Global Citizens and the U.S. Security Surveillance Dragnet

Center for Democracy & Technology

Webinar 18 July 2013

Purpose of Webinar

- Explain laws under which the U.S. National Security Agency conducts surveillance
- Constitutional and Legal Issues
- Human rights and policy ramifications
- Implications for global community
- How NGOs outside the U.S. can become more engaged

U.S. Law:
Intelligence vs. Criminal Surveillance

- Intelligence surveillance is mostly a separate statutory regime from criminal surveillance
- Key difference: purpose of surveillance
- Foreign Intelligence Surveillance Act or FISA authorizes the government to conduct surveillance to collect "foreign intelligence information" from targets inside and outside the US

FISA: Domestic vs Foreign

- Domestic: for intelligence surveillance of people in the U.S., regardless of citizenship
- relatively robust protection of intelligence
  - Court authorizes
  - Probable cause target is a spy, terrorist, or another agent of foreign power
  - Purpose: collect "foreign intelligence information"

FISA: Domestic vs Foreign

- Domestic: weak protection for non-content
- Section 215 of PATRIOT Act:
  - "relevant" to investigation
  - "tangible things" including
  - Metadata for telephone calls to/from/within US
  - Not a webinar focus, but will be happy to take questions
- Pen/Trap: prospective metadata surveillance on weak relevance standard (also not a focus)

Domestic vs. Foreign

- Foreign: FISA's protections for targeting non-Americans abroad are very weak
  - 2008 FISA Amendments Act ("Section 702")
  - No court authorization
  - No finding of probable cause
  - Targeting and minimization guidelines designed to protect Americans only
  - Purpose limitation – collect "foreign intelligence information" is the only real "protection" for people outside the U.S.

"Foreign Intelligence Information"

- Broadly defined
- Ranges from information about a terrorist attack to information relating to a protest a US base
- No court review, except with respect to targeting
- Not much protection for non-Americans

"Foreign Intelligence Information"

Foreign intelligence information is info that relates to:

- Potential hostile act by foreign power
- Sabotage, international terrorism, or espionage
- Information with respect to foreign power or foreign territory that relates to:
  - U.S. national security
  - U.S. foreign affairs
- Information that concerns an American must also meet a necessity test: must be "necessary" to protect against the hostile act, sabotage, terrorism, espionage, or to national security or foreign affairs. 50 USC 1801(e).

How Accessed: "Upstream"

- NSA taps into fiber optic cable
- Upstream surveillance can occur underseas, at cable head, or at network junctions in U.S.
- Some is encrypted
- Likely executed with assistance of large telecoms
- Section 702 directives relating to that surveillance so far non-public

How Accessed: "Downstream" PRISM

- An NSA system used to execute surveillance with the help of participating providers, Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple
- NSA surveillance request
  - Is a person, entity or personal identifier
  - Subject matter
  - Dynamic -- not approved by FISA Court
  - Report: 117,675 active PRISM targets at 5 April 2013
  - Companies deny direct access to servers

Targeting Guidelines

- Purpose: determine that target is non-American reasonably believed to be outside the U.S.
- Factors include: statements of target, human intelligence, analysis of target's contacts, review of NSA databases
- Presumption: non-American
- 51% rule (not in guidelines)

Minimization Guidelines

- Goal: minimize acquisition, dissemination and use of non-public info concerning Americans acquired by targeting people abroad
- Reality: "incidental" collection of Americans' communications with targets abroad is intended
- Is retained if includes foreign intelligence information or is encrypted
- Is provided to FBI and others if evidence of crime, serious or not, and NSA holds for 6 months
- Even attorney-client communications can be used for intelligence purposes (not in prosecution)
- Information on non-Americans is not subject to minimization and can be retained and used for any legal purpose.

Substantive Legal Challenges

- Clapper v. NSA (ACLU, 2008):
  - Human rights advocates and journalists challenge Section 702 under U.S. Constitution
  - Supreme Court dismissed on procedural grounds in Feb., 2013
- Jewel v. NSA (EFF, 2008, N.D. Cal.)
  - AT&T customers allege that mass surveillance violates U.S. Constitution and multiple surveillance statutes
  - District court rejected government's state secrets claims, dismissed the statutory claims, and allowed the constitutional claims to go forward. Case is pending
- Yahoo v. NSA (2008, at FISA Court)
  - Yahoo unsuccessfully challenged on statutory and constitutional grounds a directive issued to it under predecessor to Section 702.

Transparency Litigation

- Yahoo successfully urged FISA Court and FISA Court of Review to require government to disclose opinions and legal papers associated with its challenge. Disclosure due 26 Aug. 2013.
- Google and Microsoft, supported by civil society groups, petition FISA Court to allow disclosure of number of FISA surveillance requests received and people affected. Filed June 2013.
- Round-up of substantive challenges and transparency litigation: https://www.cdt.org/content/status-select-litigation-relating-nsa-spying-july-16-2013

Transparency Advocacy

- Letter: dozens of companies, trade associations and civil society groups released a letter a few minutes ago urging government to allow companies to disclose FISA surveillance numbers at granular level. https://www.cdt.org/files/pdfs/weneedtoknow-transparency-letter.pdf

- Legislation: bills introduced in Congress to require or encourage the government to disclose significant FISA court opinions or unclassified summaries:
  - S. 1130 "Ending Secret Law Act" (Merkley & 14 others)
  - H.R. 2399 LIBERT-E Act (Amash/Conyers & 40 others)

Summary

- FISA Section 702 empowers the NSA to compel providers of communications service to assist with broad surveillance authorities that targets non-Americans abroad.
- The amount of information collected is probably enormous.
- Targeting and minimization guidelines protect the interests of Americans only, and they don't do it well. Don't protect non-Americans.
- Substantive legal challenges focus mostly on the rights of people in the U.S., who have rights under the U.S. Constitution.
- Substantial efforts are underway to encourage more disclosure about the surveillance.
- Little debate in Washington accounts for the rights of people abroad who may be the targets of surveillance.

Human Rights Concerns Inadequately Addressed To Date

- Int'l Covention on Civil & Political Rights Art. 17
  - No arbitrary or unlawful interference with privacy … or correspondence
  - Protection of the law against such interference
- Principles on Application of Human Rights To Communications Surveillance
  - Notice of law (transparency)
  - Legitimate goal
  - Necessary and proportionate means to achieve goal
  - Authorized by competent legal authority
  - Public oversight

Other Articlulations of Human Rights Concerns

- April 17, 2013 Surveillance Report of Frank LaRue, the UN Special Rapporteur on the promotion and protection of freedom of opinion and expression: https://www.cdt.org/Z4s
- Ruggie Report: Guiding Principles on Business and Human Rights: Implementing UN Protect, Respect and Remedy Framework: https://www.cdt.org/Z4e
  - Sets forth companies' duties to respect human rights

Privacy and Civil Liberties Oversight Board (PCLOB)

- Newly re-constituted independent agency in Executive Branch of US
- Makes recommendations and findings about anti-terrorism measures to protect privacy and civil liberties.
- Conducted a July 9 workshop on Section 702 and PATRIOT Section 215 surveillance and will issue a report
- Statutory mandate not limited to rights of Americans

Advocacy Opportunity: PCLOB

- Civil society groups could urge PCLOB to account for the human rights of people abroad when it issues findings and recommendations about the Section 702 program
- CDT will soon circulate a draft sign-on letter

EU Data Protection: the FISA Amendment

- EU Parliament is considering a new comprehensive data protection regulation
- Proposed Article 42 would require data controllers and processors who receive surveillance requests from outside the EU to get permission from a supervisory authority before disclosing personal data
- Consistency with Article 2, which puts national security matters outside the scope of the EU data protection directive, may be called into question.

EU Data Protection: Advocacy Opportunities

- Regardless of whether it is adopted, Article 42 opens up discussion of trans border data flows for national security reasons.
- Possible approach: advocate for Article 42
  - Pressures U.S. to disclose more about Section 702 use
- Possible approach: advocate for requirement that personal data may not be exported to a country that seeks it for national security or law enforcement purposes unless country law and practice meets an adequate protection standard.
  - Encourages stronger standards for law enforcement and security surveillance worldwide.

Conclusion

Discussion of Other Advocacy Opportunities

and of Next Steps