Privacy

Philosophy, Law, and Technology

ML for Cybersecurity

November 19, 2020

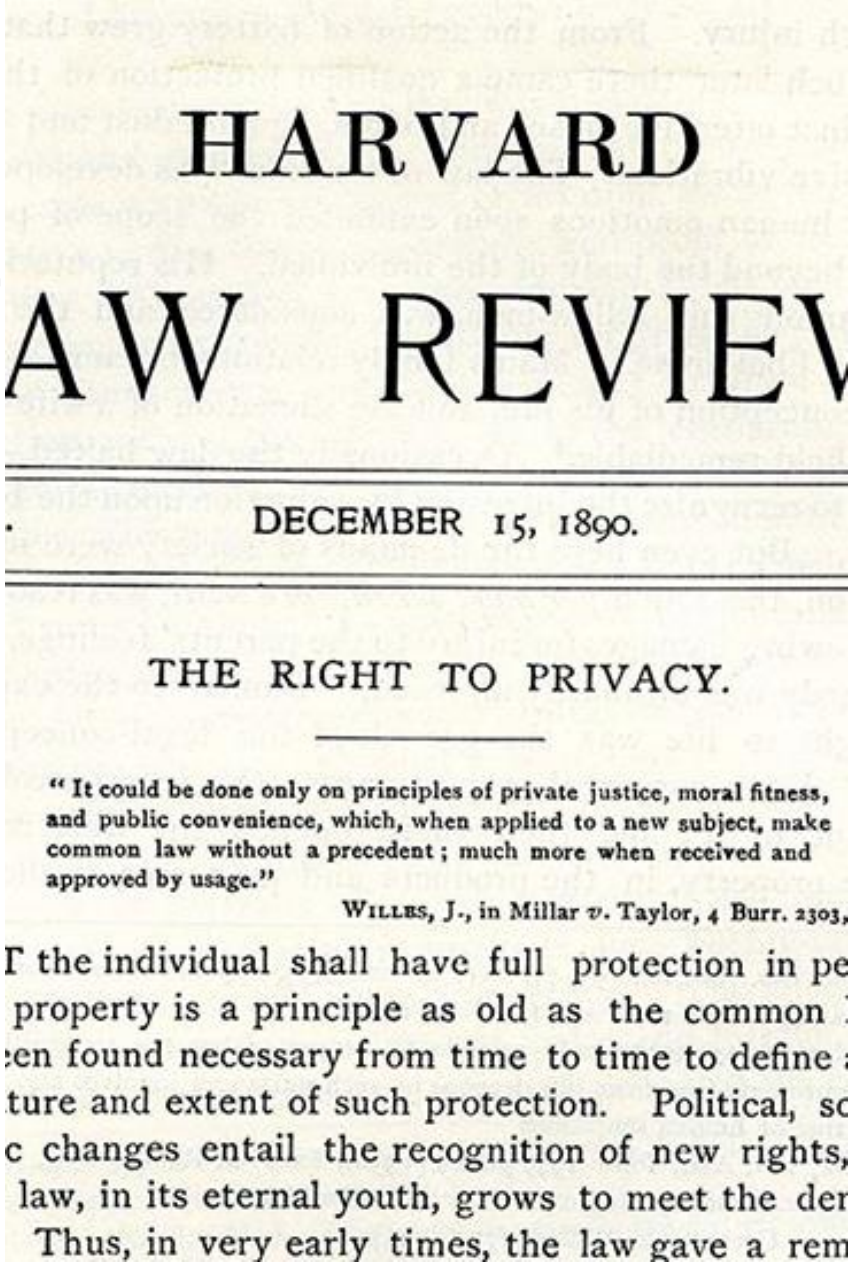
Privacy is Hard to Define

- *"Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."* Robert C. Post, Three Concepts of Privacy, 89 Geo. L.J. 2087 (2001)

DEFINING PRIVACY

The Right to Be Let Alone

- Warren and Brandeis, Harvard Law Review, **1890**
- Spurred by photography in gossip pages about high society
- Libel and slander are insufficient in considering only damage to reputation
  - The right to prevent, rather than profit from, publication
- Excludes topics of general interest



HARVARD

AW REVIEW

DECEMBER 15, 1890.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303,

Γ the individual shall have full protection in pe
property is a principle as old as the common
en found necessary from time to time to define
ture and extent of such protection. Political, so
c changes entail the recognition of new rights,
law, in its eternal youth, grows to meet the de
Thus, in very early times, the law gave a rem

Privacy as Control

- Alan Westin, Privacy and Freedom, **1967**
- “Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”
- “…each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication….”

Boundary Regulation

- Irwin Altman, **1975**
- Privacy is a dialectic and dynamic process of boundary regulation
- Continuous movement on a continuum
- Goal: optimize balance of privacy and social interaction

Balance Costs and Benefits

- Sandra Petronio, **1991**
- Communication Privacy Management (CPM) Theory
- Regulate boundaries based on perceived costs and benefits
- Rule-based management is expected
- Boundary turbulence related to clashing expectations

Contextual Integrity

- Helen Nissenbaum, **2004**
- “Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context.”
- Parameters: data subject, sender, recipient, information type, and transmission principle

PRIVACY REGULATION & LAW

Fair Information Practice Principles (FIPPs)

- US Federal Trade Commission (FTC), building on earlier frameworks

1. Notice / Awareness
2. Choice / Consent
3. Access / Participation
4. Integrity / Security
5. Enforcement / Redress

FTC's Regulatory Tools

- **Unfair practices**
  - Injure consumer
  - Violate established policy
  - Unethical
- **Deceptive practices**
  - Mislead consumer
  - Differ from reasonable consumer expectations

General Data Protection Regulation (GDPR)

- Came into effect May 25, 2018 and applies to the EU
- Distinguishes between data subjects, controllers (people who direct analysis), and processors (those who do the analysis)
- Controller informs the “data subject in a concise, transparent, intelligible and easily accessible form”
- Right of access for data subjects
- Right of erasure (with some exceptions)
- Right to object to processing for some purposes
- Privacy by design (Article 25)

General Data Protection Regulation (GDPR)

- Pseudonymization required for stored personal data
- Data breach notification to authorities within 72 hours
- Possible fines of up to 4% of worldwide turnover
- Can only process data based on six lawful bases:
  1. Consent
  2. Contract
  3. Public task
  4. Vital interest
  5. Legitimate interest
  6. Legal requirement

California Consumer Privacy Act (CCPA)

- Came into effect January 1, 2020 and applies to California residents
- Residents of California have rights to:
  - Know what personal data is collected
  - Know whether that data is sold
  - Refuse the sale of personal data
  - Access their data
  - Request erasure of their personal data
  - Not be discriminated against for exercising these privacy rights
- Fine of $7,500 for intentional and $2,500 for unintentional violations