Lecture 9:
Privacy (Contd.)

Recap

- Principles behind HAI
- Fairness, bias in data & techniques for debiasing
- Lecture on privacy in DPI
- Today – privacy laws and principles
  - Necessary to know today!
- Homework
  - How did it go?
  - Was it fun? What surprised you?

Next assignment:

- Build a user-interface for your assignment
  - Pick whoever you think will be the user of the model's predictions
  - Build an application where the model's predictions will be made available, for the user.
  - Doesn't have to have all details, but whatever is relevant.
  - Show the model's predictions in a meaningful manner
- For example:
  - If we have a COVID mortality prediction, the user would be Health Administrator, Hospital, etc. – each with different needs. Think what they would need and then build this out.
- This is just a building block for subsequent assignments—so think carefully about what the user will do with the model's predictions.

Privacy

- “Right to be left alone” (Warren & Brandeis, 1890)
- Now → Control over personal data
- Right of individuals to control access to their personal information, including how it is collected, stored, used, and shared.
- In India, privacy is a fundamental right (2017)
- It is guaranteed and protected by our constitution
  - One can go to a court of law, including against the government
- Not absolute, and can be restricted in some cases
  - National security, public order, etc.

Privacy in ML / AI

- Personal, sensitive data of people
- People have a right to control access to that data
  - Including for processing & machine learning purposes
- Care is needed when gathering, storing, using them

Key concepts in privacy

- Personal data -- Any information that can directly or indirectly identify an individual (e.g., name, age, location, gender…)
- Personally identifiable information – directly identifies (phone number, name, email)…
- Sensitive personal data:
  - Subset of personal data, whose misuse can cause harm
  - E.g., Education/health/financial records, caste, biometrics, etc.
  - Rule of thumb: If its exposure creates serious risks, it's sensitive.

Consent

- Because privacy is a fundamental right, and we still want to gather personal data of people
  - “Consent” → the individual’s clear, informed agreement to gather and use the data
- Data processing
  - Any operation on personal data, automated or manual.
  - Collection, Storing, Sharing, Running ML models, Aggregating the data for dashboards, …
  - Privacy law regulates processing, not just “collection.”
  - Consent is for all of this – collection & processing

Consent, purpose & its limitation

- You can’t just use data for anything, just because you have it
- You say what you will use it for, and use it only for that
- “Purpose limitation”
  - Data must only be used for the purpose it was collected, and not repurposed without new consent.
- Example:
  - Student survey says “this data is only to improve quality of instruction”, it cannot be used for anything else (e.g., mental heath predictor algorithms)

Privacy laws → rights & responsibilities

- Data principal → person who the data is about
- Data fiduciary / controller→ entity (person, organization) controlling the collection & processing of the data
- Data processors → subcontractors / organizations hired by controllers for processing (e.g., field survey data gathering, cloud companies)

- Principal has rights
- Fiduciary / controller has responsibilities (to protect principal rights)
- Processors – governed or not governed (depending on law)

Rights of data principles

- Right to know (what data is collected, why).
- Right to access (get a copy of personal data).
- Right to correction/erasure (fix errors or request deletion).
- Right to withdraw consent (stop processing anytime).
- Right to redressal (complain to Data Protection Board / regulators).

Responsibilities

- Responsibilities (for organizations / data fiduciaries)
- Purpose clarity: State why they collect data.
- Data minimization: Collect only what’s necessary.
- Storage limitation: Keep only as long as needed.
- Security safeguards: Protect against breaches.
  - Confidentiality → I trust you to protect privacy to keep data secure and confidential, so others don’t breach that privacy!
- Transparency & accountability: Show compliance when asked.

Practical implementations: varies by nation

- DPDP Act (India) vs. GDPR (EU)
- Two landmark privacy frameworks
- Different contexts, legal principles → slightly different implementations

DPDP Act vs. GDPR: Scope

- Digital Personal Data Protection Act
- Regulates processing of digital personal data (incl. offline data digitized later)
- Governs data fiduciaries that process personal data
  - Processors act under the instruction of the fiduciary
- Sensitive data was in earlier drafts, but removed

- General Data Protection Regulation
- Regulates processing of all personal data
- Governs everyone involved in processing (collecting, storing, using, ..) personal data
- Data controllers + processors
  - (org. ordering + cloud companies)
- Special cases → extra care

DPDP Act vs. GDPR: Consent

- DPDP requires principal to provide free, informed, specific, unambiguous
  - Exceptions to government
- Allows withdrawal
- Consent managers to manage consent lifecycle & interoperability
  - Covers digital-only interactions
- Purpose limitation
  - Exceptions to government

- GDPR requires freely-given, specific, informed, unambiguous consent
- Right to withdraw anytime
- Data used only for stated purpose

DPDP Act vs. GDPR: Principal rights

- DPDP
  - Right to access information
  - Right to correct & erase personal data
  - Right to grievance redressal
  - Right to nominate a person to exercise rights (after death/incapacity)
- GDPR
  - Right to access
  - Right to rectification
  - Right to erasure (“Right to be forgotten”)
  - Right to restrict processing
  - Right to data portability
  - Right to object to profiling

DPDP vs. GDPR: Fiduciary responsibilities

In DPDP Act, Data fiduciaries must:

- Maintain accuracy
- Implement safeguards
- Notify breaches

- Significant data fiduciaries (large orgs) must appoint data protection officer, ensure audits
- Allows government to bypass

- Under GDPR, Data controllers & processors must ensure:
  - Data minimization
  - Security safeguards
  - Appoint Data Protection Officer (DPO)
  - Report breaches (within 72 hours)

DPDP vs. GDPR: Enforcement

- Data Protection Board of India (DPBI)
- Penalties: up to ₹250 crore per violation
- No criminal liability (unlike earlier drafts)

- EU is a bunch of states
- Independent Data Protection Authorities in each EU country
- Heavy penalties: up to 4% of global annual turnover

In general:
- GDPR is seen as too stringent, getting in the way of doing anything
- DPDP Act is seen as too narrow, ambiguous about government/overseas processing

In-class activity: Help save our digital SRS please!

- In IIT Kanpur, we conduct the student reaction survey for courses.
- Until a few years back, we used paper-based SRS (anonymous OCR sheets).
  - Problem: Processing a pain as we grow
- Administration decided to make SRS digital (sensible!)
  - New portal: Students login → select course you are registered for → provide feedback
  - Teachers will only get aggregated scores and any specific feedback the students provides.
- Students say: we don't trust, this is sensitive data & can hurt our grades
- Teachers & students → go back to stone age and do OCR sheets
  - Teachers: "We want feedback, don't care how!"
  - Students: "We will give anonymous feedback only on paper, we don't trust tech!"

Help solve this problem for our DoAA team!

- Work in pairs to come up with a plan for processing (gathering, storing, analyzing) SRS, with DPDP Act as the guide
- Think in terms of:
  - Personal, personally-identifiable & sensitive data
  - Principal rights, fiduciary responsibilities & purpose limitation
  - Privacy is a fundamental right & constitution protects this right!
- Do not dumb down the system, unless absolutely needed
  E.g., Don't say no login and instead put in course ID and then fill feedback and then we end up with duplicates, mischief, inconsistencies, etc.
- Turn in sheets at the end of the class
- Will try and take the good ones to the institute!
- You may even write a Vox Populi article on the same, and do us all a favor ☺