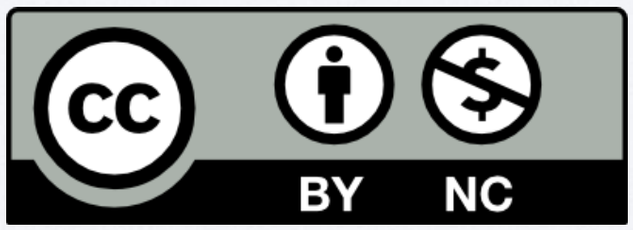
PRIVACY: MODERN CONCERNS

Steven M. Bellovin
https://www.cs.columbia.edu/~smb



It's Not a New Issue

- The Committee on Science and Law of the New York City Bar Association started its formal privacy study in 1962
    - This led to Alan Westin's 1967 book "Privacy and Freedom", a report on the committee's work
- The US Congress held hearings on technology and privacy throughout the 1960s
- Legal academics wrote extensively on the topic
- (Jewish writings circa 200 CE mention a right to physical privacy, and derive it from a Biblical text)

Notice and Consent

- **Westin**: "A central aspect of privacy is that individuals and organizations can determine for themselves which matters they want to keep private and which they are willing—or need—to reveal."

- This has been the basis for virtually *all* privacy regulation since then

Privacy Regulation

1973: A US government committee came up with the "Fair Information Practice Principles"

1974: The US government passes the *Privacy Act of 1974*, implementing them —but only for the Federal government

1980: The OECD guidelines suggested more or less the same thing

1994: The *Data Protection Directive* is enacted

2012: The GDPR is adopted

From 10,000 meters, all of these are more or less the same: notice and consent

Notice and Consent

- Sites tell you what they'll collect, and what they'll do with it

- By using the site, you are deemed to have consented to this policy

There Are Problems

Westin: "It should be recognized that consent to reveal information to a particular person or agency, for a particular purpose, is not consent for that information to be circulate to all or used for other purposes."

Michael: "The would-be invader who knows about these centralized or clustered inventories need not search for sources, and therefore he may be much more inclined to examine the records than if a major search for the sources of information were necessary."

Michael: "We can expect a great deal of information about the social, personal, and economic characteristics of individuals to be supplied voluntarily—often eagerly—in order that, wherever they are, they may have access to the benefits of the economy and the government."

Security Considerations

- **Miller:** "Another important security function that a privacy-oriented monitor program must perform is the identification of all users and terminals attempting to gain access to the files"

- He went on to suggest call-backs, token identification, and biometrics

Passwords

Dr. PIORE. The user then keys in his six-character password.

Senator LONG. Doctor

Dr. PIORE. Yes?

Senator LONG. But he could give that password to someone else, could he not?

Dr. PIORE. He can, and you find that some people do not protect their own password, and this is a human characteristic. You have a friend, and he says, "Let me use your program." It is like saying "Come up to my apartment, and here is the key to my apartment."

(US Senate Committee hearing)

Encryption

- **Miller:** "In the case of remote-access systems, protection against wiretapping can be achieved by using 'scramblers' to garble the data before transmission, and installing complementary devices in the authorized terminals to reconstitute the signal."

- "Coding has a number of tangential advantages from the privacy perspective, including verifying the source of an inquiry or input"

Hackers and Insiders!

- **Miller:** "Even the most sophisticated set of safeguards can be undermined by the people who gain access to the system in one fashion or another. The reports of college students at MIT and elsewhere defeating the monitor protections in time-sharing projects emphasize the reality of this threat."

- "There is a danger that these people will become so entranced with operating sophisticated machine systems and manipulating large masses of data that they will not be sufficiently sensitive to the question of privacy."

Metadata

Miller: "One of the simplest of the present generation of snooping devices is the pen register, which, when attached to a telephone line, records on paper a series of dashes representing all numbers dialed from the selected telephone. But this snooping capability would be increased by several orders of magnitude if a few pen registers were attached to suspects' telephone lines and the information drawn in by these devices fed into a central computer. This technique could quickly provide a revealing analysis of patterns of acquaintances and dealings among a substantial group of people."

"Optical scanners designed to decipher license numerals and send them directly to the computer obviously would make the process more efficient—and, as a by-product, might enable the compilation of comprehensive records of the movements of a person's automobile, perhaps for later inferential relational analysis."

Where Are We?

- We have not solved the technical problems identified more than 50 years ago
- But we still have notice and consent
- Does it work?
- Nope…

Problems With Notice and Consent

- Amount of data collected, and by whom
- Privacy policies
- Location data is collected, often without folks' knowledge
- Many governments

Overcollection

- Data brokers—outside parties with whom consumers have no association, and to whom they have never consented—collect, buy, and sell a tremendous amount of data

- Websites track users

- Ads are from outside brokers, who use HTTP redirection to gather even more data

- Also: third-party "like" buttons (e.g., Facebook and Twitter) and third-party authentication (e.g., Facebook and Google)

Analytics Platforms

"To those first-party profiles, Rubicon typically adds details from third-party data aggregators, like BlueKai or eXelate, such as users' sex and age, interests, estimated income range and past purchases. Finally, Rubicon applies its own analytics to estimate the fair market value of site visitors and the ad spaces they are available to see."

(New York Times)

Privacy Policies

- No one reads them
  - Cranor estimated the opportunity cost at US$3500/year to read them all
- They're deliberately vague and expansive
  - "We may collect personal information and other information about you from business partners, contractors and other third parties." (Reidenberg et al)
- "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent." (PCAST report)

Location Data

- Huge issue for mobile devices
  - Many apps collect and analyze such data
- IP geolocation also reveals a lot

Governments

- If data exists, it's available to governments
- Some governments have a complex, restricted, and somewhat painful process required to gain access to data
- Other governments don't care very much about such niceties
- Some governments collect data via espionage, technical and otherwise

It's Not Just PII

- Virtually all privacy laws are based on protecting PII: Personally Identifiable Information
  - N.B.: The definition of PII varies
- But: you don't need PII to invade folks' privacy
  - Amazon doesn't need your identity to recommend products
  - Netflix doesn't need your identity to recommend movies
- PII is actually a database key!

Deidentification

- Many people have tried "deidentifying" data: removing the PII

- Reidentification is often possible, based on other fields

- Good anonymization can destroy the utility of the data, e.g., for some medical research

Machine Learning

- Today's ML algorithms can infer things not directly observed, e.g., sexual orientation

- This is much harder to control: it is *not* based on data collection, which is usually what's regulated

- Even when some inputs are disallowed by law, there are often proxy variables that are strong correlates

Notice and Consent Is Dead

- No one knows who collects data
- No one knows what they'll do with it
- No one knows where it's stored
- And some of the most sensitive stuff, e.g., location, is dual-use: it's used for your benefit (map programs) *and* it's part of your "data shadow"

But what should replace it?

Use Controls

- Abandon collection restriction—it doesn't work (it's better in the EU, but still not great)

- Instead, let consumers specify how their data can be used: targeted advertising, statistical analysis, medical research, etc.

- It's not that easy

Problems With Use Controls

- Definitions
- Usability
- Consent across long time intervals
- Data that exists can be abused, either by hackers, scofflaws—or simply through a change in the law
- In the US, possible legal constraints

A New Privacy Paradigm?

- Must scale to very many data collectors, known and unknown
- Must scale across time
  - One design I've sketched uses the blockchain…
- Must be comprehensible by individuals
- Must account for inferred data
- Must trade off harm and benefits

I have *no* idea what such a paradigm would look like…

The IETF's Role

- Certainly, encrypt as much as possible
- Avoid creating unnecessary third-party metadata
  - One aspect: specify *every* field precisely; leave far less to the implementations
- Design more privacy protocols
- Do a privacy analysis, similar to the security considerations, for new protocols
  - GEOPRIV was a great step in that direction
- Data tagging might help—but it also creates more metadata

References

- Most of the quotes are from "Comments on Privacy" (https://osf.io/preprints/lawarxiv/5s2vt) or things that it cites
  - N.B.: That document was written for a US legal context
- Quoted: Alan Westin, Donald Michael, Arthur Miller

Questions?

Photo by Steven M. Bellovin, August 2012