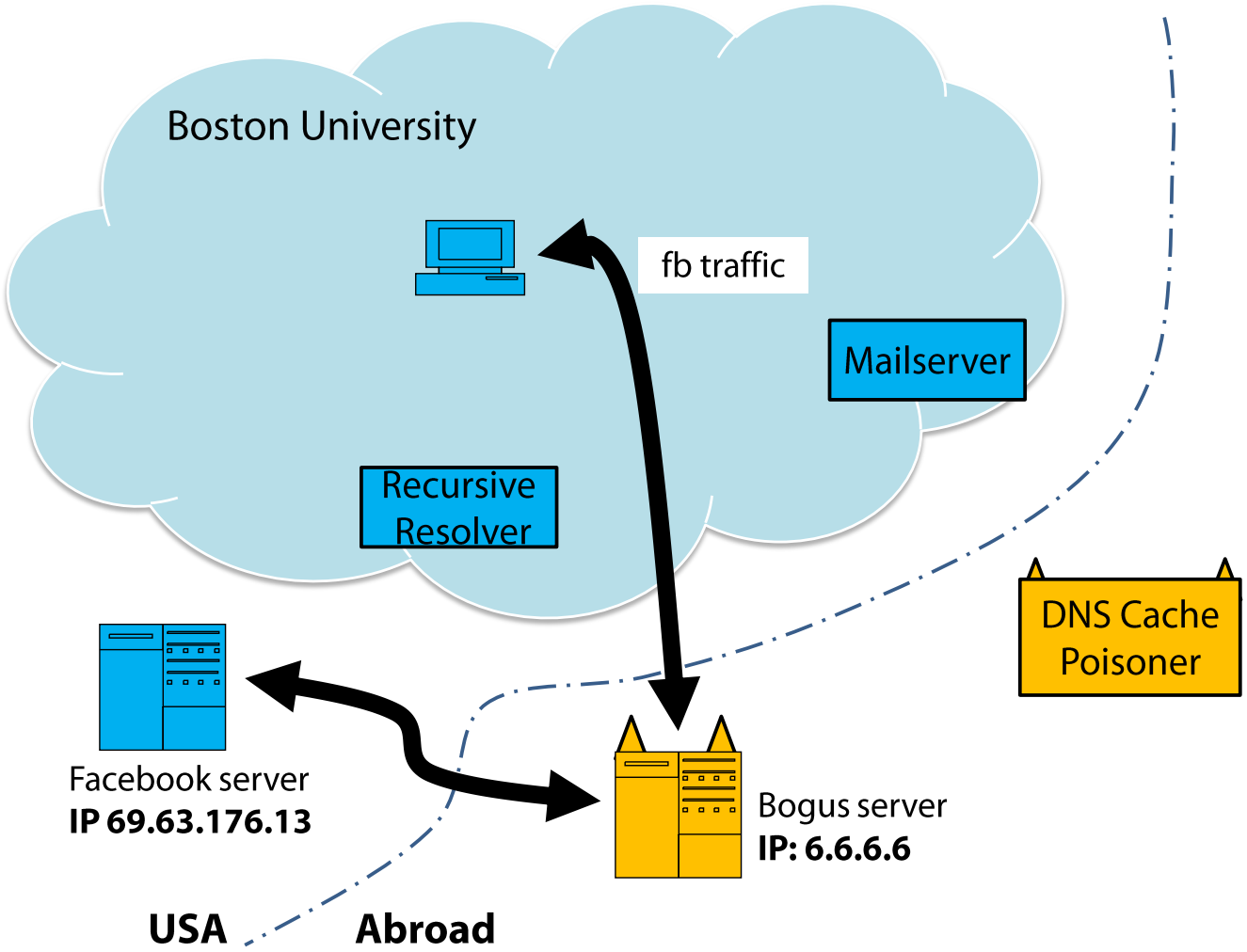
A. Herzberg and H. Shulman. Fragmentation considered poisonous. CNS'13.

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

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.