The Brave New World of Domestic Surveillance

Elizabeth Goitein

Co-Director, Liberty and National Security Program

Brennan Center for Justice at NYU School of Law

March 31, 2022

Legal Changes

History of U.S. Intelligence Collection (Early Cold War)

Lack of statutory charter or internal limitations on intelligence-collection activities

Domestic spying during the early decades of the Cold War, particularly targeting social justice movements, anti-war activists, and political opponents

Watergate-era revelations of executive overreach

- Church Committee (1975-1976) uncovered that the FBI, CIA, and NSA had been engaged in surveillance of Americans for decades

Post-Watergate Reforms

Policies/laws adopted the **"Golden Rule"**: Intelligence and law enforcement agencies may not collect information on Americans without **individualized**, **fact-based** suspicion of wrongdoing.

1. Attorney General Guidelines for Domestic FBI investigations
   - Required objective factual basis to suspect illegal activity
   - Placed limitations on collection of information about First Amendment-protected activities
2. National Security Letters
   - Communications records and financial/credit records protected by law
   - FBI may obtain records for foreign intelligence investigations with a "National Security Letter"…
   - …but must have "specific and articulable facts" indicating that the subject of the records was a foreign powers or agent of a foreign power
3. Foreign Intelligence Surveillance Act (FISA)
   - When the government is acting inside the United States, it must apply to Foreign Intelligence Surveillance Court to obtain communications to which a U.S. person is a party
   - Court may grant order only if government shows probable cause that the target is a foreign power or agent of a foreign power

Post-9/11 Erosion

1. Attorney General weakened FBI guidelines

   - "Reasonable suspicion" standard before sending agents into political/religious gatherings eliminated
   - New type of investigation, an "assessment," permitted intrusive investigative techniques with *no* factual basis to suspect criminal activity

2. Congress lowered standard for National Security Letters

   - Subject of records need not be a foreign power or agent of foreign power
   - Only restriction is that records must be "relevant" to investigation

Section 702 of FISA, in theory

Government may collect communications of any foreigner overseas, including communications with Americans, **without** an individualized court order

Substantive limitations:

- A significant purpose of surveillance must be acquiring "foreign intelligence"—defined to include any information that "relates to". . . "the conduct of foreign affairs of the United States"
- Targets of surveillance need not be foreign powers or agents of foreign powers

Ostensible protections for U.S. persons:

- Government must certify that its purpose is not to access the communications of any particular, known U.S. person
- NSA is required to "minimize" the **sharing, retention, and use** of "incidentally" collected U.S. person data

Section 702 of FISA, in practice

Minimization requirements have become maximal

- NSA shares raw data with multiple agencies (CIA, FBI, National Counterterrorism Center), which retain it for >5 years

Section 702 used to access Americans' communications

- All agencies with access to raw Section 702 data are allowed to perform "U.S. person queries"
- FBI routinely conducts U.S. person queries in purely domestic criminal assessments and investigations

Section 215, in theory

Pre-9/11, the government could apply to the FISA Court to obtain business records in foreign intelligence investigations

- The government had to show that subject of the records was a foreign power or agent of a foreign power

Section 215 of the USA PATRIOT Act (2001) expanded this authority

- The FISA Court could now allow the government to obtain "any tangible thing…"
- …as long as the thing was **relevant** to a foreign intelligence investigation

Seemingly retained the requirement of an **individualized showing** (albeit not necessarily a showing of wrongdoing)…

Section 215, in practice

Edward Snowden's disclosures (2013): **bulk collection** of Americans' phone records

- Foreign Intelligence Surveillance Court allowed the National Security Agency (NSA) to engage in bulk (non-targeted) collection of records from multiple major telephone companies, on the theory that relevant records might be buried within irrelevant ones
- The records collected included, for each customer X:
  - A list of number called by X
  - A list of numbers that had placed calls to X
  - What times each call took place
  - How long each call lasted
- That "metadata" can be crunched to reveal people's associations, activities, and beliefs

Section 215: Post-Snowden Developments

Snowden disclosures → public outrage → USA Freedom Act (2015)

- Ended NSA bulk collection; prohibited future bulk collection under Section 215 and other authorities

Section 215 reauthorization (2020)

- Trump's opposition to FISA sounded Section 215's death knell…
- …but permissive "relevance" standard persists in other surveillance and intelligence-collection contexts

Technological Changes

Records Held by Third Parties

In the 1970s, the government could acquire some personal information by looking to credit histories, phone bills, bank statements, and similar information, but would likely have difficulty using such sources to assemble a comprehensive picture of an individual's personal life.

Today, people disclose extensive amounts of personal information to third parties on a daily basis:

- Web browsing history
- E-mails channeled through internet service provider
- Documents stored in the cloud
- Text messages
- Location data

Computer programs are also now capable of synthesizing this data to reveal even more sensitive information.

Jurisprudence: The "Third Party Doctrine"

Smith v. *Maryland* (1979): police officers do not need a warrant to install a tracing device on a phone line

- A person has **no reasonable expectation of privacy** in information that is **voluntarily** disclosed to a third party ("third party doctrine")

Questions about *Smith*:

- Was it wrongly decided at the time? Is privacy a binary condition?
- Have intervening developments undermined its logic? Does living in the modern world *require* third-party disclosures (to Google, to Verizon, and so on)? Is modern surveillance more comprehensive and therefore more intrusive?

Carpenter v. *United States* (2018): police officers need a warrant to compel a telephone company to turn over cell site location records

- The third party doctrine retreats when privacy intrusions are severe and inescapable

Commercial Data

The government's interpretation of *Carpenter*: a warrant is required only when the government *compels* disclosure of geolocation data, not when it *incentivizes* disclosure.

Electronic Communications Privacy Act (1986) bars phone and Internet companies from voluntarily disclosing some customer information to government agencies.

Does **not** apply to:

- App developers
- Digital data brokers

Upshot: Phone and Internet companies cannot sell customer records to the government. But they can launder them through a data-broker "middleman."

- FBI, Drug Enforcement Administration, Department of Homeland Security, IRS, Department of Defense have purchased databases of geolocation information without a warrant
- Agencies can easily de-anonymize anonymized data

Technology, Globalization, and International Communications

In 1978 (when FISA was enacted), international calls were relatively rare. Today, they are commonplace.

- **90 billion minutes** of phone calls to and from the United States (2013)
- **300 billion emails** sent and received each day (2019)

Entanglement of the "domestic" and "foreign" spheres:

- Four times as many Americans live and work overseas now versus in 1978
- Proportion of foreign-born individuals in the United States has more than doubled
- International travel is routine

→ Surveillance of foreign targets is more likely to capture Americans' communications

Non-U.S. Perspectives on U.S. Surveillance

1. Advances in data-storage and data-processing technology allow the NSA to be less selective in targeting foreign nationals, compromising their privacy in addition to that of their American correspondents
2. U.S. surveillance laws and practices complicate data-sharing agreements between companies in the United States and European Union
    - Court of Justice of the European Union (CJEU) struck down “Safe Harbor” agreement in 2015
    - CJEU struck down “Privacy Shield” in 2020
    - 5,000 U.S. companies rely on those agreements to conduct business
    - Biden administration announced agreement on principles of new agreement, but… how long will it last?

Overseas Surveillance

Subject to neither statutory limitations nor judicial review (unless the target is a specific U.S. person)

Governed by Reagan's Executive Order No. 12333 (1981): much more permissive than the statutory schemes Congress created for surveillance inside the United States

Justification for distinguishing between domestic and overseas surveillance no longer holds:

- Americans' communications now routed and stored all over the world
- Bulk collection overseas will almost inevitably sweep in Americans' data

The CIA's Bulk Collection Program

Wyden-Heinrich disclosures (2022): CIA has been operating a bulk collection program for years

What we know:

- This collection sweeps in Americans' data
- CIA has been searching the data for Americans' information

Lingering questions:

- How does the CIA obtain this information?
- How does the CIA use this information?
- Why is there less public outrage about this disclosure than about Snowden's?

Consequences of Legal and Technological Changes

What Happens When There's No Golden Rule

The government may ~~not~~ collect information on Americans ~~unless it has~~ **without** individualized, fact-based suspicion of wrongdoing.

→ Undermines privacy

→ Undermines civil rights

- Leads to increased targeting of people of color, political protestors, and other marginalized communities

Examples across administrations:

- Post-9/11: FBI training instructions focused on individuals who grew beards, attended mosques, and expressed political grievances
- 2010: DOJ Inspector General found that FBI agents monitored left-leaning groups without adequate reason
- 2015: Department of Homeland Security (DHS) monitored social media posts of civil rights leaders protesting racism in policing
- 2018: Immigration and Customs Enforcement tracked anti-Trump protests in New York City
- 2020: DHS analyzed racial justice protestors' text messages and retained intelligence on journalists
- 2020: Department of Defense purchased geolocation information from Muslim prayer app

Questions?