Lecture 5: Privacy Theory
CSC300

Ishtiaque Ahmed

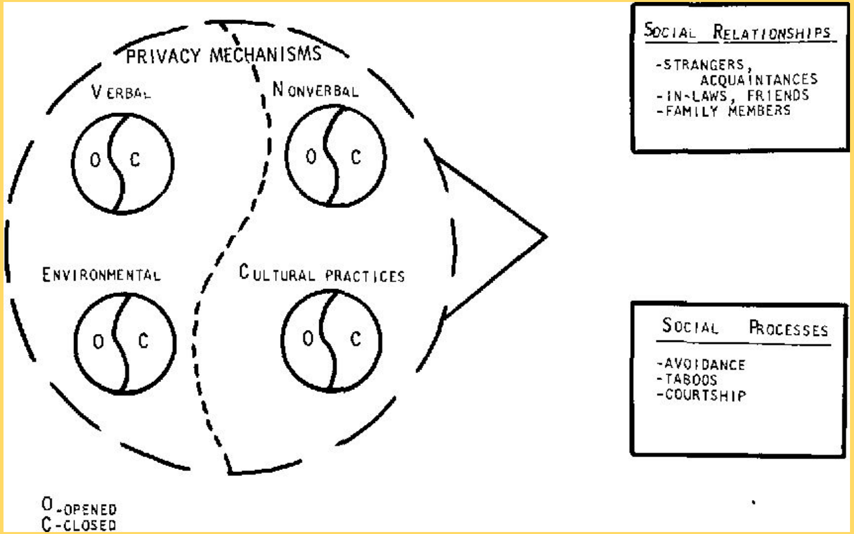
Where we are

- We have learned the theories of ethics
- We have learned how technologies can be political, and why ethics is needed
- We have learned how data also be political, and how it is used for realizing certain goals
- In this class,
  - Understand privacy from various perspectives
  - Understand the relationship between private and public
  - Understand the relationship between privacy and culture
  - Understand the importance of privacy as an ethical standard

Defining Privacy

- “Rightful control over information flow”
- Different ways of defining privacy varying with across **sociohistorical contexts**
- Involves different **aspects** that may or may not be considered or addressed in certain contexts
  - Ex. Personal privacy from your family vs. Organizational privacy that seeks to keep corporate information confidential
- To enact privacy protection and consideration one needs to have a working **theory of privacy** and what it means for **data/information to be considered private**

Defining Privacy: ‘Privacy Regulation: Culturally Universal or Culturally Specific?’



Source: Privacy Regulation: Culturally Universal or Culturally Specific?

Defining Privacy: Culturally Universal or Culturally Specific?

- **Culturally Universal** in that everyone has a **desire to regulate** openness or closedness - to optimize the amount of privacy that one has
  - Ex. Every culture has processes by which they negotiate privacy
- **Culturally Specific** in that the psychological, behavioural, or technological mechanisms that regulate interaction will differ
  - Ex. Privacy request indicated with a closed door in one culture, by a sign in another

Defining Privacy: Multimechanism Process

- Privacy regulation is a **dynamic, dialectic optimization process**
- **Dynamic Dialectic:** privacy is a boundary control process, alternation between being open and accessible and closing yourself off that shifts with circumstances
  - Ex. Using a tech example, we have incorporated privacy mechanisms into our social media networks: Available, Away, Do Not Disturb, Offline - Change them depending on how accessible you want yourself to be

Defining Privacy: Multimechanism Process

- Involves a network of behavioural mechanisms that people use to achieve desired levels of social interaction
    - **Verbal/ Paraverbal behaviours** – personal space/territoriality, culturally defined styles of responding
        - **Verbal behaviours**: In a conversation: asking for privacy, or indicating that a conversation topic is private by using select word choice
        - **Paraverbal behaviours:** Using body language to indicate discomfort discussing private topics, using technology and artifacts in one's environment to indicate privacy Ex. A lock

Defining Privacy: Multimechanism Process

- Involves a network of behavioural mechanism that people use to achieve desired levels of social interaction
    - **Operate as a system** – involve interdependence and compensatory and substitutable action, use different behaviour combinations to get desired privacy depending on circumstances
        - With the advent of technology, there are more nonhuman agents that are now involved in the system and can be used to regulate
        - Ex. Indicate desire for privacy by leaving room, saying you don’t want to be disturbed, closing door, putting on headphones, blocking notifications on phone etc. all together indicate desire for privacy

Defining Privacy: Multimechanism Process

- Privacy regulation is a **dynamic, dialectic optimization process**
- **Optimization Process** – the ideal amount of privacy may shift from time to time (it is nonmonotonic), deviations from the optimum can be personally unsatisfactory - privacy is **not a maximizing (monotonic) process**
    - Ex. When making new friends because you don't have any, might want less privacy to invite more people into your life - once someone has friends might be more private as new friends are no longer the goal

Breakout Discussion: Privacy as a Dynamic-Dialectic Process

Posting images on Instagram, especially those from meaningful events like a family holiday, can be seen as a dynamic-dialectic process.

This process involves negotiation and renegotiation of what is considered private versus public, and who is included within the privacy boundary.

Breakout Discussion: Privacy as a Dynamic-Dialectic Process

1. **Original Privacy Boundaries:** Initially, only the family members present during the holiday have access to the moments.
2. **Decision to Share on Instagram:** You're actively choosing the privacy boundary. The decision to share will depend on the moment, the photo, and your relationship with your Instagram followers.
3. **Change in Privacy Boundaries:** Once shared, the captured moment changes from private family only to a semi-public one which may include friends, acquaintances, and potentially even strangers (depending on your account's privacy settings)
4. **Who is Included in the Privacy Boundary:** The new privacy boundary, which includes the audience of your post, will interact with the moment and reshape how the moment is perceived, not just by others but also by you and your family.

Breakout Discussion: Privacy as a Dynamic-Dialectic Process

Example: Emotional Disclosure with a Friend

Consider the analogy of emotional disclosure:

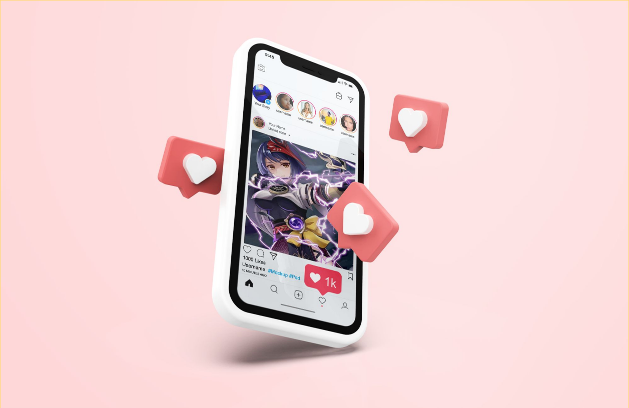
Sharing that you are sad with a friend in-person means including the friend into an limited and intimate privacy boundary (extended to just that friend).

Breakout Discussion: Privacy as a Dynamic-Dialectic Process

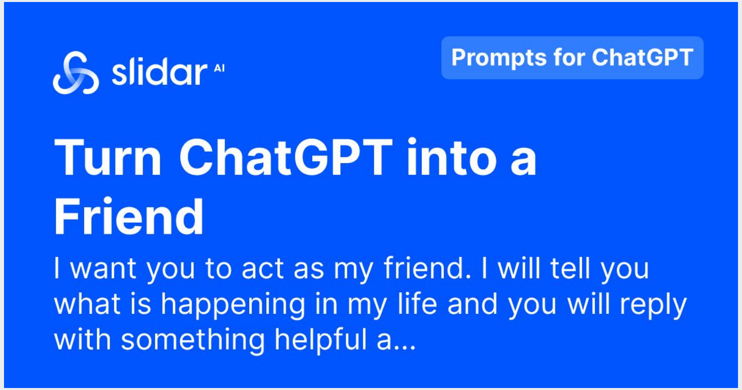
Example: Emotional Disclosure with a Friend

Consider the analogy of emotional disclosure:

In contrast, posting a status update about your sadness on Instagram shares this boundary with all your followers, vastly expanding the circle of people who are aware of your emotions.



Breakout Discussion: Privacy as a Dynamic-Dialectic Process



slidar AI

Prompts for ChatGPT

Turn ChatGPT into a Friend

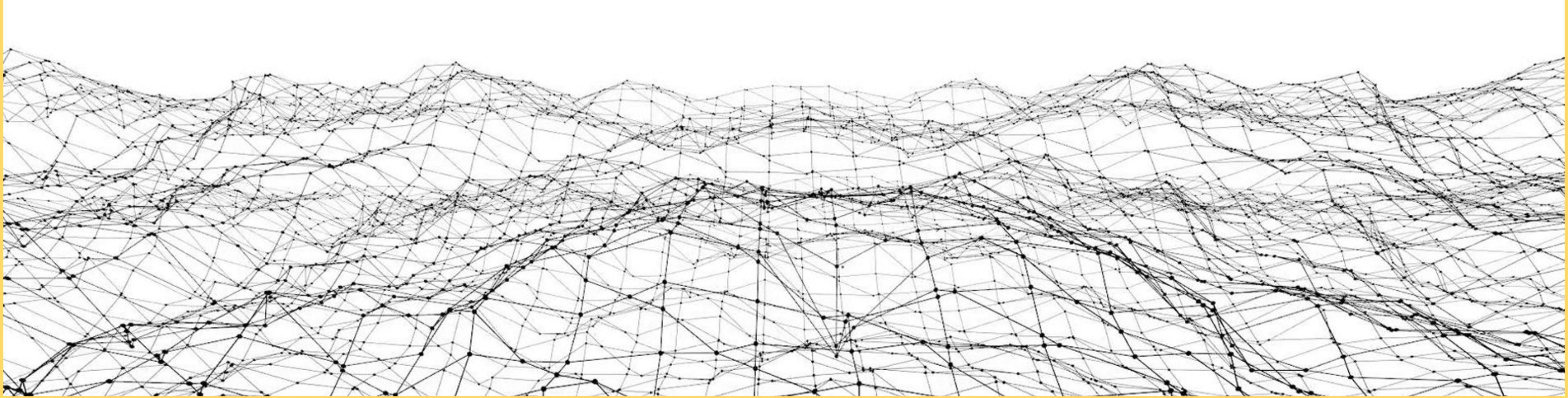
I want you to act as my friend. I will tell you what is happening in my life and you will reply with something helpful a...

Example: Emotional Disclosure with a Friend

Consider the analogy of emotional disclosure. What if we share it with ChatGPT instead ?

- On the surface, you are sharing only with ChatGPT (which is a software) which should not extend privacy boundary
- But ChatGPT saves all your queries and uses it to improve the language model. So your query will be shared as training data to OpenAI, extending the privacy boundary.
- This query will be a part of future version of ChatGPT and will be used to generate responses to all the future users. Does this extend the privacy boundary?

Defining Privacy: As Boundary Regulation: ‘Unpacking “Privacy” for a Networked World’



Defining Privacy: As Boundary Regulation

- If privacy is selective control of the self it involves a **boundary regulation process** where people optimize accessibility along a spectrum
- Generally, boundaries were **physical**, but with the advent of **information technologies**, physical boundaries are disrupted and so others must be considered

Defining Privacy: Disclosure Boundary

- **Privacy and Publicity**
  - Requires selective **disclosure of public information** and **retention of private information**
- **Maintaining privacy often requires disclosure**
  - Ex. Working PR for yourself - you manage public to keep private secret

Defining Privacy: Disclosure Boundary

- **Roles of disclosure can be used to limit rather than increase accessibility**
  - Ex. Professor setting up a website to limit strangers contacting
- ***Active participation in networked world requires disclosure***
  - **Problem**: When participation is not deliberate

Defining Privacy: Identity Boundary

- Self and Other
  - People often act as representatives or members of broader social groups that have set expectations to be incorporated into behaviours
- **Recipient design** – actions/utterances are designed with respect to specific others – self is constructed w.r.t. social arrangements
  - Others are differentiated and treated differently
    - Ex. An employee contacting their employer - formal language with respect using an email vs contacting a friend - casual language over IM

Defining Privacy: Identity Boundary (interpretations)

- **In technology, mutual access mediated by the tech** - you make assessments from a **representation that acts in proxy**
    - **Problem**: When what is conveyed is not when what is intended
        - Ex. Twitter arguments between social groups because one individual was critiquing something whereas another group thought it was an attack

Defining Privacy: Temporal Boundary

- **Past, Present, and Future**
  - Instances of disclosure are not isolated – occur as outcome of sequence of events and stretch into the future
    - Ex. A tweet doesn’t go out into a blank account, preceding tweets set a context, future tweets will fit into the context you create with present tweets, but also into the broader social context - some prediction required abt. appropriateness
  - **Privacy management decision-making occurs in the context of a temporal sequence**

Defining Privacy: Temporal Boundary

- **Privacy management mediated by what was in the past and also what may occur in the future** – management of tensions
    - **Problem:** With information technologies, past interactions are often archived and easy to access, and future interactions will be similarly stored - the tensions that must be managed are magnified
        - Ex. Pulling up ‘receipts’/previous tweets in a Twitter argument to indicate that someone has a history that contradicts what they intend to convey or say in the current moment

Breakout Discussion: Privacy as a Boundary Control Process

Example: Sharing Photo from a Family Event

Disclosure Boundary:

- How does privacy boundary change when you post the photo?
- Does it make a previously private event public to distant family members or acquaintances?
- For example, by sharing these moments, are you able to maintain a level of privacy in personal conversations, as distant relatives may feel updated and less likely to ask probing questions?

Breakout Discussion: Privacy as a Boundary Control Process

Example: Sharing Photo from a Family Event

Identity Boundary:

- How does this post reflect on your online identity?
- Do you consider the diverse audience who might see this post, such as friends, colleagues, or older family members?
- How does the generational aspect influence the content you choose to share?
- For instance, do younger users post differently if their social media audience includes peers versus older family members?

Breakout Discussion: Privacy as a Boundary Control Process

Example: Sharing Photo from a Family Event

Temporal Boundary:

- Have you shared similar family moments in the past?
- If so, how does this history influence the current post?
- Does it feel like a continuation of your usual sharing habits, or does this post represent a new openness?
- If this is the first time you're sharing such a moment, what might this say about a shift in your comfort level with sharing personal experiences online?

Defining Privacy: ‘Privacy as Contextual Integrity’

Defining Privacy: As Contextual Integrity

- Many privacy theories still fail to adequately account for public surveillance and how it breaches privacy
  - Ex. Public records being stored online, consumer profiling/data mining, RFID tags
- Three principles should inform privacy regulation by other agents:
  - **Limiting surveillance of citizens and use of info by agents of govt**
  - **Restricting access to sensitive/personal/private info**
  - **Prevent intrusion into places deemed private/personal**

Defining Privacy: As Contextual Integrity

The Three Principles:

- **Limiting surveillance of citizens and use of info by agents of government**
    - Governments often act overzealously in collecting/using info though some aspects of privacy are defended against government action
    - ***There should be a principled commitment to limited government powers in the name of individual autonomy and liberty as the government has more power than the individual***
- **Restricting access to sensitive/personal/private info**
    - Societal standards of intimacy, sensitivity, or confidentiality deem some information personal and restricted

Defining Privacy: As Contextual Integrity

The Three Principles:

- **Prevent intrusion into places deemed private/personal**
    - Certain spaces/places are considered personal and should be private from the government as well, it should be up to the discretion of the individual to invite the government into these spheres
- ***Determining the application of the principles means that boundary lines are neither static nor universal***

Defining Privacy: As Contextual Integrity

- **Contextual Integrity** is presented as a universal account of what does/does not warrant restrictive, privacy-motivated measures - a conceptual framework and not conditioned by time, location, etc.
- **All arenas of life are governed by norms of informational flow** - happens in a context of **place**, **politics**, **convention**, and **cultural expectation,** shifting across the different arenas
- **Contexts/spheres allow for a normative account of privacy in terms of contextual integrity**

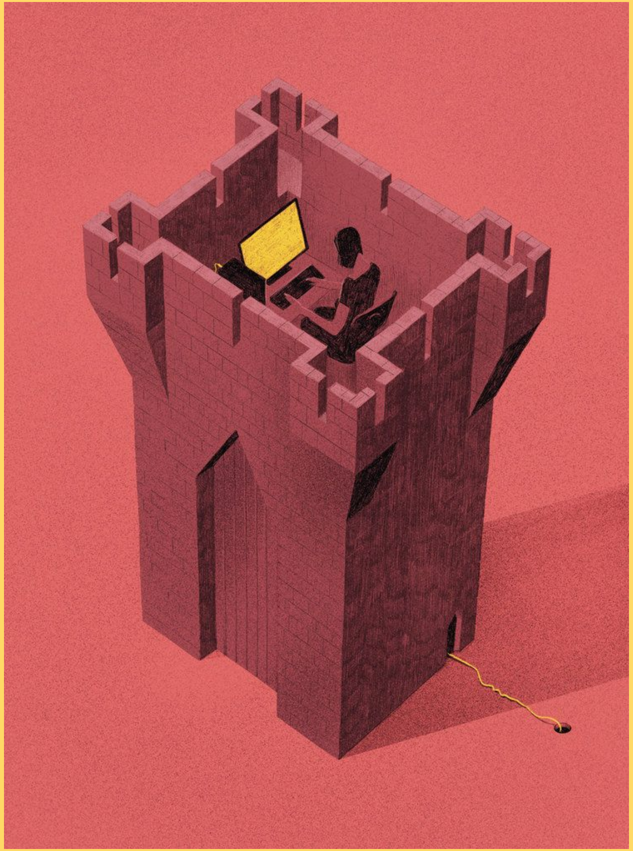
Defining Privacy: As Contextual Integrity

- **Norm of Appropriateness** - Information that is appropriate or fitting to reveal in a particular context will not be appropriate in another
  - Ex. In a medical context you will share information about physical condition but not to your barista
- **Appropriating information from one situation to another can constitute a violation**

Defining Privacy: As Contextual Integrity

- **Norms of Flow/Distribution** - The movement or transfer of information from one party to another will be unidirectional, bidirectional, or nonexistent and will come with certain expectations about how one treats the information
    - Ex. In **friendship**, flow is often bidirectional, assumed to be confidential, at one's own discretion
    - Ex. In **medical settings** the patient is expected to divulge info, but it isn't bidirectional
- **Disrupting the flow or distribution can constitute a violation**

Implementing Privacy



Source: Daniel Stolle

Implementing Privacy: Westin + the USA

- In his books “Privacy and Freedom” and “Databanks in a Free Society” Alan Westin helped to inform and prompt the US to enact **internet privacy legislation** in the 1960/70s
  - He defined privacy as a legal right and the ability to control which information we reveal about ourselves
  - Arguing that individuals should have ultimate control over their information, privacy should be an individual freedom

Implementing Privacy: GDPR

- Created in 2016 and implemented in 2018 the **General Data Protection Regulation** requires organizations processing or collecting information on European Union citizens to safeguard personal data and uphold privacy rights of those in EU territories
- It involves **seven principles of data protection** and **eight privacy rights** that can be enforced with sanctions and fines

Source: gdpr.eu

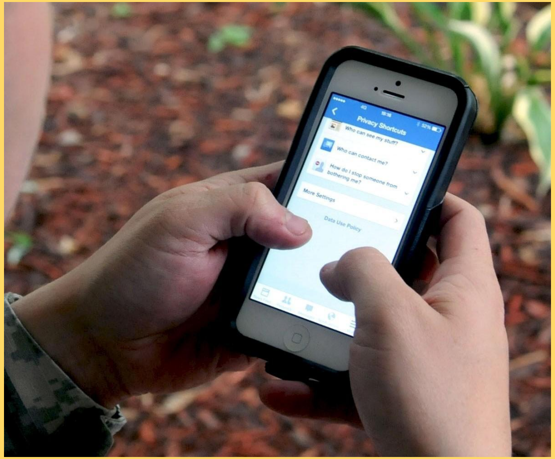
Implementing Privacy: GDPR

- **Principles include:**
  - **Lawfulness, fairness and transparency**
  - **Purpose limitation** — process data for the legitimate purposes specified
  - **Data minimization** — collect and process only as much data as absolutely necessary
  - **Accuracy**
  - **Storage limitation** only store personally identifying data for as long as necessary
  - **Integrity and confidentiality**
  - **Accountability**

Source: gdpr.eu

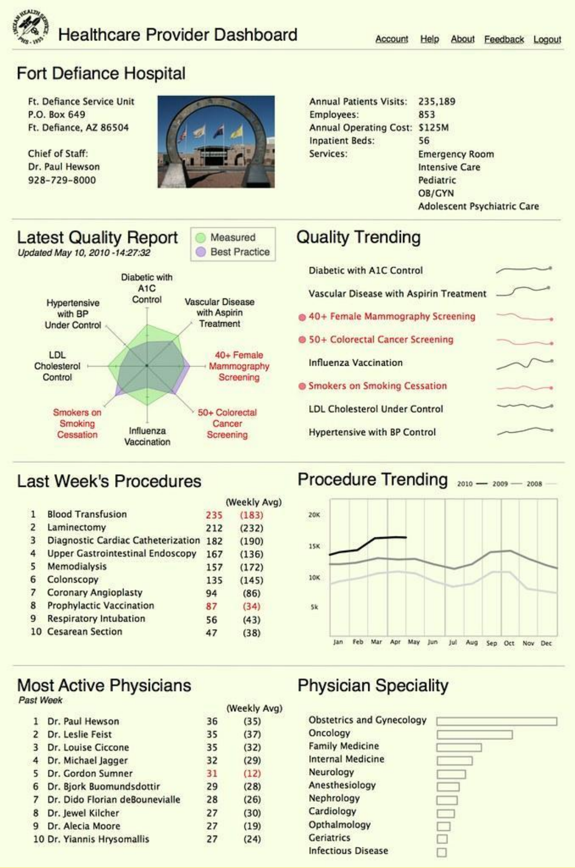
Implementing Privacy: FERPA

- The **Family Educational Rights and Privacy Act (FERPA)** is a United States federal law that protects the privacy of student education records.
  - FERPA allows parents and students over 18 certain rights with respect to education records such as the ability to access, review, and request the correction of inaccurate information
  - Some “directory” information may still be disclosed by schools without consent



Implementing Privacy: HIPPA

- The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** involved developing regulations to protect the privacy and security of certain health information.
    - The major goal is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care



Healthcare Provider Dashboard

Fort Defiance Hospital

Ft. Defiance Service Unit
P.O. Box 649
Ft. Defiance, AZ 86504

Chief of Staff:
Dr. Paul Hewson
928-729-8000

Annual Patients Visits:	235,189
Employees:	853
Annual Operating Cost:	$125M
Inpatient Beds:	56
Services:	Emergency Room Intensive Care Pediatric OB/GYN Adolescent Psychiatric Care

Latest Quality Report
Updated May 10, 2010 -14:27:32

Measured
Best Practice
Diabetic with A1C Control
Vascular Disease with Aspirin Treatment
40+ Female Mammography Screening
50+ Colorectal Cancer Screening
Influenza Vaccination
Smokers on Smoking Cessation
LDL Cholesterol Control
Hypertensive with BP Under Control

Quality Trending

- Diabetic with A1C Control
- Vascular Disease with Aspirin Treatment
- 40+ Female Mammography Screening
- 50+ Colorectal Cancer Screening
- Influenza Vaccination
- Smokers on Smoking Cessation
- LDL Cholesterol Under Control
- Hypertensive with BP Control

Last Week's Procedures

			(Weekly Avg)
1	Blood Transfusion	235	(183)
2	Laminectomy	212	(232)
3	Diagnostic Cardiac Catheterization	182	(190)
4	Upper Gastrointestinal Endoscopy	167	(136)
5	Memodialysis	157	(172)
6	Colonscopy	135	(145)
7	Coronary Angioplasty	94	(86)
8	Prophylactic Vaccination	87	(34)
9	Respiratory Intubation	56	(43)
10	Cesarean Section	47	(38)

Procedure Trending

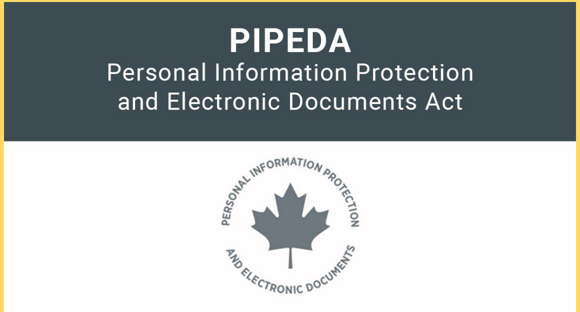
Most Active Physicians
Past Week

			(Weekly Avg)
1	Dr. Paul Hewson	36	(35)
2	Dr. Leslie Feist	35	(37)
3	Dr. Louise Ciccone	35	(32)
4	Dr. Michael Jagger	32	(29)
5	Dr. Gordon Sumner	31	(12)
6	Dr. Bjork Buomundsdottir	29	(28)
7	Dr. Dido Florian deBounevialle	28	(26)
8	Dr. Jewel Kilcher	27	(30)
9	Dr. Alecia Moore	27	(19)
10	Dr. Yiannis Hrysomallis	27	(24)

Physician Speciality

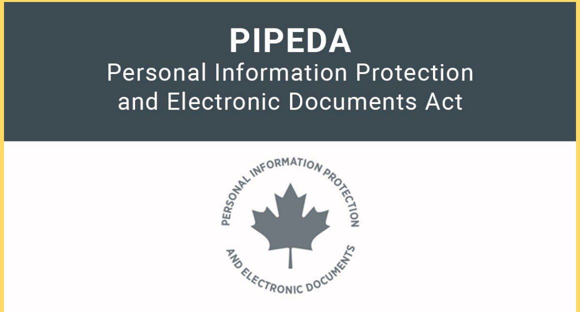
Implementing Privacy: PIPEDA

- In Canada, the Personal Information Protection and Electronic Documents Act
- PIPEDA applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity


PIPEDA
Personal Information Protection
and Electronic Documents Act
PERSONAL INFORMATION PROTECTION
AND ELECTRONIC DOCUMENTS

Implementing Privacy: PIPEDA

- According to PIPEDA, **personal information includes any factual or subjective information, recorded or not, about an identifiable individual,** such as:
  - age, name, ID numbers, income, ethnic origin, or blood type;
  - opinions, evaluations, comments, social status, or disciplinary actions; and
  - employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)



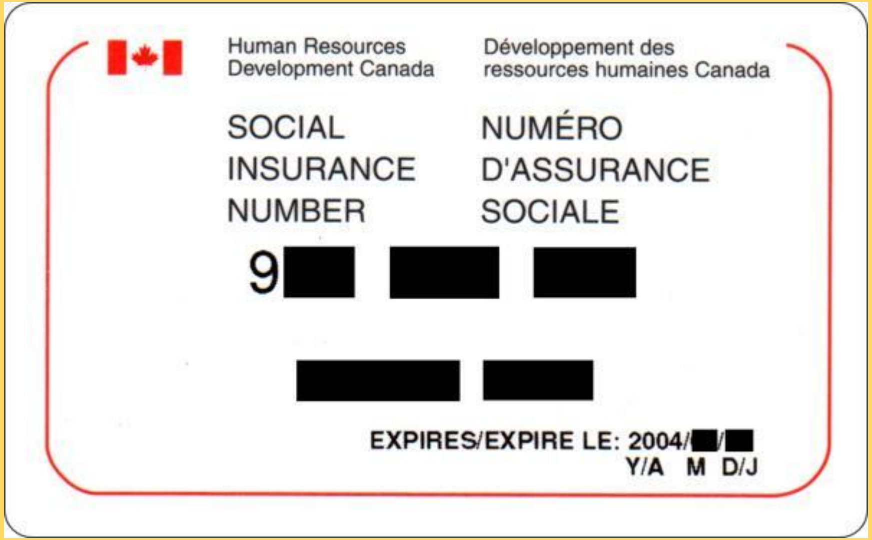
PIPEDA
Personal Information Protection
and Electronic Documents Act

Breakout Discussion: Personal Information

For some information, it is intuitive as to why it would be considered personal information (SSN/SIN, Address, etc.) but for others, it might not be as clear.

Discuss:

- Why might opinions, evaluations, or comments be considered personal information that deserves privacy (as this is listed in PIPEDA as protected personal information)
- Why might educational grades and records be considered personal information that deserves privacy (as this is listed in FERPA as protected personal information)



Human Resources Development Canada

Développement des ressources humaines Canada

SOCIAL INSURANCE NUMBER

NUMÉRO D'ASSURANCE SOCIALE

9[redacted] [redacted] [redacted]

[redacted] [redacted]

EXPIRES/EXPIRE LE: 2004/[redacted]/[redacted]
Y/A M D/J

Breakout Discussion: Personal Information

- What makes some personal information sensitive and subject to protection?
  - Ex. Shoe size is not particularly sensitive information but it is technically personal, however people are very willing to share shoe size with acquaintances but not as willing to share clothing size - what is it that creates this distinction
- How might what is considered personal information and what is relevant personal information vary culturally?
  - Ex. Resume applications in Canada do not typically require a headshot/photograph of the applicant and to some extent this might be considered unnecessary personal information and removed by hiring managers. In some countries, it is the norm to apply with a professional headshot. In both cases this kind of personal information may lead an applicant to be subject to some kind of bias or prejudice from a prejudiced recruiter but whether the photo is to be omitted is subject to different cultural privacy norms

Privacy by Design

Source: Ico

Privacy by Design

- Important to incorporate privacy considerations into the design of technologies and information ecosystems
    - Different considerations might be relevant for different environments
- **Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices** by **Ann Cavoukian** provides an overview of principles that may be reasonably followed in design

Source: EUROPEAN DATA PROTECTION SUPERVISOR

Privacy by Design: 7 Principles

1. Proactive not Reactive; Preventative not Remedial

- To anticipate and prevent privacy invasion before it occurs, rather than remediating privacy risks, they should be anticipated and prevented

2. Privacy as the Default Setting

- Privacy of personal information should be protected and maintained as a default in a given environment
- Action should not be required on the part of the user to ensure privacy of their information, they may choose to disclose it with further action, but protection should be default

Privacy by Design: 7 Principles

3. Privacy Embedded into Design

- Privacy must be a core aspect of the application/environment and be integrated into its functionality - it cannot be an extra consideration or add-on
- It must be imbedded in a holistic, integrated way

Privacy by Design: 7 Principles

4. Full Functionality – Positive-Sum, not Zero-Sum

- Privacy must accommodate all interests in a “win-win” situation rather than in a zero-sum manner that involves trade-offs
- To the greatest extent possible, all requirements are optimized - avoid false dichotomies such as privacy vs. security, seek to optimize both

Privacy by Design: 7 Principles

5. End-to-End Security – Full Lifecycle Protection

- Privacy must be incorporated before any data collection, implementation, or manipulation occurs, throughout the life cycle of the data
    - Data is to be collected and retained securely and destroyed at the end of its life cycle

Source: Ico

Privacy by Design: 7 Principles

6. Visibility and Transparency – Keep it Open

- All stakeholders must be assured that the environment is operating according to stated promises, using visibility and transparency to ensure accountability and trust

Source: Ico

Privacy by Design: 7 Principles

7. Respect for User Privacy – Keep it User-Centric

- The interests of the individual user are to be maintained by keeping the environment user-friendly using the following principles to allow users to manage their own data:
  - **Consent**: should be required for data collection, use, and disclosure
  - **Accuracy**: private information should be as accurate and up-to-date as possible
  - **Access**: users should be provided access to collected data and informed on its use, they should be able to challenge the accuracy and completeness of the data and be allowed to amend it

Case Study
Sidewalk Labs

Source: Sidewalk Labs

Case Study: Sidewalk Labs

- Intended to be a “smart city” in downtown Toronto, building a neighbourhood “from the internet up”
- Intended to use new technologies to track use of parks, retail locations, garbage/recycling disposal units, etc. to allow for and inform more holistic urban planning

- Which principles did it violate? Which principles did it respect?

Source: Sidewalk Labs

Case Study: Sidewalk Labs

Principle 1 -Proactive not Reactive; Preventative not Remedial: It appeared after people began to question privacy laws surrounding the design that privacy protection was not proactive and incorporated into it - trying to remedy the scandal and questioning demonstrated reactive/remedial design

Source: Sidewalk Labs

Case Study: Sidewalk Labs

Principle 2 - Privacy as the Default Setting: Data collection and an consent-less violation of privacy was the default setting

Principle 3 - Privacy Embedded into Design: Privacy was not a major concern for Sidewalk Labs, and was not embedded into the design

Source: Sidewalk Labs

Case Study: Sidewalk Labs

Principle 4 - Full Functionality: It is unclear how users (residents or visitors of the area) would be accommodated in the design and what trade-offs they would have to make, it seemed that corporate requirements were optimized rather than user privacy

Source: Sidewalk Labs

Case Study: Sidewalk Labs

Principle 5 - End-to-End Security – Full Lifecycle Protection: It was not immediately clear how the private information collected would be treated and whether it would follow industry standard data retention and protection protocols for private information

Principle 6 - Visibility and Transparency: It was unclear which personal information Sidewalk Labs intended to collect and how it would be utilized

Source: Sidewalk Labs

Case Study: Sidewalk Labs

Principle 7 - Respect for User Privacy – Keep it User-Centric: Anyone that enters the area would be subject to tracking and data collection; it was not outlined how users might indicate consent to this, access information that is collected, and ensure its accuracy and responsible use/disclosure

Source: Sidewalk Labs

Thank you!