Technology and Privacy

Comp 1400
March 2016

- Research interests
  - Law and Technology
  - Privacy technology and its regulation
- Because:
  - Technology determines culture and society
- Other interests
  - Visualization
  - Mobile/social platforms
  - Human cognition

Sources

- Lawrence Lessig, “Code: And Other Laws of Cyberspace” Version 2.0, ISBN-13: 978-0465039142, c. 2006, http://codev2.cc/
- See also CBC news reports related to C-13 and C-51 (The first link is related to the Brussels bombing this week):
  - http://news.nationalpost.com/news/canada/canadian-politics/trudeau-condemns-deplorable-brussels-attacks-security-increased
  - http://www.cbc.ca/news/politics/cyberbullying-bill-draws-fire-from-diverse-mix-of-critics-1.2803637
  - http://www.cbc.ca/news/politics/c-51-controversial-anti-terrorism-bill-is-now-law-so-what-changes-1.3108608
- C-13: Statutes of Canada 41 Parl. 62-63 Elizabeth II, 2013-2014 http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6830553
- S-4: Statutes of Canada 41 parl 2nd,62-63-64 Elizabeth II, 2013-2014-2015 http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=8057593
- C-51: Statutes of Canada, Statutes of Canada 41 parl 2nd,62-63-64 Elizabeth II, 2013-2014-2015, https://openparliament.ca/bills/41-2/C-51/
- Provincial Health Information Act, as revised 2015, Statutes of Newfoundland and Labrador, P-7.01, see http://www.health.gov.nl.ca/health/phia/

Politics of the Internet

- Fundamental design of packet-switching:
  - Shared responsibility for delivery
  - free access
  - End-to-end packet delivery
- First Age: free information sharing, low entry cost, rapid growth of infrastructure
- Second Age: business development (ISPs, commercial websites, social networking)
- Third Age: regulation and surveillance

Technology shapes culture

- Design of internet is not inevitable
  - Packets are not secure
  - Nodes should behave according to a protocol
  - Source is not inherently identifiable
- But people act and think like it is
- Lawrence Lessig: Code is law
  - Self-enforcing: code is more powerful than law
  - Creates expectations
  - Legislators and law makers respond to environment

Example of technology shaping policy

- Assymetric cryptography
- Provides for end-to-end security, but could be deployed in different ways
- Also known as “public key” cryptography
- Shaped how the internet has developed technically and economically

Assymetric Cryptography

- Problem: how do we keep information secure (meaning secret)?
- Cryptographic Key: encrypt the message using a key, the receiver decrypts with a key. Message cannot be read by internet hops “in between”
- But how do we keep the key a secret?
- Asymmetric cryptography allows for two keys: one for encryption, one for decryption.
- The encryption key is public, so anyone can encode a message with my public key, but only I can decrypt the message.
- I can publish my “public” encryption key freely

Second “business age” of Internet

- Public key encryption built into communication systems (SSL, Browsers)
- Need a means of authentication
- Asymmetric cryptography can be used for digital signatures:
  - Only I can encrypt message, but you can verify the message was encrypted by my private key.
- The problem is authenticating the key: how do you know that is my key you are using?
- General answer: third party trust mechanisms
- Note that this is clearly an add-on to the internet infrastructure
- Internet only built for end-to-end transmission:
  - Certificates, cookies, added to support authentication and verification of messages (and to maintain state)

Third age of internet

- Governments want to control activity on internet
- Maintain control of domestic population: “law enforcement” ~ POGG
- Domestic surveillance
- Themed as “lawful access”

Recent Legislative efforts

- Federal Cyberbullying Law (Bill C-13)
  - Increased powers for investigation without oversight (ISPs hand over message header information upon investigative warrant)
  - ISPs have to maintain message information
  - Increased protection for voluntary disclosure by ISPs to a request by an investigating authority.
  - Not restricted to cyberbullying – applies to investigations generally
- Digital Privacy Act (Bill S-4)
  - Includes private investigations
  - s. 7(3)(d.1):

    an organization may disclose personal information without the knowledge or consent of the individual… if the disclosure is made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;
- Anti-Terrorism Act (Bill C-51)
  - Allows government agencies (CSIS, CSEC, RCMP, RCA, etc) to share information regarding unspecified “activities that undermine the security of Canada”
    - Encompasses activities that includes ““changing or unduly influencing a government I Canada”, “by force or by unlawful means.”
    - Excludes “lawful advocacy, protest, dissent or artistic expression” (protests and stikes are not excluded)
    - No specific oversight or external enforcement provisions
- *Total surveillance state?*

Cultural Constructs

- Cultural constructs being created around specific technological capabilities
  - Security can be improved by collecting and processing data; possibly in a manner that creates a surveillance state
  - The intrusion into peoples lives is worth the risk
  - Focus is on possible over-reach and abuses by government actors
  - Missing the point that the technology itself may be suspect (creation of an infrastructure that allows the data to be captured)

Another Example: Health Informatics

- Since mid-90's, efforts to create a pan-Canadian health record
- Promoted as a means of improving primary care delivery
- Empirical evidence shows there is little improvement in health outcomes for point-of-care
- Large benefits to be had in Health Surveillance, requires sharing of data (“secondary use”)
- But how to share data in a complex health care system while respecting patient privacy?

Health Informatics: Legislative constructs

- Provinces and territories parliaments pass Health Information Acts
- Created concepts of “Information Custodian” that can share information within a “Circle of Care”
- Care providers can share patient information based on designated caregiver “roles”
- Patients do not have direct access to their own information

Health Informatics: Technological Constructs

- Large centralized data repositories for health records
- Technical mechanisms for controlling access (Role Based Access Control)
- Security and authentication protocols established
- NOT based on public/private key mechanism
- As system is evolving, data is held and managed by central authority (quasi governmental or crown corporation)
- Could be established differently:
  - Held or controlled privately by patients
- Reflected in signed privacy releases/permission

Conclusion

- Interest in how technology shapes culture, specifically as reflected in legislative and legal constructs
- Technology can be highly politicized and used as a tool to influence and direct social change
- Can be used to impose change without oversight or participation
- Long term impact for technical infrastructure built/decided now