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

Axel Arnbak¹    Sharon Goldberg²

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

²Assistant Professor, Computer Science, Boston University

Telecommunications Policy Research Conference (TPRC’42).
Arlington, VA. September 13, 2014

http://ssrn.com/abstract=2460462
Legal loopholes could allow wider NSA surveillance, researchers say
Three weeks after the CBS News piece was published...

Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans

By John Napier Tye  July 18

John Napier Tye served as section chief for Internet freedom in the State Department’s Bureau of Democracy, Human Rights and Labor from January 2011 to April 2014. He is now a legal director of...
Quoting John Napier Tye:

“Based in part on classified facts that I am prohibited by law from publishing, I believe that Americans should be even more concerned about the collection and storage of their communications under Executive Order 12333 than under Section 215.

...

Consider the possibility that Section 215 collection does not represent the outer limits of collection on U.S. persons but rather is a mechanism to backfill that portion of U.S. person data that cannot be collected **overseas** under 12333.”

Source: http://wapo.st/1wFc5rX
Outline

Legal Analysis
Three key legal regimes: When EO 12333 applies.
American Internet traffic hardly protected under EO 12333

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

Reactions

Discussion, Possible Remedies
Legal Analysis
Three key legal regimes: When EO 12333 applies.
American Internet traffic hardly protected under EO 12333

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

Reactions

Discussion, Possible Remedies
Three key legal regimes for network surveillance
Legal protection decreases significantly

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

- Foreign Intelligence Surveillance Act, notably s. 702
  - Surveillance Conducted on U.S. Soil
  - International Communications
  - Examples: ‘PRISM’, ‘UPSTREAM’

- Executive Order 12333.
  - ‘Electronic surveillance’ not covered by the FISA definition.
  - ‘Primary legal authority’ according to the NSA.
  - Example: ‘MUSCULAR’

DISCLAIMER: Please read the paper. FISA and EO 12333 are complicated, old and partly still classified law.
Three key legal regimes for network surveillance
Legal protection decreases significantly

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

- Foreign Intelligence Surveillance Act, notably s. 702
  - Surveillance Conducted on U.S. Soil
  - International Communications
  - Examples: ‘PRISM’, ‘UPSTREAM’

DISCLAIMER: Please read the paper. FISA and EO 12333 are complicated, old and partly still classified law.
Three key legal regimes for network surveillance
Legal protection decreases significantly

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

▶ Foreign Intelligence Surveillance Act, notably s. 702
  ▶ Surveillance Conducted on U.S. Soil
  ▶ International Communications
  ▶ Examples: ‘PRISM’, ‘UPSTREAM’

▶ Executive Order 12333.
  ▶ ‘Electronic surveillance’ not covered by the FISA definition.
  ▶ ‘Primary legal authority’ according to the NSA.
  ▶ 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:
  1. Is conducted abroad*, AND
  2. Does not ’intentionally target a U.S. person’.

- Traffic **presumed** ‘foreign’ if the above legal criteria are met.
- Presumed ‘foreign’ entities (i.e., persons, organizations, etc.) receive little constitutional protection in the U.S.
  - US Supreme Court [1990], *United States v. Verdugo-Urquidez*

*May also apply domestically, under partly classified circumstances. See ars.to/1z10Lkg.*
‘Targeting’ vs ‘Incidental’ collection?

To quote John Napier Tye:

“Incidental” collection may sound insignificant, but it is a legal loophole that can be stretched very wide. Remember that the NSA is building a data center in Utah five times the size of the U.S. Capitol building, with its own power plant that will reportedly burn $40 million a year in electricity.

“Incidental collection” might need its own power plant.

FISA ‘targeting’ & ‘minimization’ proc. (dealing w. incidental collection) are public. But under EO 12333, USSID 18 is redacted & other docs remain classified.

Please read the paper for more discussion.
More on ‘targeting’; this covers only FISA, not even EO 12333.

Nearly half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to U.S. citizens or residents. NSA analysts masked, or minimized, more than 65,000 such references to protect Americans privacy, but The Post found nearly 900 additional e-mail addresses, unmasked in the files, that could be strongly linked to U.S. citizens or U.S. residents. ... The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless.

Source: http://wapo.st/1mVEPXG
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.
  - Various definitions in EO 12333 (s. 2.3 and s. 2.4) hardly changed since 1981.

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.
  - Various definitions in EO 12333 (s. 2.3 and s. 2.4) hardly changed since 1981.

- Antiquated laws fail to capture new technologies:
  - Bulk surveillance doesn’t ‘intentionally target a U.S. person’;
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.
  - Various definitions in EO 12333 (s. 2.3 and s. 2.4) hardly changed since 1981.

- Antiquated laws fail to capture new technologies:
  - Bulk surveillance doesn’t ‘intentionally target a U.S. person’;
  - Also, FISA’s definition of ‘installing a device’ for surveillance.

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
  - But, ‘foreignness presumed’ when conducted abroad under USSID 18,
  - USSID 18 s. 4: exceptions overruling 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.

These are only a few of many examples we could give.
Long-term outlook for EO 12333 surveillance & reform:

- Fundamental issue:
  EO 12333 is under the Executive Branch.
  - Wide Executive authorities for overseas national security operations, art. II U.S. Constitution
  - Thus, less 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.
Long-term outlook for EO 12333 surveillance & reform:

- Fundamental issue:
  EO 12333 is under the Executive Branch.
  - Wide Executive authorities for overseas national security operations, art. II U.S. Constitution
  - Thus, less 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.
And after Tye’s Op-Ed appeared, this came out...

Note the “catch-all” authority of EO12333

http://t.co/YbDdp3vh0X
Outline

Legal Analysis
Three key legal regimes: When EO 12333 applies.
American Internet traffic hardly protected under EO 12333

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

Reactions

Discussion, Possible Remedies
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.”

MUSCULAR Source: http://wapo.st/1bCL7HK
Routing can naturally divert traffic abroad.

Mapping the Internet: BU/NEU GeoRouting Project

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

http://georoute.bu.edu/
BGP manipulations can divert traffic abroad.

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.

Why does this BGP manipulation fall under EO 12333?

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

- FISA regulates ‘installing a device’ for surveillance only for ‘other than wire or radio communication’;
  - Thus, EO 12333 regulates this (wireline) BGP manipulation.
Why does this BGP manipulation fall under EO 12333?

DISCLAIMER:

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

- FISA regulates ‘installing a device’ for surveillance only for ‘other than wire or radio communication’;
  - Thus, EO 12333 regulates this (wireline) BGP manipulation.

- No U.S. person is ‘intentionally targeted’.
  - Traffic is collected in bulk.
  - The manipulating router in Iceland broadcasts just one message to its neighbors.
Why does this BGP manipulation fall under EO 12333?

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

▶ FISA regulates ‘installing a device’ for surveillance only for ‘other than wire or radio communication’;
  ▶ Thus, EO 12333 regulates this (wireline) BGP manipulation.

▶ No U.S. person is ‘intentionally targeted’.
  ▶ Traffic is collected in bulk.
  ▶ The manipulating router in Iceland broadcasts just one message to its neighbors.

▶ Traffic is collected abroad, in Iceland.
DNS manipulations can divert traffic abroad.

What's the IP of facebook.com?
It's 69.63.176.13.

Facebook server
IP 69.63.176.13

USA Abroad

DNS manipulations can divert traffic abroad.

DNS manipulations can divert traffic abroad.

DNS manipulations can divert traffic abroad.

DNS manipulations can divert traffic abroad.

DNS manipulations can divert traffic abroad.

DNS manipulations can divert traffic abroad.

DNS manipulations can divert traffic abroad.

Why does this DNS manipulation fall under EO 12333?

DISCLAIMER:

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

- FISA regulates ‘installing a device’ for surveillance only for ‘other than wire or radio communication’;
  - Thus, EO 12333 regulates this (wireline) DNS manipulation.
Why does this DNS manipulation fall under EO 12333?

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

- FISA regulates ‘installing a device’ for surveillance only for ‘other than wire or radio communication’;
  - Thus, EO 12333 regulates this (wireline) DNS manipulation.

- No U.S. person is ‘intentionally targeted’.
  - Traffic from Boston University is collected in bulk.
  - The target is traffic from not-yet-identified users or machines.
  - (As in the MUSCULAR program).
Why does this DNS manipulation fall under EO 12333?

DISCLAIMER:

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

- FISA regulates ‘installing a device’ for surveillance only for ‘other than wire or radio communication’;
  - Thus, EO 12333 regulates this (wireline) DNS manipulation.

- No U.S. person is ‘intentionally targeted’.
  - Traffic from Boston University is collected in bulk.
  - The target is traffic from not-yet-identified users or machines.
  - (As in the MUSCULAR program).

- Traffic is collected abroad, at the bogus server.
Legal Analysis
Three key legal regimes: When EO 12333 applies.
American Internet traffic hardly protected under EO 12333

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

Reactions
Discussion, Possible Remedies
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

"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
Privacy and Civil Liberties Oversight Board (PCLOB) is now investigating EO 12333.

http://wapo.st/1A6cCYk
Outline

**Legal Analysis**
Three key legal regimes: When EO 12333 applies.
American Internet traffic hardly protected under EO 12333

**Technical Analysis**
American traffic can naturally flow abroad
Protocol manipulations can divert traffic abroad

**Reactions**

**Discussion, Possible Remedies**
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.
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.
  ▶ For example, by manipulating BGP or DNS.
  ▶ Many other techniques are possible. (See paper.)
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.
  - For example, by manipulating BGP or DNS.
  - Many other techniques are possible. (See paper.)

- EO 12333 regime is entirely under the Executive branch.
- Many legal interpretations remain classified.
- The PCLOB investigation is also under the Executive branch.
Possible remedies?

- Technical solutions can help, but are not a panacea:
  - Even encrypted traffic leaks ‘metadata’
  - DNSSEC can secure DNS, but is far from being fully deployed.
  - The RPKI can stop some attacks on BGP, but not all. Also, its not fully deployed yet either.

Update antiquated FISA definition of ‘electronic surveillance.’
And of ‘installing a device.’
Reconsider core principles in U.S. surveillance law:
1. Whether the point of collection determines the legal regime.
2. Whether collection (not ‘targeting’) constitutes privacy harm.
3. Whether foreigners enjoy Fourth Amendment protections.

Thanks!
Possible remedies?

- Technical solutions can help, but are not a panacea:
  - Even encrypted traffic leaks ‘metadata’
  - DNSSEC can secure DNS, but is far from being fully deployed.
  - The RPKI can stop some attacks on BGP, but not all. Also, its not fully deployed yet either.

- Update antiquated FISA definition of ‘electronic surveillance’. And of ‘installing a device’.
Possible remedies?

- Technical solutions can help, but are not a panacea:
  - Even encrypted traffic leaks ‘metadata’
  - DNSSEC can secure DNS, but is far from being fully deployed.
  - The RPKI can stop some attacks on BGP, but not all. Also, it’s not fully deployed yet either.

- Update antiquated FISA definition of ‘electronic surveillance’. And of ‘installing a device’.

- Reconsider core principles in U.S. surveillance law:
  1. Whether the point of collection determines the legal regime.
  2. Whether collection (not ‘targeting’) constitutes privacy harm.
  3. Whether foreigners enjoy Fourth Amendment protections.
Possible remedies?

- Technical solutions can help, but are not a panacea:
  - Even encrypted traffic leaks ‘metadata’
  - DNSSEC can secure DNS, but is far from being fully deployed.
  - The RPKI can stop some attacks on BGP, but not all. Also, it's not fully deployed yet either.

- Update antiquated FISA definition of ‘electronic surveillance’. And of ‘installing a device’.

- Reconsider core principles in U.S. surveillance law:
  1. Whether the point of collection determines the legal regime.
  2. Whether collection (not ‘targeting’) constitutes privacy harm.
  3. Whether foreigners enjoy Fourth Amendment protections.

Thanks!
Collection with ‘consent’ of the ‘U.S. Person’; s. 4.1.c(1) USSID 18

(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:

c. (U/FOUO) With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

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
Exemptions for processing ‘U.S. Person’ data; s. 5.4.d USSID 18

(U) Intercepted Material

5.3. (U) Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

5.4. (U) Non-foreign Communications.

a. (U) Communications between persons in the UNITED STATES. Private communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. (U) Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) (U) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) (U) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

(a) (U) Establish or maintain intercept, or

(b) (U) Minimize unwanted intercept, or

(c) (U) Support cryptologic operations related to FOREIGN COMMUNICATIONS.
Exemptions for processing ‘U.S. Person’ data; s. 5.4.d USSID 18

d. (U) Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

(1) Significant FOREIGN INTELLIGENCE, or

(2) Evidence of a crime or threat of death or serious bodily harm to any person, or

(3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS’s waiver is sought should be forwarded to NSA/CSS, Attn: Signals Intelligence Directorate Office of Oversight & Compliance (SV).

‘foreign intelligence’ is information ‘relating to the foreign affairs of the U.S.’ (cf. art. 1801(e)(2) of FISA).
Relevant legal documents

- s. 2 USSID 18

(U) References 2.1 (U) The following documents are references to this USSID:

- (U) 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, as amended.

- NSA/CSS Policy No. 1-23 refers to a classified Annex A of EO 12333 and the DoD Directives, which is particularized for N.S.A. conduct.

- See also http://www.emptywheel.net/2014/05/30/snowden-a-classified-executive-order/
This is the issue date; revisions or renewals have occurred since the issue date.