Loopholes to Circumvent the Constitution
Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad

Axel Arnbak\textsuperscript{1}  Sharon Goldberg\textsuperscript{2}

\textsuperscript{1}Institute for Information Law (IViR, University of Amsterdam);
Harvard University - Berkman Center for Internet & Society

\textsuperscript{2}Computer Science, Boston University

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

http://ssrn.com/abstract=2460462
Legal loopholes could allow wider NSA surveillance, researchers say
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
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’

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

Disclaimer: Arriving at a definite legal conclusion is difficult from the ‘outside’ because many interpretations remain classified.
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:

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,
EO 12333 is more permissive than FISA

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

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.

Source: http://wapo.st/1mVEPXG
A Few Days After We Released Our Paper...

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

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

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

“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

Mapping the Internet: BU/NEU GeoRouting Project

bu/nu Neuroute 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.

BGP Manipulations Can Divert Traffic Abroad

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

BGP Manipulations Can Divert Traffic Abroad

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

DNS Manipulations Can Divert Traffic Abroad

DNS Manipulations Can Divert Traffic Abroad

DNS Manipulations Can Divert Traffic Abroad

Facebook server  
IP 69.63.176.13

Recursive Resolver

Mailserver

fb's IP?

DNS Cache Poisoner

Bogus server  
IP: 6.6.6.6

USA Abroad

DNS Manipulations Can Divert Traffic Abroad

DNS Manipulations Can Divert Traffic Abroad


---

Facebook server
IP 69.63.176.13

Bogus server
IP: 6.6.6.6

DNS Cache Poisoner

USA

Abroad

Recursive Resolver

What’s the IP of facebook.com?

It’s 6.6.6.6.

Mailserver

Boston University
DNS Manipulations Can Divert Traffic Abroad

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
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.
“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.