AAAI-23 Bridge: AI & Law

Breakout 4: Privacy

Paul Ohm
Professor of Law

GEORGETOWN UNIVERSITY

Agenda

1. “Privacy” means…
2. Privacy Law
3. The data used to power ML and AI
4. Using ML/AI to attack privacy
5. Using ML/AI to defend privacy
6. New privacy rights and remedies
7. Friction

“Privacy” means…

- Right to be let alone
- Right to control information about oneself
- Personhood and autonomy
- Intimacy
- Personal growth
- Contextual integrity

“Privacy” means…

- Right to be let alone
- Right to control information about oneself
- Personhood and autonomy
- Intimacy
- Personal growth
- Contextual integrity

Definition 2.4 (Differential Privacy). A randomized algorithm $\mathcal{M}$ with domain $\mathbb{N}^{|\mathcal{X}|}$ is (ε, δ)-differentially private if for all $\mathcal{S} \subseteq \text{Range}(\mathcal{M})$ and for all $x, y \in \mathbb{N}^{|\mathcal{X}|}$ such that $\|x - y\|_1 \leq 1$:

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] \leq \exp(\varepsilon) \Pr[\mathcal{M}(y) \in \mathcal{S}] + \delta,$$

Privacy Law

- Data Protection law (GDPR, CCPA, CPA)
- Consumer protection approach (FTC Act)
  - Unfairness
  - Deception
- Newer proposals
  - Duties of fairness or loyalty
  - Data transparency or disclosure
  - Data governance rules (CPOs, PIAs, privacy-by-design, audits)
  - Ground rules for data collection and sharing

The Data Used to Power ML and AI

- Surveillance and Information capitalism
- Data minimization and privacy-by-design
- Less data for training generally

Using ML/AI to Attack Privacy

- Inferences and sensitive information
  - Gaydar, Target
  - Dobbs
  - Facial recognition
- Legal developments:
  - Colorado Privacy Act
  - Jones and Carpenter

Colorado Privacy Act Rules

"Sensitive Data Inference" or "Sensitive Data Inferences" means inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status.

Controllers must obtain Consent to Process Sensitive Data, including Sensitive Data Inferences . . . .

Using ML/AI to Defend Privacy

- Differential privacy
- Federated learning
- AI auditors

New Privacy Rights and Remedies

- Right to delete / right to be forgotten
  - Machine unlearning
- Legitimate interests and secondary purposes
- Model/AI disgorgement

Friction

- Paul Ohm and Jonathan Frankle, *Desirable Inefficiency*, 32 Florida Law Review 357 (2018).
- Brett Frischmann & Susan Benesch, Friction-In-Design Regulation as 21St Century Time, Place, Manner (forthcoming 2023).
- Paul Ohm & Brett Frischmann, *Governance Seams* (forthcoming 2023).
- Ellen Goodman, *Digital Fidelity and Friction*, 21 Nev. L.J. 623 (2021).

The Takeaway:

Study something other than human behavior!!!

Discussion