Regulating Privacy

How is Privacy Regulated?

- The General Data Protection Regulation (GDPR)
- The US
  - The Federal Trade Commission
  - The Federal government
  - Sector-specific (and state) regulations

GDPR

- An EU regulation, binding on member countries
  - Succeeds two earlier “directives”
- Strict privacy rules
- Enforced by government Data Protection Authorities
- Based on a design from a US Dept. of HEW advisory committee report in 1973: the FIPPs (Fair Information Practice Principles)

Personal RIghts Under the FIPPs in the GDPR

- Access to data
- Accountability: companies must document how they comply
- Data processing only with consent, lawful obligation, or other valid reasons
- Transparency about data handling
- Security
- The right to be forgotten—we'll discuss more on this in a few weeks

The Federal Trade Commission

- With one exception, data about children, the FTC has no explicit statutory authority about privacy
  - In 1995, though, Congress urged it to get involved in privacy
  - It does not issue regulations
- The FTC can act against “unfair or deceptive trade practices” that cause “harm”
- What does that mean?

The FTC and Privacy Policies

- If a company violates its own privacy policies, that's obviously deceptive
- But—there's no requirement for a protective privacy policy
- And: what is "harm"?

The FTC and Security Breaches (or Issues)

- If a company skimps on security measures, that might be unfair competition
- If a company skimped on security measures *and* promised to keep your data secure, that's deceptive
  - But: what is the norm for security measures?
  - Most companies don't fight the FTC on this; Wyndham Hotels and LabMD did
- And again—what is "harm"?

What is “Harm”?

- Unclear!
- Often established by case law
- Easy case: financial loss to consumers
- Almost as easy: leaked health information
- Hard: other disclosure of personal data
- (Brand-new draft: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222)

The Federal Government and Privacy

- In 1974 (and partly because of Watergate), the Privacy Act of 1974 was passed, make those law—but only for the Federal government
- Main impact today: any government agency that keeps a “system of records” must create and publish “privacy impact assessments” (PIAs)
- But: lots of data collection is mandated by statute

Sector-Specific Privacy Laws (and States)

- The US has many sector-specific privacy laws
  - FERPA, for educational data
  - FCRA, for credit reports
  - HIPAA, for health data
  - Etc.
- They’re all different…
- And: some states are enacting their own, strict privacy laws
- Major issue for a possible comprehensive Federal law: should state laws be preempted?

CS@CU

Daily Bird 2.0

Great blue heron on the ice in Morningside Park, December 24, 2019

CS@CU