CS 4873: Computing, Society & Professionalism

Blair MacIntyre | Professor | School of Interactive Computing

Week 8: Privacy and the Government

March 10, 2021

Slides adapted from Sauvik Das, Munmun de Choudhury, and Amy Bruckman

What should the role
of government be
with respect to
privacy?

Governments and Privacy

- Government policy has a significant impact on individual privacy

- Government must balance competing desires:
  - Desire to be left alone and free from surveillance
  - Desire for safety and security

- Different governments balance these desires differently.

One extreme: no oversight

- Tax havens and offshore money laundering
- Wealthy people often store money in tax havens for fraud, tax evasion etc.
  - E.g., Panama Papers leak

The other extreme: surveillance states

- Government keeps track of everything in order to assure that its citizens are behaving up to standards

- 2007 study by Privacy International found eight countries that were rated as being 'endemic surveillance societies'
  - China, Malaysia, Russia, Singapore, UK, Taiwan, Thailand and U.S.A.

Big data meets Big Brother as China moves to rate its citizens

The Chinese government plans to launch its Social Credit System in 2020. The aim?
To judge the trustworthiness – or otherwise – of its 1.3 billion residents

#1. CREDIT HISTORY

Reflects a user's past payment history and indebtedness. This consists of areas such as credit card repayment, utility bill payments and user ratings from e-commerce websites such as Ta obao.

#2. FULFILLMENT CAPACITY

Reflects the user's ability of adhering to contracts such as financial products and loans. It is evaluated based on asset information, including payment for social insurances, properties and cars, etc.

Indicators also include use of Alibaba's financial products, services and AliPay account balances.

#3. IDENTITY CHARACTERISTICS

Rates the extent and accuracy of a user's personal info. For example, home address, length of time of residence, mobile phone number, education level and employment. User can fill in information or import information from LinkedIn or other external systems.

#4. SOCIAL RELATIONSHIP

Reveals the user's influence within their personal network, their influence to the network and their friends' credit scores.
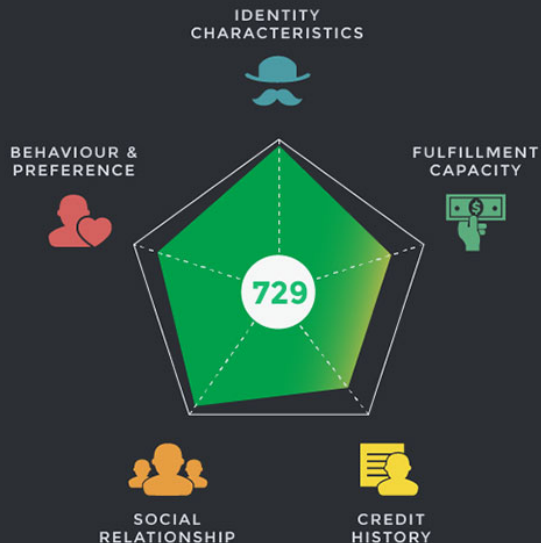
#5. BEHAVIOUR & PREFERENCE

Shows a user's online behavior, including how active they are, what websites they visit, the products they shops at and the consumer segment the user belongs to, etc.

THE DATA IS DISTILLED DOWN INTO A

NUMBER BETWEEN 350 & 950

THIS IS

IDENTITY CHARACTERISTICS

BEHAVIOUR & PREFERENCE

FULFILLMENT CAPACITY

729

SOCIAL RELATIONSHIP

CREDIT HISTORY

THE SESAME SCORE

The precise weightings are shrouded in mystery, however Sesame's Director of Technology shared this with Chinese magazine Caixin in February 2018:[6]

> Someone who plays video games for 10 hours a day, for example, would be considered an **idle person**, and someone who frequently buys diapers would be considered as probably a parent, who on balance is more likely to have a **sense of responsibility**.

Do you think the Sesame Score is a net positive or net negative? Why?

- Think about this.
    - Remember: It's okay to have either opinion.

- It's also okay to think it's bad overall but recognize some positives, or good overall but recognize some negatives

- Pause here and write down what you think
    - You'll want it for the discussion section

Gamified citizens

- High sesame scores equates to:
  - Boosts on dating apps; discounts on bills; better loan terms; skipping queues at the airport
- Low sesame score equates to:
  - Barred from traveling; slow internet; job prospect limitations

- Carrots and sticks:
  - Incentivizes / rewards being a "model" citizen as defined by the government:
    - e.g., paying bills on time; being productive with your time
  - Disincentivizes / punishes associating with "non"-model citizens (interacting with a low-score person could lower your own score)
  - Disincentivizes / punishes voicing dissenting opinions

China is not the only surveillance state

- It's just one of the more "on-the-nose" examples.

A series of questions:

- Do you support (by the government):
  - "expanded camera surveillance on streets and in public places"
  - "law enforcement monitoring of Internet discussions in chat rooms and other forums"
  - "closer monitoring of banking and credit card transactions to trace funding sources"
  - "expanded governmental monitoring of cell phones and emails to intercept communications"

- Pause and think about these

U.S. Government and Privacy

- National security concerns significantly outweighed privacy concerns post 9/11 attacks. 2006 poll showed that:
  - 70% of Americans supported expanded camera surveillance
  - 62% supported law enforcement monitoring of Internet discussions
  - 61% supported closer monitoring of banking and credit card transactions
  - 52% supported expanded governmental monitoring of cell phones and emails

Solove's taxonomy of privacy

- **Information collection**: Activities that gather personal information

- **Information processing:** Activities that store, manipulate, and use personal information that has been collected

- **Information dissemination:** Activities that spread personal information

- **Invasion**: Activities that intrude upon a person's daily life, interrupt someone's solitude, or interfere with decision-making

U.S. Government and Information Collection

- Information collection safeguards:
  - **Employee Polygraph Protection Act**: Prohibits employers from use lie detectors
  - **Children's Online Privacy Protection Act**: Online services must gain parental consent before collecting info on children < 12 years old
  - **Genetic Information Non-discrimination Act**: Employers and health insurance companies can't take genes into account
- Infringements:
  - **Census records** (required to ensure fair representation in Congress, also used to find draft resistors and Japanese Americans in WW2)
  - **IRS records**: require a lot of deeply personal information
  - CCTV cameras (more than 30 million in US)

# U.S. Government Privacy Safeguards & Infringements

- Information processing :
  - IRS uses data mining to look for income tax fraud
  - **Syndromic surveillance system**: Data mining system that searches for patterns indicating outbreak of an epidemic or bioterrorism (911 calls, Internet searches)
  - **Predictive policing**: Law enforcement using data mining to determine areas that are likely to require additional policing

U.S. Government Privacy Safeguards & Infringements

- Information dissemination related policy:
  - **FERPA**: Students allowed to review educational records, request changes to erroneous records and prevent release of records without permission
  - **HIPAA**: Limits how medical institutions can share and use medical info
  - **Freedom of Information Act**: ensure public has access to records for the executive branch of the U.S. gov't

U.S. Government Privacy Safeguards & Infringements

- Invasion safeguards:
  - **National Do Not Call Registry**: prevents telemarketers from calling numbers in the registry
  - **Advanced Imaging Technology Scanners**: Original TSA scanners revealed highly accurate anatomical features. New machines show generic outlines.
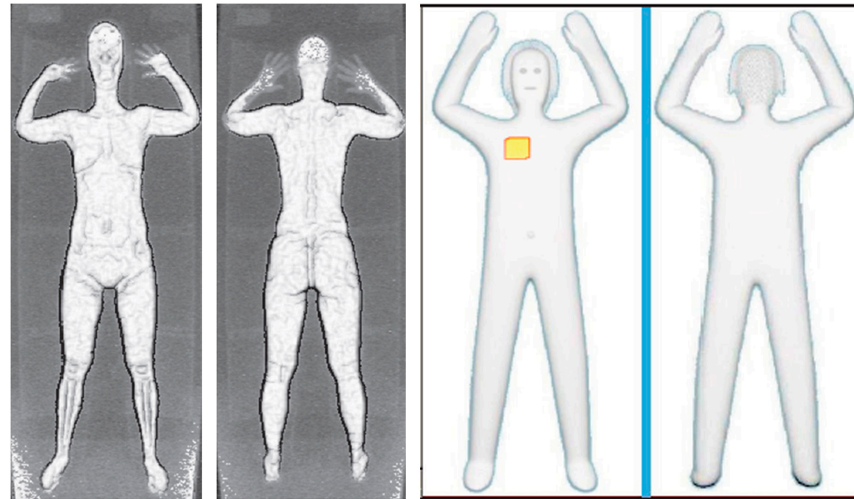
Conflicting privacy policies of different countries

- US/EU airline conflict
  - US requires info on all international passengers arriving in US
  - EU allows access to info on a case-by-case basis, based on suspicion.
    - Airlines handing over this data for EU citizens would be breaking EU law
- Compromise?
  - US reduces the amount of data requested and provides assurances on how data will be used
  - 2014 EU review found that U.S. DHS not in compliance – reviews records without probable cause

EU-US Privacy Shield

- In 2000, the U.S/EU agreed on a "safe harbor" policy
  - Companies outside EU that agree to EU's privacy practices may receive data on EU citizens
  - Ruled to be insufficient by EU court
- 2016 – "Privacy Shield"
  - Requires certification (safe harbor was self-certification)
  - Requires review (external audit or self review)
  - If EU controller transfers data to a US Privacy Shield org, both parties must enter a written contract

GDPR vs Privacy Shield?

- In 2018, the EU enacted "General Data Protection Regulation" (GDPR)

- The GDPR has specific requirements regarding the transfer of data out of the EU. One of these requirements is that the transfer must only happen to countries deemed as having adequate data protection laws. The EU does not list the US as one of the countries that meets this requirement.

- Privacy Shield allows US companies, or EU companies working with US companies, to meet this requirement of the GDPR.

Facebook Threatens EU Pullout

By **PYMNTS**

Posted on September 21, 2020

| SHARE | TWEET | SHARE | SHARE | PRINT | EMAIL |

In a bit of high-tech saber-rattling, **Facebook** is threatening to pull the plug on its social media platform in the European Union if a controversial decision by Irish regulators is allowed to stand.

Yvonne Cunnane, Facebook Ireland's head of data protection and associate general counsel, has informed Ireland's Data Protection Commission of dire consequences should the regulator uphold a ruling that restricts the transfer of data between Europe and the U.S., according to Metro.

Facebook's Cunnane laid out the threat in a sworn affidavit to the Irish regulator, hinting that the social media giant might be prepared to shut down its operations in a region where it has more than 400 million users.

SSNs

- Started off just as a way to track social security contributions
  - Usage spread to other parts of gov't
  - Now often used as both identifiers and passwords
- But: bad identifiers because not unique
  - In early days, some people accidentally assigned same SSN because numbers were assigned by local governments
- SSN's aren't secure
  - Not random: First three digits is where you were born, next two indicates age, last four are random
  - Don't have a checksum or other error correction, so easy to guess fraudulent SSNs

REAL ID Act

- Federal standards for diver's licenses
  - More documents needed to get your license
  - Must be machine readable
  - Will probably include a biometric
- Will be needed to fly on a plane, open a bank account, or use government services
- Passed in 2005. Some states slower to approve than others – TSA pushed back implementation deadline to 2020

National ID cards

- Pros:
  - Currently, we have no great mechanism for identifying residents
  - Would make it difficult for people to enter country illegally and for those people to find work
  - Could reduce crime
  - Many democratic countries use them (e.g., France, Spain, Germany)
- Cons
  - Can be forged, impossible to make a 100% accurate biometric
  - No evidence that it reduces crime
  - Makes it easier for the government to data mine citizens

Closing Thoughts

- What special responsibilities do computer professionals have with respect to understanding and protecting the privacy rights of their fellow citizens?

ars TECHNICA   BIZ & IT   TECH   SCIENCE   POLICY   CARS   GAMING & CULTURE   STORE

GAB HACK —

Gab, a haven for pro-Trump conspiracy theories, has been hacked again

Failure to purge authentication tokens taken in first breach leads to second one.

DAN GOODIN - 3/8/2021, 11:53 PM

Beleaguered social networking site Gab was breached on Monday, marking the second time in as many weeks that hackers have gained unauthorized access to a platform that caters to users...

Enlarge

ars TECHNICA   BIZ & IT   TECH   SCIENCE   POLICY   CARS   GAMING & CULTURE   STORE

THAT'S SETTLED —

Equifax to pay $575M for data breach, promises to protect data next time

The company promises free credit monitoring and not to screw up with security.

KATE COX - 7/22/2019, 12:43 PM