Technology and Privacy
Comp 1400

E. Brown
brown@mun.ca
Nov 2018

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

Sources

- Lawrence Lessig, "Code: And Other Laws of Cyberspace" Version 2.0, ISBN-13: 978-0465039142, c. 2006, http://codev2.cc/
- Brief on Bill C-59, ICLM group submission to the parliamentary hearings on Bill C-59, online: http://iclmg.ca/wp-content/uploads/sites/37/2018/01/ICLMG-Brief-on-Bill-C-59.pdf (accessed Aug 22, 2018)
- 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
- Bill C-59 under second reading, as of Aug 22, 2018: http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading
- Overview of privacy legislation in Canada, Office of the Privacy Commissioner of Canada, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/ (accessed August 2018)
- 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/
- Executive Order: Enhancing Public Safety in the Interior of the United States, Office of the Press Secretary, White House, Jan 25, 2017, see https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united
- Quebec acts to protect press freedom after police tracking of journalists, Globe and Mail, Nov 1, 2016, http://www.theglobeandmail.com/news/national/tracking-of-journalist-patrick-lagace-highlights-need-for-clearer-laws-daniel-therrien/article32616985/
- Canadian charter of Rights and Freedoms https://laws-lois.justice.gc.ca/eng/Const/page-15.html

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
  - Not verifiable = opaque
  - Legislators and law makers respond to environment
    - (in the absence of social policy)

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
  - economically
  - regulatory

Asymmetric 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 and Foreign surveillance
- Themed as “lawful access”

Recent Legislation – Privacy and State surveillance

- Canada: Federal Bill C-59 (first reading completed as of Nov 15, 2018) re-vamps legislation for Canada’s intelligence services:
  - Creates a review agency and an Intelligence Commissioner for oversight, which responds to disclosed activities and reports: they do not investigate
  - Does not clean-up lawful access provisions
  - No specific acknowledgement of “Five Eyes” data sharing agreement among spy agencies
  - CSE powers: Provides for Canadian Security Establishment (CSE)
    - to engage in cyber-defense and “active cyber operations” against foreign targets
      - “installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting or intercepting anything on or through the global information infrastructure” and “carrying out any other activity that is reasonable 20 in the circumstances and reasonably necessary in aid of any other activity, or class of activities, authorized by the authorization.”
    - “foreign facing” not directly targeting Canadians
    - including any publicly available information (including Canadian information)
    - Authorization by ministerial approval is required when actions are a contravention of a law of Canada
  - CSIS provisions:
    - Closed list of actions CSIS can take, some of which would otherwise be Charter violations
    - Warrant by “secret” Federal court required when violation of individual rights is involved
    - Some reduction of “disruption” powers targeted at communications CSIS has had for 15 years
    - New powers to collect specific types of datasets

Surveillance of Patrick Lagace

- Oct 2016, La Press journalist Patrick Lagace reports his iPhone has been monitored by Montreal police
- Police internal investigation to find sources of a leak
- Search warrents did not cover the call logs of police officers..
- Outcome: Ministerial directive to improve process for obtaining warrants

Canadian data in the U.S.

- US Presidental Executive Order, Jan 23, 2017:

  Section 14 of the Executive Order states:

  - *Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.*

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)

“Cambridge Analytica”

- Aleksandr Kogan, a data scientist at Cambridge University, developed an app called "This Is Your Digital Life" (sometimes stylised as "thisisyourdigitallife"). He provided the app to Cambridge Analytica. Cambridge Analytica in turn arranged an informed consent process for research in which several hundred thousand Facebook users would agree to complete a survey only for academic use. However, Facebook's design allowed this app not only to collect the personal information of people who agreed to take the survey, but also the personal information of all the people in those users' Facebook social network. In this way Cambridge Analytica acquired data from millions of Facebook users. (Wikipedia, https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal#Process)

- Cambridge Analytica marketed their ability for targeted marketing using psychographic profiling of individuals based on their data collection and analysis. Notably the Trump presidential campaign was one of their clients.
  - Christian Wylie was credited as being a principle whistleblower at C.A. surrounding their general business practices, not just regarding Facebook. Here he answers a question about doing intelligence work for the Russians, from Senator Feinstein before the Judiciary Committee https://youtu.be/PCpDi57x4uc?t=2852
- In March 2018, multiple media outlets reported on C.A.’s business practices; an expose by Channel 4 News was particularly damaging to CEO Alexander Nix at https://youtu.be/mpbeOCKZFfQ?t=778
- The New York times and The Observer investiagtions led to revealations that Facebook knew about massive data theft from 2015 and did nothing to inform their users.

- Facebook’s immediate response: An apology tour and policy changes
  - In a statement posted on his Facebook wall, Zuckerberg avoided the word “sorry” but did express partial blame for Facebook’s role in not doing enough to protect user privacy.
  - He laid out three steps Facebook will take now, including investigating all apps that were able to access user data before 2014, when the company began changing its permissions for developers. Facebook will put restrictions on the data apps can access, limiting them to a person’s name, photo and email. Finally, Zuckerberg said Facebook will make an easy tool that lets everyone see which apps have access to their data and allow them to revoke access.
  - "I've been working to understand exactly what happened and how to make sure this doesn't happen again," he wrote. “The good news is that the most important actions to prevent this from happening again today we have already taken years ago. But we also made mistakes, there's more to do, and we need to step up and do it."
- After two rounds of congressional hearings, Zukerberg’s responses are more refined.
  - The second time before joint session of the Commerce and Judiciary committee for two days of questions
    - Wall street journal exerpts from his testimony:
    - https://www.wsj.com/video/mark-zuckerberg-testimony-before-congress-the-highlights/521515F3-2DFC-4243-88C1-E4F22B766211.html

The wrong questions..

“Here’s what’s going to happen — there are going to be a whole bunch of bills introduced to regulate Facebook... It’s up to you whether they pass or not. You can go back home [and] spend $10 million on lobbyists and fight us, or you can go back home and help us solve this problem.”

- Sen. John Kennedy, R-La. to Mark Zuckerberg

Conclusion

- Technology shapes culture, and specifically is reflected in new legal and cultural constructs
  - Companies like facebook are creating many of these constructs (friends, data sharing, privacy controls) and legislators are simply responding to their actions, (so who is in control?)
- Technology (data collection) can be highly politicized and used as a tool to influence and direct social change
  - determined by the interest of private companies
- Change occurs without oversight or participation
  - Long term impact for technical infrastructure built/decided now
  - Government and regulatory institutions responding after the social impact is already felt – in a policy vacuum