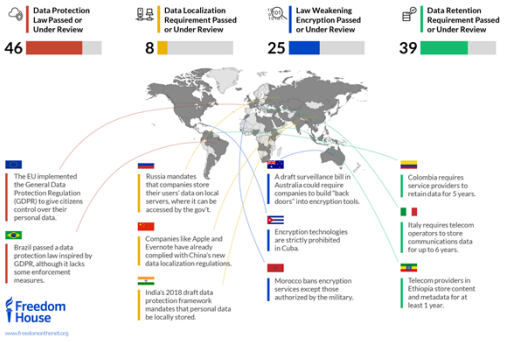
Moral and Legal Foundations of Privacy

April 25, 2023

V. International Privacy

Where your Privacy Is (and Isn't) Protected



Movius - U.S. and EU Privacy Policy: Comparison of Regulatory Approaches

EU/US Privacy Comparison

- Vastly different approaches in the US and EU.
- Due to differences in values and social norms.
- European approach:
  - Close participation between business and government to serve the public good.
  - Government is a partner to business.
- American approach:
  - Emphasizes the role of private actors and market forces.

EU/US Privacy Comparison

- Data privacy heavily regulated in Europe.
- Europeans look at privacy as a fundamental human right.
- In the U.S., the Constitution does not use the word "privacy" and does not guarantee a right to privacy.
- Privacy is "a commodity subject to the market and is cast in economic terms."
  - Patriot Act after 9/11
  - Foreign Intelligence Surveillance Court (FISC)

1995 EU Directive on Privacy

- Deals with processing of personal data:
  - "Personal data":
    - "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2a)
  - Very broad. Personal data when someone is able to connect the information to a person. *E.g.*: address, credit card number, bank statements, criminal record, etc.

1995 EU Directive on Privacy

- "Processing":
  - "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;" (art. 2 b)
- The data "controller" must comply whether or not it is established in the EU or uses equipment in the EU to process data

1995 EU Directive on Privacy

- 1995 Directive was written before the Internet became widespread (and long before Facebook, Google, and others changed the way we interact with each other online).
- There was little authority on the scope of the 1995 directive, and whether it applied to online businesses that solicited EU customers or not.
  - *i.e.*, was the EU customer's computer or phone "equipment situated with in the EU in order to process data" done by the "controller"?

GDPR Data Protection Reform

2018 EU General Data Protection Regulation (GDPR)

- 2015 data protection regulations that went into effect May 25, 2018.
- Much tougher than previous regulations:
  - Allow national watchdogs to issue fines upward of $100s of millions.
  - Includes right to be forgotten (to be discussed later).
  - Companies must inform national regulators within 3 days of a data breach.
  - Anyone under 16 must obtain parental consent before using Facebook, etc. (but can be lowered to 13).

2018 EU General Data Protection Regulation (GDPR)

- Explicitly applies to any company that operates in EU, even if based elsewhere.
- National authorities given great leeway to implement the rules.
- Facebook has already had issues in the past with national privacy watchdogs. This is sure to increase the number of issues in the future.

2018 EU General Data Protection Regulation (GDPR)

- Transparency: must inform person when data is being processed
- Data may be processed only:
  - With consent;
  - Necessary for entering or performance of contract;
  - Necessary for compliance with legal obligation;
  - Necessary to protect vital interests of the person;
  - Necessary for public interest of official duty; or
  - Necessary for legitimate interests of controller of info. or disclosed third parties, EXCEPT where overridden by fundamental rights and freedoms of person.
- Person can request deletion or correction of data.

2018 EU General Data Protection Regulation (GDPR)

- A "controller" can only process personal data for specified legitimate purposes.
  - Must also be proportionate processing, accurately maintained/updated, and kept only for a reasonable time.
- A person may object to use for direct marketing.
- There may be even higher standards for very personal information.
- Can only transfer outside the EU if the country has adequate protections.
  - The 2016 EU-US Privacy Shield has been determined adequate for EU-US transfers.

EU-US Privacy Shield

EU/US Privacy Shield (2016)

- 2016 Agreement between EU and US that provides a legal mechanism to transfer personal data from the EU to the US and still "protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses."
- Stronger obligation on US companies to protect the personal data of Europeans.
- Stronger monitoring and enforcement by US Federal Trade Commission (FTC).

EU/US Privacy Shield (2016)

- Improvement over older Safe Harbor framework that the EU Court of Justice found to be invalid in October 2015.
- Requires that complaints be resolved by companies within 45 days and allows for Alternative Dispute Resolution if no resolution.
- Joint review by EU and US every year.
- US companies must register and self-certify.
- Over 5,000 U.S. companies rely on this framework to process and transfer EU data.

~~EU-US Privacy Shield~~

The *Schrems II* Case Invalidates the Privacy Shield

The *Schrems II* Case (2020)

- In July 2020, the Court of Justice of the European Union (CJEU) declared the EU-US Privacy Shield invalid.
- Case stems from a complaint by Max Schrems, an Austrian citizen, who had been a Facebook user since 2008.
- He claimed that Facebook Ireland's transfer of his personal data to the US violated his privacy rights because US law did not provide sufficient legal protections.

The *Schrems II* Case (2020)

- Mr. Schrems is actually the person who led to the 2016 revision to the EU-US Privacy Shield (the *Schrems I* case).
- After that 2016 revision, Mr. Schrems claimed that his privacy rights were still being violated, and that US law still did not provide sufficient protections.
- The CJEU agreed that the US does not provide for an "essentially equivalent, and therefor sufficient, level of protection" guaranteed by EU law (such as GDPR)

The *Schrems II* Case (2020)

- As a result, “EU companies can no longer transfer data to the US based on the Privacy Shield framework,” else risk a penalty of €20 million
- There are ways around this, but they are extremely complicated and may be ineffective.

Google Spain v. Gonzalez

The Right To Be Forgotten

Google Spain v. Gonzalez

- Google search results for Mr. Gonzalez (a Spanish lawyer) returned a 1998 auction notice of his repossessed home in a Spanish newspaper.
- Gonzalez was embarrassed and requested that the newspaper remove all reference to him from their website.
- He argued that the debt had been resolved years ago and was no longer relevant to his search results.
- Gonzalez also asked Google to remove his personal data.
- Neither did, so he sued in the Spanish courts.

Google Spain v. Gonzalez

- The Spanish court found that individuals have a “right to be forgotten.”
- This is a right to ask search engines to remove links with personal information about them if the information is:
  - Inaccurate;
  - Inadequate;
  - Irrelevant; or
  - Excessive.

The Right To Be Forgotten

- Google now blocks access to certain links in its search results in Europe.
- Google also set up a procedure where individuals can request removal of a link.
- April 2021: Google states it has received nearly 1.1 million requests to remove a total of 4.1 million links, removing about 47% of them.
- News sites are exempt from the rule.
- GDPR codifies the right and adds requirements.

The Right To Be Forgotten

- The right is limited to the EU, though.
- France's privacy regulator (CNIL) required Google to remove links worldwide, not just in the EU.
- Since the original decision in Google Spain v. Gonzalez never defined how, when, and where Google had to remove links, Google challenged CNIL's decision.
- The EU court ruled in Google's favor and confirmed that CNIL can compel Google to remove links in the EU, but cannot do so worldwide.

Basu – Key Takeaways from India's Data Protection Bill

New Privacy Laws Proposed in India

Privacy Law in India

- India introduced its Personal Data Protection Bill in Parliament on December 11, 2019, and it appears ready to be passed into law sometime in 2020.
- This Bill arises from a 2017 landmark case in India, *K.S. Puttaswamy vs. Union of India*, where the Supreme Court of India affirmed the right to privacy as a fundamental right of the people.

Privacy Law in India

- The Bill has three stated motivations:
  - "[T]he right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of information privacy."
  - "[T]he growth of the digital economy has expanded the use of data as a critical means of communications between persons."
  - "[I]t is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion."

Privacy Law in India

- The Bill contains a number of the same consent-related provisions as EU's GDPR.
  - To collect personal data, "data fiduciaries" must obtain consent from the individuals whose data is at issue.
  - "Data fiduciaries" is broadly defined to cover pretty much any business or person that deals in individual data.
- Includes protections for data belonging to children.
- Individuals can request information from data fiduciaries about information being collected on them and have a right to correct or erase the data: a "right to be forgotten."

Privacy Law in India

- Some data can only be processed or stored in India:
  - "Critical personal data" must be stored and processed only in India.
  - "Sensitive personal information" must be stored within India but can be copied elsewhere in certain circumstances.

Privacy Law in India

- There are concerns that it grants the government too many exemptions for data collection.
- The government can collect data if it is "necessary or expedient" in the "interests of sovereignty and integrity of India, national security, friendly relations with foreign states, or public order."
- This is very broad and does not provide clear rules with which the government must comply.

Wenyan – China Is Waking Up to Data Protection and Privacy

Lee – China's Draft Privacy Law in the International Context

New Privacy Laws Proposed in China

Wenyan - Privacy Law in China

- "2018-2019 could be viewed as the time when the Chinese public woke up to privacy."
  - Article provides examples of public outcry against the Zao app (a face-swap app like Russian FaceApp), comments by Robin Li, founder of Baidu, and Alibaba.
- The China's National People's Congress (NPC) was in the process of drafting China's personal data protection law that "will lead to a comprehensive framework for individual data rights and protection."
- This framework is similar to GDPR in many ways, but is more explicitly tied to national security and social stability goals.

Wenyan - Privacy Law in China

- While the law is under discussion, the Cyberspace Administration of China (CAC) the country's highest administrative Internet regulator, issued a Data Protection Regulatory Guideline in June 2019.
- The Guideline lays out rules regarding how internet companies can and cannot collect and use customer data.
- For example, the Guideline focuses on how users can control their data in mobile apps.

Wenyan - Privacy Law in China

- The Guideline prohibits the following mobile app practices as illegal or excessive:
  - No publicly available user data rules.
  - No explicit statement of the purpose, method, or scope of collecting user information.
  - Information collection without consent.
  - Collecting personal information unrelated to the service provided.
  - Failure to delete or correct personal information as required by law.
  - Bundling the main service with extended functions to force the user to provide personal data for all services.

Lee - Privacy Law in China

- In October 2020 the NPC released its draft of the long-awaited Personal Information Protection Law (PIPL)
- The PIPL "represents a third way" of data privacy protection, the other two being the "U.S. approach, which applies different rules for specific industries or classes of consumers," and the E.U. approach, "which enshrines fundamental rights across contexts."

Lee - Privacy Law in China

- PIPL "emphasizes consumer privacy while also prioritizing national security through data localization measures, cross-border data flow restrictions, and continued surveillance and law enforcement powers."
- PIPL "shows similarities with the GDPR" when it comes to reach outside China's borders.
  - PIPL applies "to personal information processing outside China to provide products or services to Chinese citizens or to analyze and evaluate the behavior of Chinese citizens."

Lee - Privacy Law in China

- BUT: PIPL differs from GDPR most significantly as related to national security.
  - GDPR "promotes the free flow of data across borders, providing several legal transfer mechanisms."
  - PIPL, on the other hand, requires the Cyberspace Administration of China (CAC) to provide security assessments before many different categories of people or companies can transfer personal data abroad.
  - PIPL also requires that information processed by the state be stored in China.
- If an overseas company is found to violate China's national security or public interests, it can be put on a blacklist and prohibited from processing Chinese personal data.

Lee - Privacy Law in China

- Further unlike GDPR, PIPL "lacks clear measures and boundaries to protect citizens privacy when national security or the public interest are invoked" by the state.
- Like with GDPR, every major corporation in the world will need to adopt a PIPL compliance strategy.
- But, at least as drafted, PIPL compliance would not be easy.
  - Some of the terms are overlapping and confusing.
  - The draft sends mixed signals related to "consent."

Final Exam Discussion