Privacy I

"*The future is private*" – Mark Zuckerberg (2019)

…But is it?

Next up in PHIL 232…

- For the last few days we've been looking at the basic outline of some of the most commonly discussed ethical theories and concepts.

  The idea: From here on out, we'll be able to *apply* those theories and concepts and use them to investigate some important issues related to computing and ICT.

- You'll recall from before: In the present day (and very likely into at least the immediate future) computing and ICT are all-but-undoubtedly among the most significant forces shaping human life and social institutions…

- …Which is to say, computing technology is *powerful*. And, by virtue of that power, the people who shape and direct computing technology [and that may include *you*, soon enough] are also capable of exercising great power.

- A (somewhat nasty) implication: You could think of the topics that we'll be looking at for the next few weeks (privacy, expression, intellectual property, etc.) as **things you may be expected – or *tempted*, or *compelled* – to do, to exercise power over**.

Aspects of Privacy

1. Freedom from **intrusion** into records, data, dwelling, etc. (being left alone)

2. **Control** of personal information

3. Freedom from **surveillance** (e.g., from being tracked, followed, watched)

1 and 2 are often discussed together under the heading "**data privacy**." The idea of "**dataveillance**" suggests how all of these are becoming less distinct, however.

Privacy Threats

Intentional

- Institutional uses of personal information for 'legitimate' purposes and processes (by governments, corporations, private parties)
- Unauthorized use or release by "insiders"
- Theft of information

Unintentional

- Inadvertent leakage of information
- Our own actions/carelessness/ignorance

Some Descriptive (Historical / Anthropological) Background

- Possibly it's simply a fact about human nature that people typically have an interest in or inclination to snoop into other people's affairs.

- In fact, some scholars argue, the *very idea* of privacy may be inaccessible to people living in close proximity to others in small-scale, traditional societies.

  I.e.: Can you even conceive of privacy if you live in a doorless, 1-2 room dwelling with your extended family, in a small community where everyone knows everyone else's business?

De Facto Privacy Protection

- On the other hand, prior to modern technologies, people generally enjoyed fairly good ***de facto*** privacy protection:

  E.g.: Limitations of human memory, inefficiencies in paper record-keeping; limitations of information-gathering practices used in pre-digital times.

- Unless a person had done something especially *memorable* (whether good or bad), memories would likely fade; even events judged to be worth recording on paper (or clay tablets, or whatever) would likely eventually become relatively *inaccessible.*

Privacy, Computing, and ICT

- In a number of obvious (and sometimes less obvious) ways, privacy is threatened by ICT and computing.

- Thanks to ICT, large quantities of personal information can now be collected, stored, processed, and retrieved at low (and decreasing) cost. (E.g., search query data, financial transactions, location tracking data, metadata, data mining, etc.)

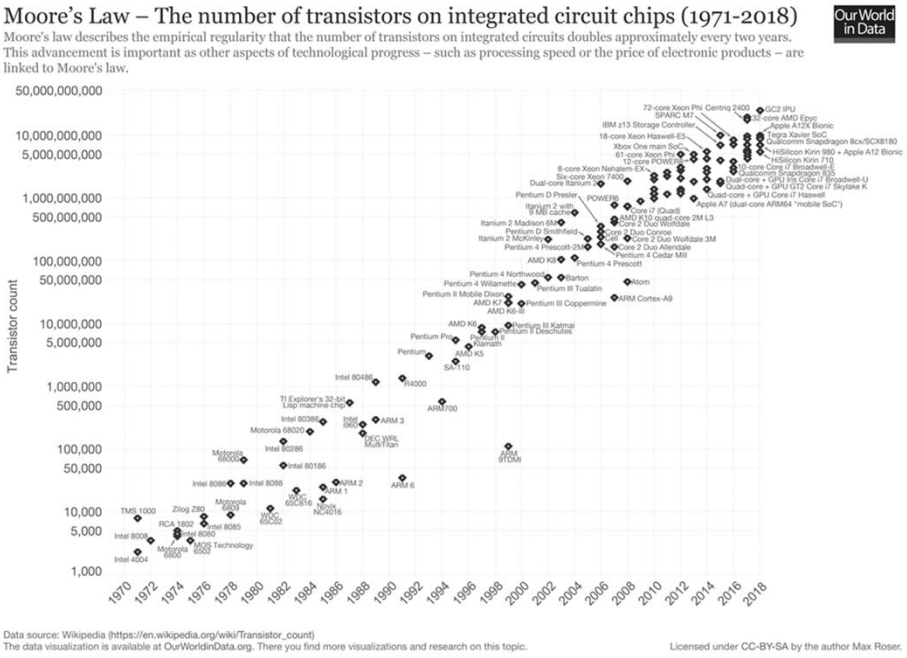
  Surveillance is cheaper, more effective (and so more widespread) than ever before. (E.g., CCTV, facial recognition, 'dataveillance')

"Moore's Law"

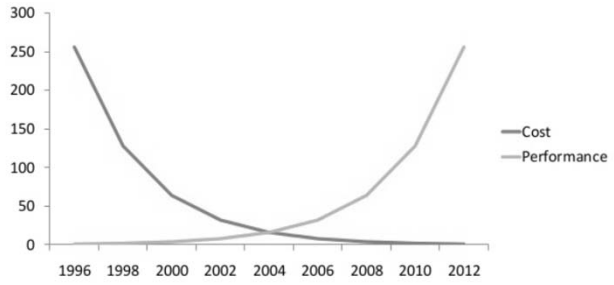
- Worth noting: Technologies (presumably) have regularly posed threats to privacy in the past. (E.g., written records vs. relying on human memory.)

- But in recent decades, computing and ICT have experienced literally *exponential* increases in power, speed, cost-effectiveness, etc.

  This is a direct reflection of **Moore's Law**: Intel co-founder Gordon Moore's (1965) observation that the number of transistors on an integrated circuit doubles about every 24 months…



So, In General….



Privacy Implications

- As computing and ICT become progressively faster, more powerful, cheaper-per-unit-of-work, privacy will become more expensive and harder to maintain.
- One aspect of this: ICT creates *new ways* to collect and use personal data, new ways to put people under surveillance, ways that would have been impractical or prohibitively expensive previously…

Commodification: "Secondary Use"

- Personal information has become (literally) a **commodity**, something that is routinely bought, sold and traded.

  Cf. ChoicePoint (LexisNexis Risk Solutions), Autonomy Corp, Clearview AI, etc.

- Surveillance technologies (cameras, facial/gait recognition, dataveillance) will become cheaper, more effective, more ubiquitous. Cf. **David Brin's** (1998) "corollary to Moore's Law"…

The Nature of Information

- Still other threats to privacy stem from the new forms, the new media, in which information can be stored and processed.

- As mentioned, once upon a time people could at least rely on various forms of *de facto* privacy protection.

  Increasingly, though, those protections are undermined by the nature of digital information…

Analog vs. Digital Information

- **Analog information** (e.g., written records, word of mouth communications, memories): Relatively costly to store and reproduce, fragile, and apt to degrade (unless considerable effort is put in to its preservation).

- **Digital information**: Cheaply and easily stored and reproduced (with no or minimal degradation), sturdy, and highly durable (unless some effort is put into destroying it).

  Online digital information is, one could say, *unforgiving*…

calgaryherald.com

Images from Alberta MLA Deborah Drever's Facebook feed, 2014; 2010

Why Value Privacy?

- OK, so…privacy is 'under threat', especially from computing and ICT…

  …but why (ethically speaking) should we care? Why *value* privacy?

- Could it be that privacy is *only valuable to people who have something to hide*?

Privacy: Ethical Justifications

I. Privacy as a Natural (Negative) Right

- Locke: Among our basic, inalienable rights is a right to **property**. (Part of the package: "Life, Liberty, Property")
- The right to private property, on the Lockean view, is a consequence of our natural right of ownership over our own bodies: We acquire property rights when we "*mix our labour*" (i.e., the activity of our bodies) with materials in the commons.

  I.e., our ownership of property is a natural extension of our **self-ownership**…

- …So, since I ‘own’ my body, no one else has a right to interfere with my body without my consent (e.g., by assaulting me); since I own this parcel of land, no one else has a right to trespass on it without my permission, etc.

- A natural right to privacy might work in the same way: My personal data, my thoughts and actions, constitutes a “personal space,” and no one has a right to enter or change or use that personal space without my **informed consent** (at least not without special justification – e.g., a judicial warrant).

II. Privacy and Autonomy

- Kant: A rational being’s freedom and rationality are what distinguish her from the rest of nature.

  Our capacity for normative self-determination is what makes us deserving of respect and what obliges us to respect the self-determination of others: I deserve respect because I can freely determine my future and my destiny; it would be *logically inconsistent* of me not to respect this same capacity for self-determination in others…

…so, on a Kantian view, to respect someone is to respect her **autonomy** – we must take account of how *our* actions might affect her projects and decision-making.

- If I **openly** watch someone else's actions, then I *change the context of those actions* and perhaps alter her behaviour. She may become self-conscious, e.g., or alter her behavior to meet (or to thwart) my expectations or approval.
- If I **covertly** (secretly) observe someone else's actions, I may not affect his autonomy consciously, but I nonetheless *"deliberately deceive [that] person about his world"* (S. I. Benn, 1980).

  I.e., a person thinks that her world is (currently) unobserved but, by secretly observing, I alter the conditions of his life *for reasons that cannot be her own*.

III. Utilitarian Justifications

I. Being under surveillance is unpleasant and mentally taxing. So, in cases where the unpleasantness exceeds the utility gained from surveillance, U would hold that surveillance is not justified (but also conversely).

II. Personal information about me obtained/used by others may be *inaccurate*. If the value of maintaining accurate information is high enough, U would justify a right to (some degree of) **control** over personal information.

III. In other cases (e.g., a person's dealings with her physician or lawyer), personal information may be potentially damaging precisely *because* it is (or is perceived to be) accurate.

In such cases, U could justify an obligation on the part of professionals to maintain **client confidentiality** (including data privacy).

- U: I.e., a world in which (some degree of) confidentiality and privacy are maintained may be better, in U terms, than a world in which they are not.

Governments vs. Private Parties

- Another (kind of) corollary to Moore's Law (and related phenomena): **When a technology is new, it is generally *expensive* and requires relatively rare, costly expertise to make it work**.

  So, e.g., wiretapping, 'dataveillance', serious data mining, etc. are made possible by new technological developments but, at least at first, those new technologies will only be accessible to entities with quite deep pockets – in particular, *governments*…

- …But, as ICTs develop (at least to date), they will predictably become cheaper, more efficient, and more widespread. (Cf., yet again, Moore's Law).

  So, private parties will increasingly find new uses, new ways of manipulating, personal information.

- In the present: While government databases are quite extensive and quite well-established; **search query data**, **smartphone location data**, **financial transaction data**, etc. are typically held by private parties in the first instance, but can be requested/demanded by governments…

Justifying Privacy: Public vs. Private

- Uncontroversially, governments have a fundamental obligation to protect their citizens. In a democracy, citizens (allegedly) will have **consented** to give governments the power to do this.

- So, the police, CSIS, CATSA, CSE, the FBI, the NSA, etc., all regularly override presumed rights to privacy (via, e.g., wiretaps, direct surveillance, etc.).

  The justification: Government agencies have a higher-order duty to preserve law and order and/or to protect the lives and property of citizens…

- …On the other hand, for a democracy to function, it is pretty widely recognized (at least within functioning democracies) that citizens must have rights to keep some things away from the prying eyes of government.

  Political Autonomy: I.e., without at least some rights to privacy, what are rights to **freedom of expression** or **civil liberties**, or rights to **political participation** actually worth?

The Private Sector

- For private sector organizations, the connection between personal privacy and political autonomy is less clear and the strength of the moral claims to privacy are perhaps less clear as well.
- One formulation of the dispute pits the rights of **data subjects** (whose data may be held without their knowledge and/or without their consent) against the rights claimed by **data gatherers** to create data stores and to profit from them.

Ownership of Personal Information

- A way of framing this: Who *owns* personal information (and therefore has a right to control it)?
- Different states, different legal systems, take diverging views on this:

  See, e.g., Canada's *Personal Information Protection and Electronic Documents Act* [PIPEDA] (2000); the EU's *General Data Protection Regulation* [GDPR] (2018); the Fourth Amendment to the U.S. Constitution.

Privacy as Property Right: 'Opt-in'

- Privacy and consumer advocates tend to see personal information (following from the analogy with property rights) as something that *the data subject 'owns' by default*.
- On such a view, the main question regarding the use of personal information is one of **informed consent**: Where consent means a requirement to **"opt-in"** to any particular use.

  A related option: *Paying* data subjects for use of their data (through discounts, prizes, "free" services). But for poor people this may amount to coercion; many people will understand all of the uses to which their data might be put.

Privacy as Data Protection: 'Opt-out'

- On the other hand, data-gatherers (and laws that protect them), tend to construe the property rights in question as *their own* (i.e., the economic value that they have created through gathering information and putting it into a useful form).

- The main question about privacy, on this view, is thus one of (adequate) **privacy <u>protection</u>**. [Recall U.]

  For the private sector, this typically means being given an opportunity to **"opt-out"**