Digital Communications & Data Analytics: Some Privacy, National Security & Law Enforcement Issues

Professors Dan Richman & Matt Waxman
Columbia Law School

Some Basic Constitutional Background

- 4th Amendment says: [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause…"
  - Searches must be reasonable, and they generally require a warrant
- Only after 1967 did this apply to the content of phone conversations
- Supreme Court cases in the 1970s held that accessing certain things, including transactional records (think metadata), is not a search

What Does this Mean in Today's Digital World?

- "Translation" challenges: how does 4th Amendment apply to email? Browser history?

- Issues of scale & pervasiveness of data collected and analyzed:

  - Justice Sotomayor in *United States v. Jones* (2012): "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."

- Who should make the rules?

A Brief Example: Snowden & Telephony Metadata

- This program basically involved collection of call data (but not content) for all phone calls in the United States, which was then analyzed under certain specific protocols.

- One, among many, legal questions was whether there's a 4th Amendment issue here (since in the 1970s, the Supreme Court said that phone call records are not protected).
  - Does magnitude of data and the way the data is used alter that analysis?

Encryption & "Going Dark"

- Consider cell tower debate
- Debate becomes more heated with encryption development and marketing
  - Risks making warrants irrelevant
- Examples: Apple iPhone, WhatsApp, etc.
- Privacy, information security, national security, law enforcement interests

Encryption & "Going Dark" (II)

- What does debate look like?
  - Business model arguments
  - "Golden Age of Surveillance"
  - Good for only the dumb bad guys

- What are some proposed solutions
  - Let the market decide
  - Government-mandated access

- Are there intermediate solutions?
  - Data at-rest vs. in-motion
  - International coordination?
  - Government hacking (perhaps with vulnerability disclosure)?