Privacy II

Protecting Privacy: Technologies, Markets, and Laws

Privacy Threats: The Story So Far

As we've discussed:

- Virtually anything and everything we do on the internet can be (and often is) recorded.
- Huge amounts of personal data are stored by governments and private sector organizations.
- Users are often not aware of data collection.
- Software is complex (to make, to implement, and, especially for users and regulators, *to understand*) .
- Leaks/data losses happen (accidentally or through theft or misuse)…

…And, thanks to recent developments in computing and ICT:

- Collection of 'small', disparate items can provide in aggregate a detailed profile of individuals or organizations. (E.g., data mining, dataveillance, **profiling**).
- **Re-identification** has become much easier due to the quantity of information and power of data analysis tools.
- If information is placed on a public web site (even once; even if it is subsequently removed), it may be available to everyone, potentially forever.

Protecting Privacy: Individuals

- To some extent, individuals can help to protect their own privacy. E.g., by:
  - Being careful about what they post on social media (e.g., "away from home" status)
  - Being careful about what companies they deal with
  - Using privacy-protecting settings on their devices
  - In general, being careful about what they consent to
- But, when it comes to computing and ICT, there are obvious limitations. Most of us, most of the time, cannot directly protect information about ourselves…

- …especially once it has been shared, especially in cases where supplying it is either **non-voluntary** (e.g., taxation) or **practically unavoidable** (e.g., credit card use, online financial transactions, internet search).

- Instead, most of us, most of the time, have to depend upon (i.e., *trust*) businesses, organizations, and governments to protect our privacy.

  But, of course, our privacy also needs to be *protected from* businesses, organizations, and governments.

Protecting Privacy: Technologies

- Individuals and organizations can also choose (or, in some circumstances, be required) to use privacy protection technologies. E.g.:

  - **Ad blockers/cookie disablers** (to prevent tracking and profiling)
  - 'Do Not Track' settings in browsers; VPNs (ditto)
  - **Public Key Encryption** (PGP, TLS) and **Digital Cash** (Bitcoin, Ethereum)

Protecting Privacy: Law

- In general, laws exist, *inter alia*, to protect us from others and, at least in (broadly) liberal constitutional societies, to protect us from governments.

  Similarly, privacy laws and (legal) privacy rights may held either against other private parties or held against governments.

- There is debate, however, about how extensive these protections should be and what purpose they should serve…

Free Market View

- "**Freedom of Contract**": Individuals are (and should be) free to make voluntary agreements – including agreements about how much/what forms of privacy they want. [Compare: safety, environmental protection.]

- In fact, there may be considerable diversity of individual tastes and values relating to privacy.

  E.g.: Some may be willing to trade some privacy for convenience or efficiency; others may chose to pay extra for heightened privacy protection…

- The Main Argument: The market will respond to consumer preferences about privacy (and other things, like safety) since market participants have a financial incentive to do so.
- Moreover, **contracts** (e.g., purchase agreements) can be made (relatively) clear and specific and are (relatively) readily enforceable. (Compare: "opt-in")
- Regulatory (e.g., government) solutions, by contrast, may not accurately reflect consumer preferences and may be ineffectively or unfairly enforced and/or may stifle innovation.

Consumer Protection View

- **Imbalance of Power**: The market view assumes that individuals know enough about privacy threats to make informed decisions. But this is often simply not the case.
- Instead, consumers need to be protected from their own lack of knowledge, judgment, or interest. (Compare: "opt-out")

  E.g.: The potential uses (including **secondary uses**) of personal information are nearly boundless – *very* few individuals are able to accurately appraise this…

- Implication: Informed consent is not a sufficient protection. Not only are individuals unlikely to be adequately 'informed', they also lack **bargaining power** to actually realize their privacy preferences. (Compare: negotiating a loan.)
- Moreover, errors in databases, leaks of personal information, etc., can have massive and costly effects – possibly more than individuals *should* consent to.
- So: **Regulations** – Legal positive rights to privacy protection.

Privacy Laws

- Constitutional protections against privacy violations typically apply to governments (and/or their agents, or government-regulated industries).

  E.g., the U.S. Fourth Amendment; Section 8 of the *Canadian Charter of Rights and Freedoms*.

- Legislative protections may also apply to individuals and private parties (e.g., companies and corporations).

  E.g., U.S. *Fair Credit Reporting Act* (1970); Canada's PIPEDA (2000)

The U.S. Fourth Amendment

"*The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*."

- Sets limits on government's rights to search homes and businesses and/or to seize documents and other personal effects. Requires that government provide **probable cause**.

The Role of Technology

- In 1789, physical search and seizure was the obvious focus for privacy protections against state intrusion.
- Now, however, much personal information is no longer stored in homes; it often resides in huge data stores that may be outside of citizens' control.
- Also: New technologies allow the government to search homes without entering them and search persons from a distance without their knowledge. E.g., "**noninvasive but deeply revealing**" searches (particle sniffers, thermal imaging systems, location trackers)

Olmstead v. United States (1928)

- SCOTUS allows the use of wiretaps on telephone lines without a court order.
- SCOTUS: The Fourth Amendment to applies only to physical intrusion and only to the search or seizure of material things, not to conversations.

Katz v. United States (1967)

- SCOTUS effectively reverses its position, ruling that the Fourth Amendment *does* apply to conversations.
- SCOTUS: The Fourth Amendment protects people, not places. To intrude into a place where a reasonable person has a reasonable expectation of privacy requires a court order.

Kyllo v. United States (2001)

- SCOTUS rules that police may not use thermal imaging devices to search a home from the outside without a search warrant.

- SCOTUS: Where "*government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search*.'" (emphasis added)

Section 8 of the *Charter*

"*Everyone has the right to be secure against unreasonable search or seizure*."

- Protects personal information against unreasonable intrusion from the state, including information that can be obtained through physical searches, entering someone's property or through surveillance.

- Covers information about which there is a **reasonable expectation of privacy** – information which would *not* tend to reveal intimate details of an individual's lifestyle or personal choices may not be protected.

R v. TELUS Communications Co. (2013)

- SCC finds that the reasonable expectation of privacy protected by S. 8 applies to ICTs such as text messages, even if the data in question is located on a third-party server.

R v. Marakah (2017)

- SCC: An individual may have a reasonable expectation of privacy in an ‘electronic conversation’; texts found on another person’s device therefore may still be protected against unreasonable search and seizure.

R. v. Jones (2017)

- Relying on its reasoning in *Marakah*, SCC rules that the sender of a text message has a reasonable expectation of privacy in records of that message stored in a service provider’s ‘infrastructure’.

R v Fearon (2014)

- SCC holds that police search of a cell phone without a warrant during an arrest does not violate the Charter. Police must follow several search guidelines, however.

R v. Shergill (2019)

- Ontario Court of Justice holds that an accused person cannot be compelled to unlock or provide a password for his device.

"A Right to Privacy"

- In 1890 Warren and Brandeis published a law review article first articulating a general right to privacy – prompted by new technologies such as photography and mass-circulation newspapers.
- "**The inviolate personality**" – Individuals have a "right to be let alone" based on, but distinct from, property rights.

Samuel Warren

Louis Brandeis

PIPEDA (2000)

- Governs how federally regulated businesses handle personal information. *Inter alia,* individual data subjects:
- Have a right to know why an organization collects, uses or discloses their personal information. (I.e., **consent** must be obtained)
- Have an expectation that organizations will collect, use or disclose their information reasonably and appropriately, and not use the information for any purpose other than that to which they have consented…

- …Have an expectation that organizations will protect their personal information by taking appropriate security measures
- Have an expectation that the personal information an organization holds about them to be accurate, complete and up-to-date
- Have right to access their personal information and ask for corrections if necessary
- Have a right to complain about how organization handles their personal information if they feel their privacy rights have not been respected.

EU Privacy Regulations

- EU privacy rules are considerably more strict than U.S. regulations

  Data Privacy Directive (1995)
  General Data Protection Regulation (2018),
  and, just recently, the *Digital Services Act* (2022)

- The GDPR prohibits transfer of personal information to countries outside the EU that do not have an adequate system of privacy protection. I.e., the GDPR imposes requirements on businesses located *outside* the EU.

The "Right to be Forgotten"

Created by the a decision of the Court of Justice of the European Union (CJEU) in 2014. The CJEU held, *inter alia*:

1. Internet search engine operators (ISEOs) such as Google are "**controllers of personal data**" under EU law.

2. Individuals have a right, under certain circumstances, to request that ISEOs remove links to legally available personal information about them and ISEOs must consider such requests.

- Les dues meitats indivises d'un habitatge al carrer Montseny, 8, propietat de MARIO COSTEJA GONZÁLEZ i ALICIA VARGAS COTS, respectivament. Superfície: 90 m². Càrregues: 8,5 milions de ptes. Tipus de subhasta: 2 milions de ptes. cadascuna de les meitats.

hemeroteca.lavanguardia.com

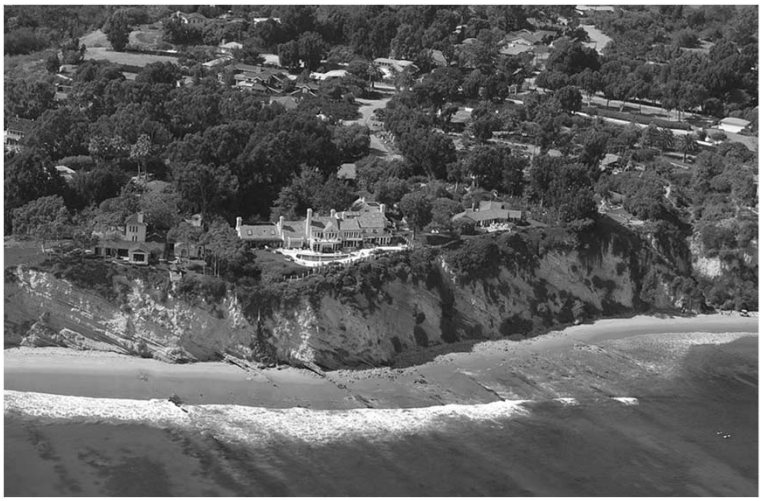
Foreclosure auction notice published in *La Vanguardia*, Jan. 19, 1998

The "Streisand Effect" ?

newsweek.com

Mario Costeja González, 2013

The "Streisand Effect"



en.wikipedia.org

"Image 3850," Kenneth Adelman, 2005

The Right to be Forgotten

- N.B., a positive (claim) right. In effect, a right to request **de-linking** (de-indexing).

  I.e., the underlying data source is <u>not</u> erased, simply filtered from the ISEO's search results within the EU.

- As of July, 2015: **282,407** requests; **≈ 411,000** URLs removed (≈ 40% of those requested for removal).

- But fairly easily circumvented. (Newman)

Privacy: Ethics

- Besides individual actions, technologies, and laws, privacy is, of course, also (at least potentially) protected by professional ethical codes and/or principles proposed for adoption by privacy-focused organizations.

Fair Information Principles

Per B&H (62):

1. Inform people when you collect information
2. Collect only the data needed
3. Offer a way for people to opt out
4. Keep data only as long as needed
5. Maintain accuracy of data
6. Protect security of data
7. Develop policies for responding to law enforcement requests for data