CS 280

Risk and Reward in the Information Society

Privacy

Privacy Topics:

- Ethical and legal basis for privacy protection
- Ethical and legal framework for freedom of information
- Privacy implications of online systems
- Technological strategies for privacy protection
- Freedom of expression in cyberspace
- International and intercultural implications

Right to Privacy

- Generally understood to mean:
  - Freedom from **intrusion**.
  - **Control of information** about oneself.
  - Freedom from **surveillance**.
- Negative or positive right?
  - Negative: **theoretically** imposes no burdens on other people
  - **Protecting privacy**, as it turns out, does impose some burdens

Quotes

- "there's no place for the state in the bedrooms of the nation" ... "what's done in private between adults doesn't concern the Criminal Code"
  - Pierre Trudeau, 1967
- "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."
  - Eric Schmidt, CEO Google, 2009

Privacy and tradeoffs

- Privacy versus security
- Privacy versus efficiency
- Privacy versus technical innovation
- Privacy versus free speech

- Privacy also conflicts with privacy
  - e.g. Right to be forgotten leads to news articles about those advocating for their right to be forgotten
  - Barbara Striesand Effect
  - can’t get rid of info

Privacy viewpoints

- (a) Governments and Corporations shouldn't know everything about us
  - Unreasonable suspicion of wrongdoing
  - Denied for an insurance claim
  - Legal but offensive / amoral behaviour
- (b) What are you trying to hide?
  - Governments and corporations need information about citizens and customers to plan, make decisions
  - surveillance protects public safety

Right to Privacy: Canadian Charter (Privacy *from* Government institutions)

- Section 8:
  - “Everyone has the right to be secure against unreasonable search or seizure.”
  - Equivalent to the US 4th amendment
- Reasonable expectation of privacy
  - Hunter v. Southam: section 8 of the Charter guarantees a "broad and general right" to privacy.
  - individuals are only entitled to a "***reasonable expectation***" of privacy.

What is a reasonable expectation of privacy?

- May Include:

  (i) presence at the time of the search;

  (ii) possession or control of the property or place searched;

  (iii) ownership of the property or place;

  (iv) historical use of the property or item;

  (v) the ability to regulate access;

  (vi) the existence of a subjective expectation of privacy; and

  (vii) the objective reasonableness of the expectation.

  - *R. v. Edwards [1996] 1 S.C.R. 128 at para. 2*

Reasonable Expectation of Privacy and Slippery Slopes

- Reasonable expectation is a contextual thing
  - "most well-informed people know that…"
- Expectation of online privacy is eroding
  - "email = postcard", "browsing history is public"
  - ISPs keep records. Banking? Purchasing?
  - if these are not subject to a reasonable expectation of privacy online,what's the difference with off-line versions?
    - -> Govt access to banking records?

Privacy (from Canadian law decisions)

- “privacy is grounded in physical and moral autonomy – the freedom to engage in one’s own thoughts, actions, decisions”
  - R. v. Dagg,[1997] 2 S.C.R. 403 at para. 65
- Privacy includes
  - Bodily
  - Territorial
  - Informational

Informational Privacy

- "In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the ***reasonable expectations*** of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected."
  - R. v. Dyment,[1988] 2 S.C.R. 417 at 431-2

Privacy violations or not?

- Phone tap?
- Video / photo surveillance?
  - on a public street?
- Infra-red scanning of a house?
- Sniffer dogs at airports and bus stations?

- Tend to be decided by specific legislation

Reasonable expectation is less likely:

- information in the hands of third parties with no obligation to maintain confidentiality:
  - *R v Hutchings* - phone number
  - *R v Ryan* - counseling records
  - *R v Dersch* - blood samples
  - *R v Weir* - email
- where police techniques are unintrusive:
  - *R v Tessling* - FLIR = forward-looking infra-red
  - *R v Wong* - video surveillance
  - *R v Duarte* - audio surveillance

Electronic devices have reasonable expectation

- http://criminalnotebook.ca/index.php/Established_Areas_of_Privacy#cite_ref-88
  - *R v Marakah 2017* - electronic devices are considered with similar privacy as territorial
    - Computers are highly personal
    - when taken to a repair shop, expectation of privacy is reduced
- Also *R v Cole 2012* - employee's personal information, even when stored on computer, has reasonable expectation of privacy.

Government use of private data

- Assertion: Canadians trust government a bit more than business; US trust business a bit more than government
  - discuss?

- Privacy act (1974)
- Computer Matching and Privacy Protection act (1988)
- Canadian Privacy act (1983)
  - How the government treats personal information
  - these acts are old, and some want it updated

Privacy Act (Canada): Collection

- Government institutions can collect info:
  - Relevant information only
  - Directly from person (when possible)
  - Person is informed of purpose
  - Retained so person can verify
  - Not used for another purpose without consent
  - Not disclosed without consent
    - except in some legal situations

Privacy Act (Canada): Data Banks

- Govt institutions will hold info in a bank indexed by a person's name or ID
- Index of data banks and their use published at least once a year
- Citizens & residents have right to access information about them held in a bank
  - and correct if inaccurate

- Which institutions have your information?

Dpt Agriculture and Agri-Food; Dpt CDN Heritage; Dpt Citizenship and Immigration; Dpt the Environment; Dpt Finance; Dpt Fisheries and Oceans; Dpt Foreign Affairs and InterNTL Trade; Dpt Health; Dpt Human Resources and Skills Development; Dpt Indian Affairs and Northern Development; Dpt Industry; Dpt Justice; Dpt NTL Defence (including the CDN Forces); Dpt Natural Resources; Dpt Public Safety and Emergency Preparedness; Dpt Public Works and Government Services; Dpt Transport; Dpt Veterans Affairs; Dpt Western Economic Diversification; Assisted Human Reproduction Agency of CA; Bank of CA; Business Development Bank of CA; CA Border Services Agency; CA Council for the Arts; CA Deposit Insurance Corporation; CA Development Investment Corporation; CA Emission Reduction Incentives Agency; CA Employment Insurance Commission; CA Industrial Relations Board; CA Lands Company Limited; CA Mortgage and Housing Corporation; CA Post Corporation; CA Revenue Agency; CA School of Public Service; CDN Advisory Council on the Status of Women; CDN Air Transport Security Authority; CDN Artists and Producers Professional Relations Tribunal; CDN Centre for Occupational Health and Safety; CDN Commercial Corporation; CDN Cultural Property Export Review Board; CDN Dairy Commission; CDN Environmental Assessment Agency; CDN Food Inspection Agency; CDN Forces Grievance Board; CDN Government Specifications Board; CDN Grain Commission; CDN Human Rights Commission; CDN Human Rights Tribunal; CDN Institutes of Health Research; CDN InterNTL Development Agency; CDN InterNTL Trade Tribunal; CDN Museum of Civilization; CDN Museum of Nature; CDN Nuclear Safety Commission; CDN Polar Commission; CDN Race Relations Foundation; CDN Radio-television and Telecommunications Commission; CDN Security Intelligence Service; CDN Space Agency; CDN Tourism Commission; CDN Transportation Accident Investigation and Safety Board; CDN Transportation Agency; CDN Wheat Board; Copyright Board; Correctional Service of CA; Farm Credit CA; Financement agricole CA; Federal-Provincial Relations Office; Financial Consumer Agency of CA; Financial Transactions and Reports Analysis Centre of CA; Grain Transportation Agency Administrator; Great Lakes Pilotage Authority; Hazardous Materials Information Review Commission; Historic Sites and Monuments Board of CA; Immigration and Refugee Board; Intl Centre for Human Rights and Democratic Development; Intl Development Research Centre; Law Commission of CA; Library and Archives of CA; Merchant Seamen Compensation Board; Military Police Complaints Commission; NTL Arts Centre Corporation; The NTL Battlefields Commission; NTL Capital Commission; NTL Energy Board; NTL Farm Products Council; NTL Film Board; NTL Gallery of CA; NTL Museum of Science and Technology; NTL Parole Board; NTL Research Council of CA; NTL Round Table on the Environment and the Economy; Natural Sciences and Engineering Research Council; Ofc. Indian Residential Schools Resolution of CA; Ofc. Infrastructure of CA; Ofc. Privatization and Regulatory Affairs; Ofc. the

Some Government agencies who might have your info

- Citizenship and Immigration
- Department of National Defence (including the Canadian Forces)
- Canada Employment Insurance Commission
- Canada Mortgage and Housing Corporation
- Canada Post Corporation
- Canada Revenue Agency
- Canadian Security Intelligence Service (CSIS)
- Correctional Service of Canada
- Immigration and Refugee Board
- Library and Archives of Canada
- Natural Sciences and Engineering Research Council
- Ofc. Chief Electoral Officer
- Parks Canada Agency
- Public Health Agency
- Royal Canadian Mounted Police (RCMP)
- Statistics Canada

Privacy Act and Access to Information Act

- Privacy Act (1983)
  - Grants right to access *your* personal information held by the government
  - protection of that information against unauthorized use and disclosure.
- Access to Information Act (1983)
  - right to access *other* information in federal government records.
  - subject to exemptions and exclusions

Access to Information Act

- Exemptions (most of the actual act)
  - international and defence
  - policing and security
  - information which could threaten safety
  - trade secrets held by the govt
  - Personal information (as in Privacy Act)
- Exclusions (not applicable)
  - Public, museum and library material
  - Queen’s privy council communication

Bill C-51: Anti-terrorism act 2015

- Allows sharing of information between agencies in certain circumstances:

- Canadian Border Services Agency
- Canada Revenue Agency
- Canadian Armed Forces
- Canadian Food Inspection Agency
- Canadian Nuclear Safety Commission
- CSIS
- CSE
- Citizen and Immigration
- Finance
- Foreign Affairs, Trade, and Development
- Health
- National Defence
- Public Safety
- Transport
- FINTRAC
- Public Health Agency
- RCMP

Bill C-51

- Changes the way privacy is perceived by government agencies
- Broadly worded, allowing agencies to share information for a wide range of purposes
  - Information that “undermines the security of Canada” whatever that might mean
  - Not the CSIS definition of national security
  - Also could include “public safety” (i.e. internal security) and “financial stability”

Government information concerns

- Do governments follow their own rules?
- What use are good Canadian laws if US laws are different?
- What does the government do that we don’t know about?

USA PATRIOT ACT

- Passed just after 9/11
- "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001”
  - US loves them some acronyms
- Allows FBI to search telephone, email and bank records without a warrant
- Few Checks and balances
- Data stored on US soil can be searched at any time for any reason

Consequences of patriot act

- Many government contracts require data to be stored on Canadian soil
- Amazon and IBM now have two Canadian data centres for precisely this reason
  - Amazon's second data centre (Montreal) is quite recent
  - Before that you'd need to have access to European redundancy

Protecting Privacy and the Patriot Act

- Patriot act also has a provision for secret subpoenas
  - US govt can issue a warrant for your data, a***nd forbid the company from informing you of the warrant***
- Some companies have started to use a “warranty canary.” for example:
  - “Apple has never received an order under Section 215 of the USA Patriot Act.”
  - Notably, they removed this in 2013. Reddit removed theirs in 2016

- Does anyone put tape over their webcam?

Corporate privacy: PIPEDA

- Recall Privacy act; Access to Information act
  - Government collection and use of information
- PIPEDA
  - *Personal Information Protection and Electronic Documents Act*
  - Business collection and use of information
  - Applied to all commercial entities as of 2004

- PIPEDIA is to businesses as the privacy act is to govt

PIPEDA

- Under PIPEDA, personal information must be:
  - collected with consent and for a reasonable purpose
  - used and disclosed for the limited purpose for which it was collected
  - accurate
  - accessible for inspection and correction
  - stored securely
- Similar to requirements of government in Privacy Act

PIPEDA 10 principles

1. Accountability
2. Identifying purposes for information collection
3. Consent of the individual is required
4. Limiting Collection of personal information
5. Limiting Use, Disclosure, and Retention
   - except where required by law
6. Accuracy
7. Security Safeguards
8. Openness regarding policies and practices
9. Individual Access
10. Challenging Compliance

PIPEDA changing business practices

- Most websites and organizations now overtly post their "privacy policy"
  - Usually prefaced: *"We at ___ know that you are concerned about privacy and we are dedicated to ensuring your information is kept private"*
- Protects consumers?
  - Can't sell or use for other purposes
  - Most customers don't know pipeda's rules
  - Most customers don't read the privacy policy

Company mail

- All records kept
  - Can search through later, apply new technologies, look for suspicious behaviour after the fact
- PIPEDA protects consumers
  - Not employees. Read your company's policy!

Work E-Mail Not Protected by Attorney-Client Privilege

- January, 2011
- a woman sending email to her lawyer from her work email is like
  - "consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard."
- Previously, emails with disclaimers are considered private by the court.

Privacy, Data Sharing, and EULA

- *"…you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services."*
  - (https://www.makeuseof.com/tag/10-ridiculous-eula-clauses-agreed/)
- Not as bad as you might think: all EULAs for internet services have a clause like this. It's lawyer-speak for "we'll move your data around on the internet"
  - (mostly. Probably)

Personal information = $$

- Gathering personal information is easy, as long as you, the customer, give consent
  - Contest entry forms
  - Warranty cards (not required for warranty validity)
  - “can I have your postal code for demographics?”
  - Loyalty programs
  - More?

Data Mining

- Credit cards check each transaction against “purchase history”
  - If you suddenly buy 10 big-screen TVs, maybe a stolen card
- Joint account issues
  - Man buys expensive gift for wife. joint card
  - Credit company calls wife to verify.
- Security issues

Data Mining: Beer and Diapers

- Grocery store discovers that beer and diapers are commonly purchased together on Friday afternoons by 25-34yr males
- Places beer next to diapers
  - sells more of both
  - marketing decision -> behavior prediction, hence privacy
- True? probably not. but popular example

Data Mining: Pregnancy

- http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0
- Target keeps track of what people buy to help predict what they will buy
- Target started to include ads for baby stuff in the fliers for a teenager
- Data mining knew she was pregnant before she did
  - 25 products that, when bought in certain ratios, were a good indicator of pregnancy

Target's dilemma

- "Using data to predict a woman's pregnancy, Target realized soon after Pole perfected his model, could be a public-relations disaster. So the question became: how could they get their advertisements into expectant mothers' hands without making it appear they were spying on them? How do you take advantage of someone's habits without letting them know you're studying their lives?"

Data Mining: ads

- Mine keywords from your search
- Choose advertising relevant to the results of your search
  - Invasion of privacy?
  - targeted ads better than banners for v!agra?
  - How do canadian laws protect us when surfing US sites?

Ad tracking

- If google/facebook was only mining data from our searches to present ads, that would be one thing
- Ad tracker networks collect data on your internet traffic
  - 75% of websites are tracked by ads
  - Many websites tracked by multiple (dozens?) of trackers
  - Even with ad blockers, your demographics can be used to construct a profile
    - location, time of day, site visited etc

Ad tracking and AI

- More on AI later, but:
  - AI makes use of aggregate data to make a decision
  - AI quality is entirely dependent on data quality

- Deciding which ad to serve to you at what time, to have the highest likelihood of convincing you to click, is a multi-million dollar industry

- https://www.youtube.com/watch?v=KW0eUrUiyxo
- (sorry, CGP grey again)

Behavior tracking and mobile games

- https://www.raywenderlich.com/39647/40-secrets-to-making-money-with-in-app-purchases
  - Great dev resource, lists common behavioural tactics for in-app purchases. This is not invasion of privacy
- https://trea.com/information/system-and-method-for-driving-microtransactions-in-multiplayer-video-games/patentgrant/bbb03316-05ac-43ee-be5b-cbb8ce0a6c97
- System and method for driving microtransactions in multiplayer video games
  - This is a privacy problem
    - Match a novice player to an expert
    - Offer in-app purchase just as the game gets hard
      - “save me” type IAPs.

Tracking, stakeholders, and metrics

- We might imagine mobile games are designed to be enjoyable
- We might imagine youtube serves us videos it thinks we will like.

- We are not the customer, we are the product

- Enagement and interaction time is the general metric; clickthroughs and micro transactions are the specific metric

Advertising and privacy

- If someone looked over your shoulder at your browser, and saw your ads, how much could they infer about your browsing patterns?

- Ads are served entirely based on your online data

Invisible Information Gathering: Reasonable expectation of privacy?

- Email interception (boss? govt? corp?)
- Loyalty cards
- Web tracking and Cookies
- ISP Logs
- Music players sending track info
- Spyware
- Digital cameras, cell phones,
- More?

Lost in the noise?

- Isn’t there too much data to worry about finding little ol’ me?
- Digital communication is packeted
  - Each packet is tagged for re-assembly
  - traceable to a sender and a recipient
  - All internet communication is (theoretically) traceable
  - Indexes, google-style searching can put it together
- reasonable expectation of privacy?
  - Email, Voip, cell phones, IM, FB, twitter

App Privacy

- Apps gaining access to private information is a common malware approach
  - Apps now have to ask permission for each data access point
  - Many people still just say yes
    - Why does my flashlight need my list of email contacts?

Apps, Malware, and App Store Policy

- Android's early "open" approach meant apps could do what they want
  - frequently, they did
  - Android criticized apple's closed approach, and then implemented it
    - Side loading is still possible, and a common source of malware
  - Apps are sandboxed and by default have few permissions, but apps can (and do) ask for permissions
- 99% of malware is on andorid. More later

Privacy and Services

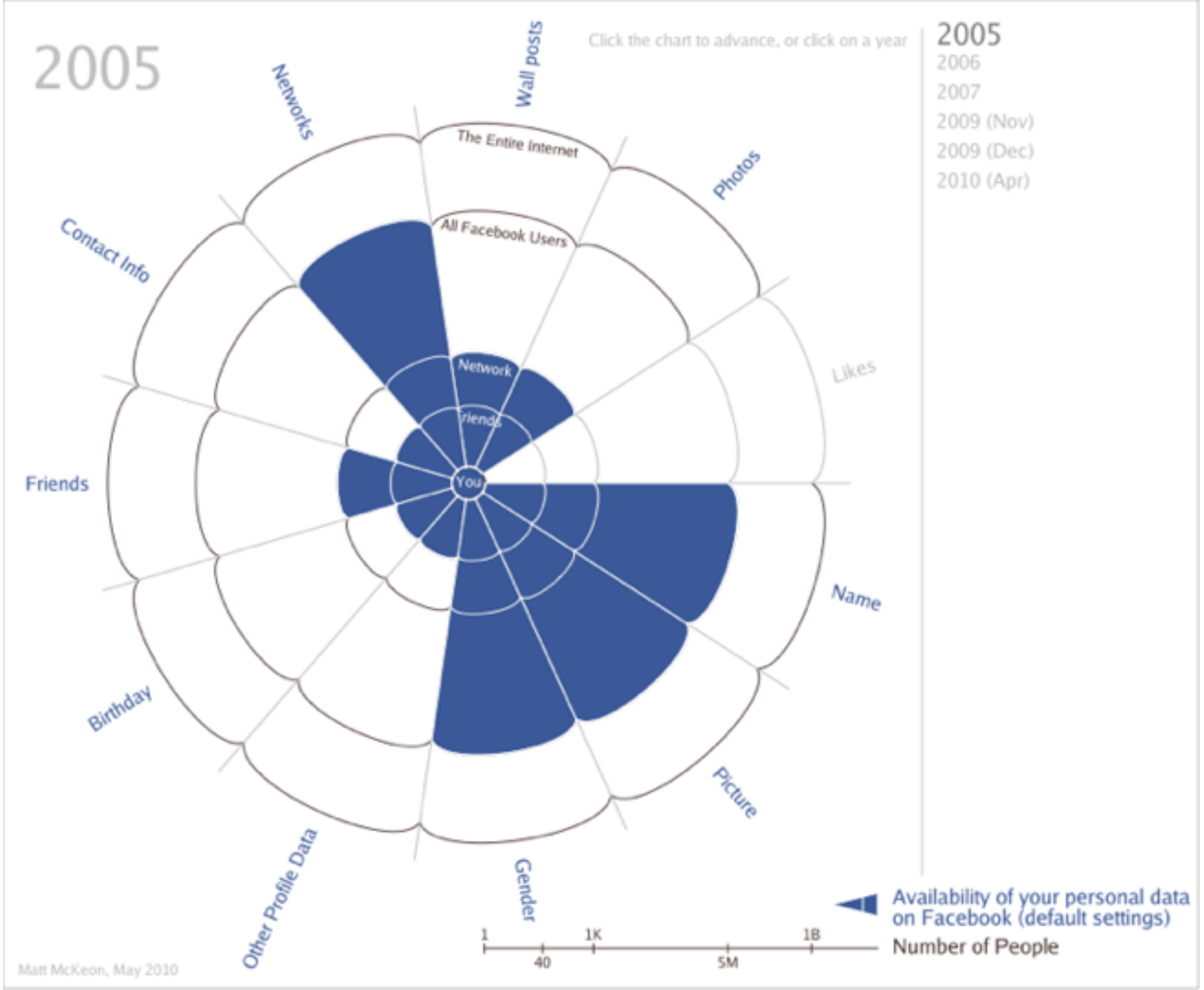
- Location services, build their maps by tracking the location of their users
  - Salted, Differential, but still tracked
  - Traffic services work this way
- skyhook: build a database of WIFI signals (including yours)
  - Base station IDs used as a mapping system
- Find friends / find phone. Geotagging. These are useful but what if they are hacked?

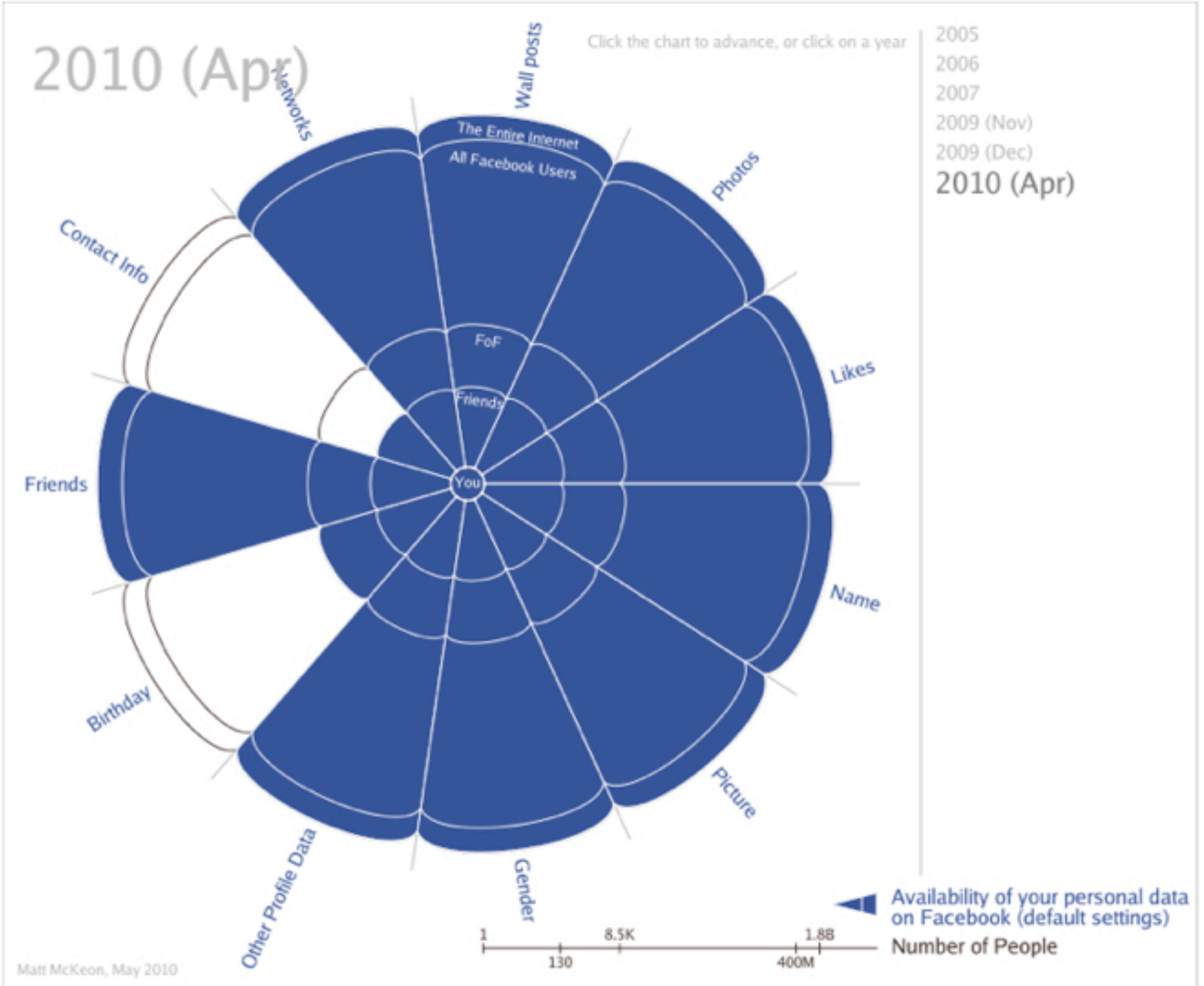

PEOPLE IN THE SIXTIES:
I BETTER NOT SAY THAT OR
THE GOVERNMENT WILL WIRETAP MY HOUSE
WWW.MURICATODAY.COM
PEOPLE TODAY:
HEY WIRETAP,
DO YOU HAVE A RECIPE FOR PANCAKES?

Social Media and Privacy

- Sharing personal information has progressed to sharing information in public
  - Facebook: share with friends (default private)
  - Linkedin: share with business folks
  - Twitter: share with everyone (default public)

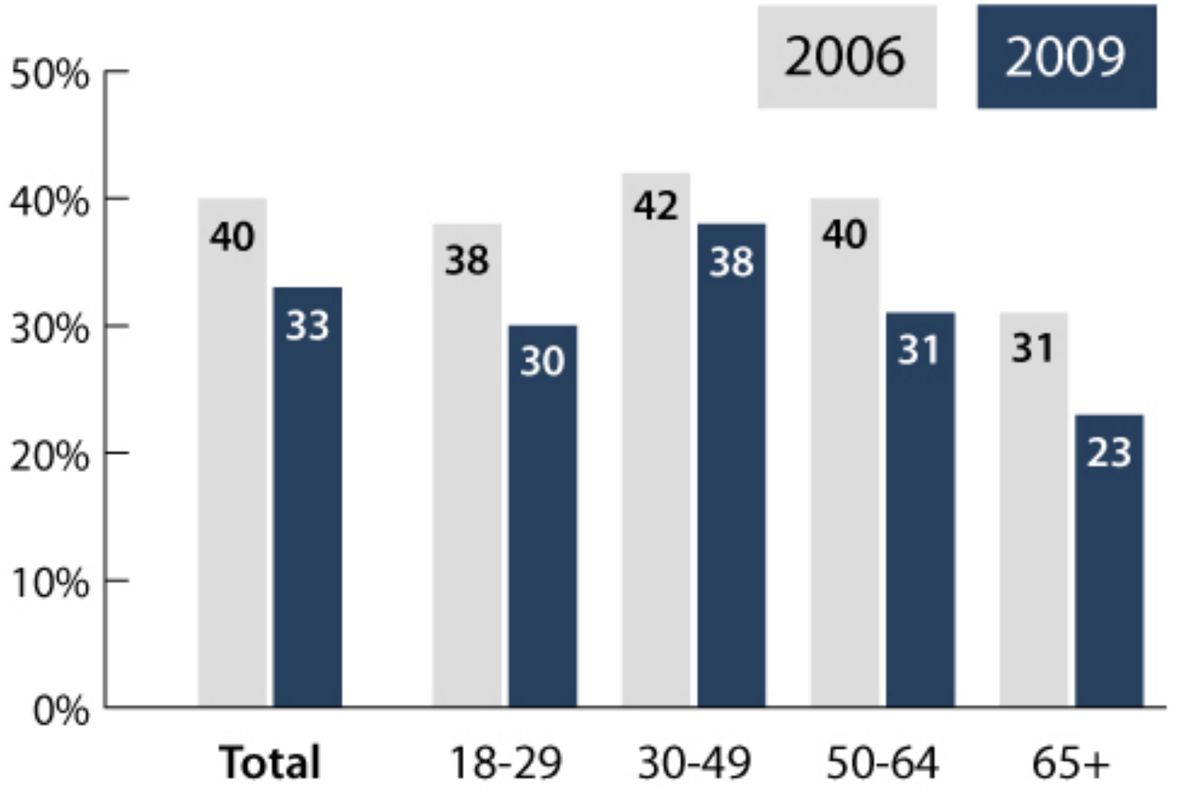
- Information shared, and scope, has increased
- Concerns about information have decreased


2005
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Wall posts
Networks
Photos
Contact Info
Likes
Friends
Name
Birthday
Picture
Other Profile Data
Gender
The Entire Internet
All Facebook Users
Network
Friends
You
Availability of your personal data on Facebook (default settings)
1
40
1K
5M
1B
Number of People
Matt McKeon, May 2010


2010 (Apr)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Contact Info
Friends
The Entire Internet
All Facebook Users
FoF
Friends
You
Availability of your personal data on Facebook (default settings)
1
130
8.5K
400M
1.8B
Number of People
Matt McKeon, May 2010

Concerns over personal information

% of internet users in each age group who say they worry about how much information is available online about them, over time



Source: Pew Internet & American Life Project Survey, August 18-September 14, 2009. Margin of error is plus or minus 2 percentage points for results based on all adults [n=2,253]. For smaller subgroups, the margin of error may be larger. Please see the Methodology section for details.

Pew Internet
Pew Internet & American Life Project

Privacy-consious social media

- Anonymous social media
  - Reddit - no real names needed (but history, and therefore personal info, is maintained)
  - Snapchat - posts dissappear (but can be screenshotted)
  - YikYak - posts are completely anonymous, no user info maintained (popular for bullying)
- Doxxing: finding and publishing personal information (documents = docs = dox) about someone you don’t like

Facebook Privacy

- Competing with Twitter
- Rolled out features as opt-out
  - touted as new features
- 2007: facebook sued by CIPPIC and University of Ottawa
  - breaches of PIPEDA
  - lead to changes in facebook
- Nathalie Blanchard (Quebec) denied insurance claims for depression based on photos on facebook

Facebook data ownership

- Who owns the data?
  - two people contribute
  - what if one person deletes the account
- Memorials
  - facebook user pages maintained after death

  - Aside: What happens to your password-protected data when you die?
  - Does anyone else have your password? Is it in your will?

Privacy and Age

- Assert: Children should be able to “wipe the e-slate clean” at 18
  - We all do dumb things when we’re young

- Children get an email address from school at a young age
  - Who maintains the privacy / integrity of that email address?
  - How long can the student use it?

Phishing: easier with private information

- Pretending to be a trustworthy party to obtain personal information
- Not limited to internet
  - Phone scams
  - but much easier to find targets with email
- Click on this link
  - takes you to a fake site that looks real
  - Password? they have everything about you

Dear PayPal Client,

During our regularly scheduled account maintenance and verification, we have detected an error in your billing information on file with PayPal. This might be due to one of the following reasons:

- A recent change in your personal information (I.E. change of address)

- Submitting invalid information during initial Sign Up process

- An inability to accurately verify your selected option of payment

In accordance with the PayPal User Agreement and in order to make sure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. In order to secure your account and quickly restore full access, we may require some specific information from you.

https://www.paypal.com/cgi-bin/webscr?cmd=_login

Other personal data attacks

- Catfishing - pretend to be someone else and scam people on dating sites
- Blackmail - steal sensitive personal data and demand a payout
- Identity Theft - construct a complete profile of a person and use that to imitate them online

Lawful Access

- government and police are allowed to access otherwise private information, when conditions warrant
  - search and seizure,
  - production orders (you are ordered to produce this document)
  - interception of private communications.
- Strongly controlled by charter rights
- https://www.loc.gov/law/help/encrypted-communications/canada.php

Accessing personal electronics

- If law enforcement has a warrant, should they have the ***ability*** to break in to a secured device?

  - YES: if data on the device could help the investigation, the owner should be compelled to unlock. If owner is unavailable, the manufacturer should unlock
  - NO: digital locks don't work that way. If a manufacturer builds in a back door, it's orders of magnitude more likely that it will be broken by hackers, removing the security for all owners.

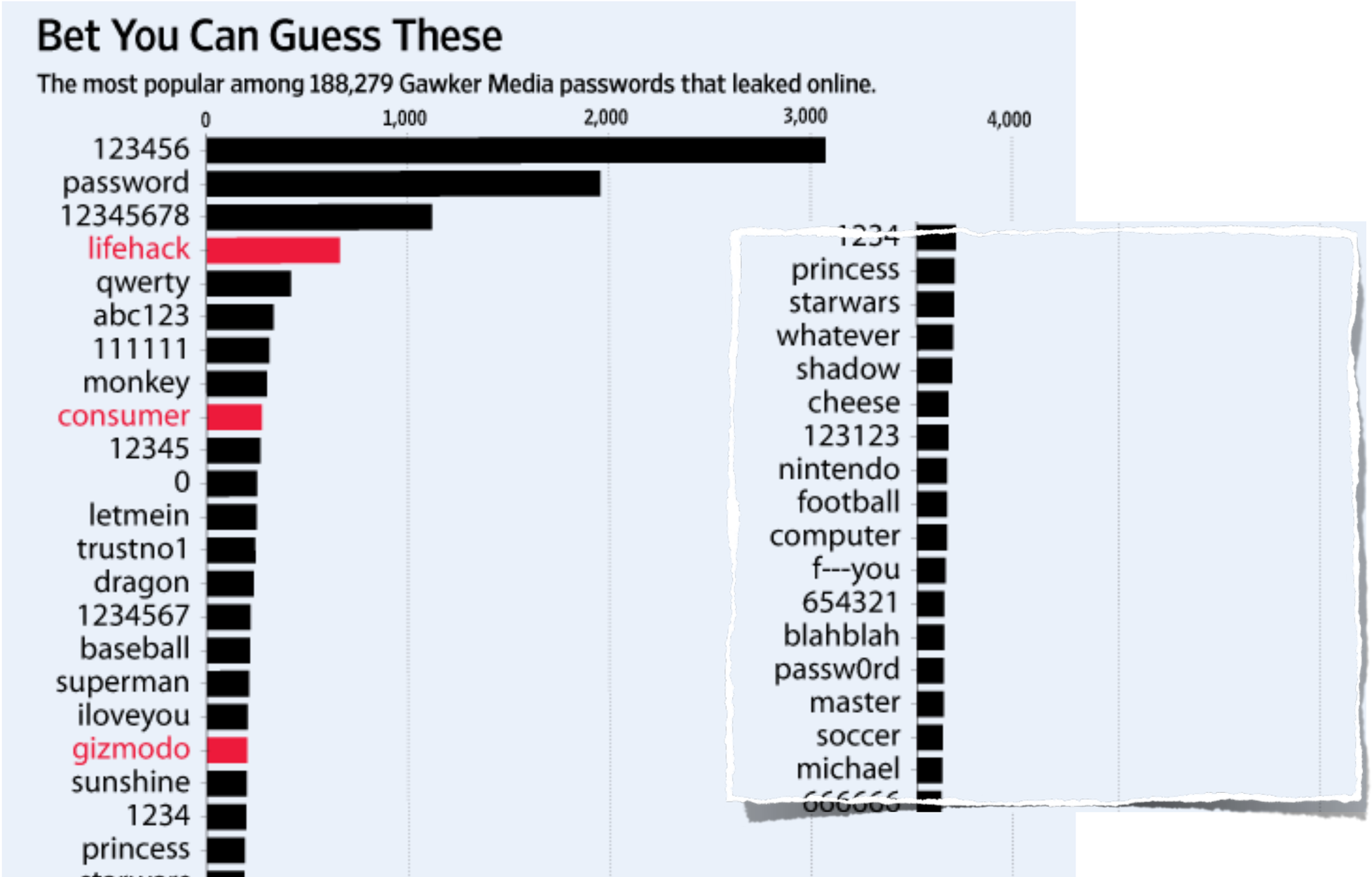
Solutions to Privacy Issues

- Awareness
  - learn about PIPEDA, privacy policies
  - challenge businesses and govt organizations with shady practices
  - Don’t give any info
    - not even for “demographic purposes”
    - If they want it, they can pay for it. it’s worth lots of money to them
  - Trust
    - 3rd party verification for websites

Passwords

- Do you change often?
- Do you have common ones you use?
- do you use good passwords?
- Are you forced to change?
  - does that help or hinder?

Gawker media password breach



Protecting in the event of a breach

- Zero-day exploits exist, data protection is not perfect
- If/when data is stolen, can it still be protected?
- Encryption: jumble the data in a way known only to you
- Differential privacy: Collect the data with random deviations in a way that preserves the statistical qualities but removes personal information
- Data Salting / Dithering: randomly alter the data in a way known only to you

Solutions: Technology

- Citizens
  - Anonymizers, Encryption, two-factor authentication
- Organizations
  - Independent numbering system
  - better security question than “mothers maiden name”
  - Secure databases, strong authorization, access logging and accountability
  - Audit trails
    - privacy issue?

Two-factor authentication

- Choose two of
  - Something you have, something you know, something you are

  - Something you have: your device, or a credit card, or an encryption fob
  - Something you know: your password, pin, security questions
  - Something you are: biometrics.

Biometrics

- Using a part of yourself to identify yourself
  - Classic example: Fingerprints
- Good: harder to circumvent, less likely to have duplicate people with same ID, everyone has one
- Bad: circumvention can be painful, privacy
  - Movies: cutting out eyes, cutting off hands
- Main advantage: Live matching
  - You need to be you right now for the thing to work

Comparison of Biometrics (Yun 2003)

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

Biometric examples: phones

- Fingerprints; Iris Scanners; Face ID
- Usually used as part of two-factor identification
  - “better than nothing”
  - “better than a passcode”

- Considerations of biometrics
  - Criticalness of the data being protected
  - Aggressiveness/resourcefulness of attackers

Issues for biometric implementations

- Must have options
  - Hand in cast = no fingerprints
  - Blind person = no retina scan
- Circumvention
  - Someone gets my bio-data, I'm compromised for life
- Modification
  - Laser eye surgery, cosmetic surgery, laryngitis

Consequences of Biometric errors

- False positives
  - Criminal gains trusted access
  - More security, more trust because if heightened confidence
- False negatives
  - True individual does not get access
  - No recourse
    - How do you prove it's you when your fingerprint doesn't match?

Biometrics and poisoning the well

- Apple's new face ID on iPhone x
  - Many people compare it to samsung's face ID that can be defeated with a photograph
  - Apple's tech can be defeated, but requires significantly more to do so
    - Accurate 3d model of the person's face, for one
  - Fingerprint scanners that can be defeated using a photocopy