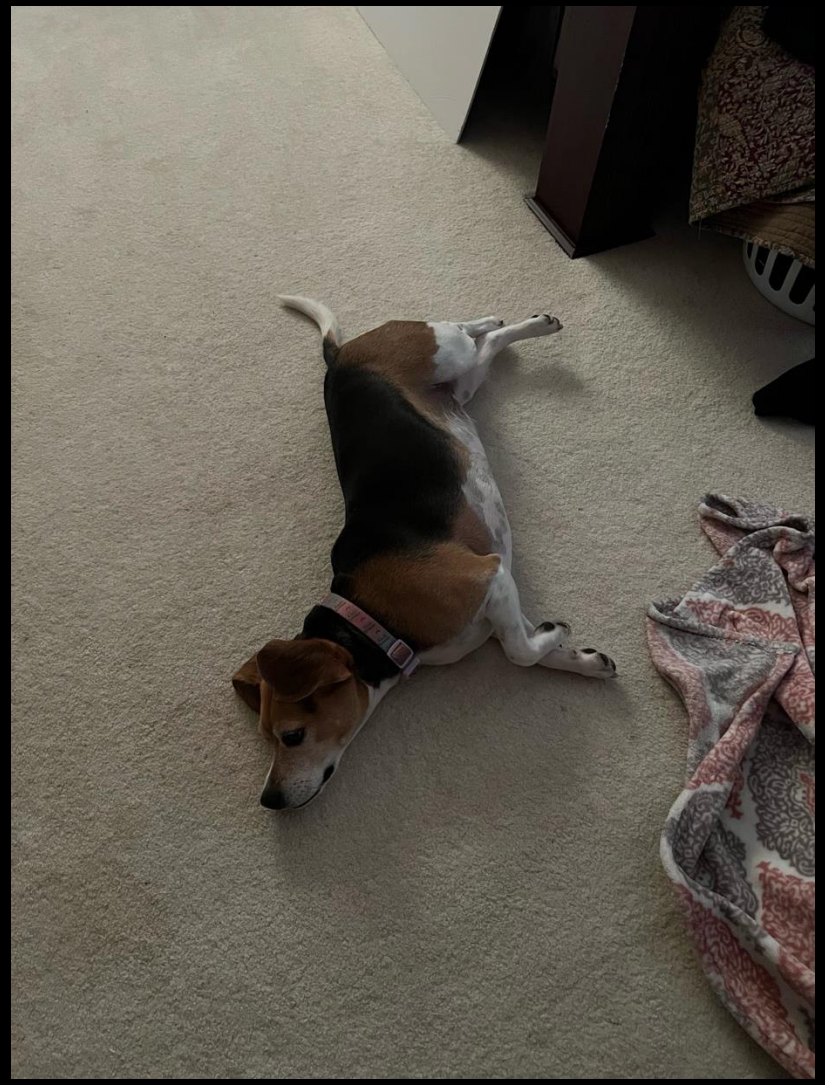
DS 593: Privacy in Practice

Privacy, Law, and Regulation

Instructor: Alishah Chator

News?



Executive Order to the State Department Sideswipes Freedom Tools, Threatens Censorship Resistance, Privacy, and Anonymity of Millions

BY **CORYNNE MCSHERRY** AND **CINDY COHN** | JANUARY 30, 2025

There are many examples of freedom technologies, but here are a few that should be readily understandable to EFF's audience: First, the Tor Project, which helps ensure that people can navigate the internet securely and privately and without fear of being tracked, both protecting themselves and avoiding censorship. Second, the Guardian Project, which creates privacy tools, open-source software libraries, and customized software solutions that can be used by individuals and groups around the world to protect personal data from unjust intrusion, interception and monitoring. Third, the Open Observatory of Network Interference, or OONI, has been carefully measuring government internet censorship in countries around the world since 2012. Fourth, the *Save* App from OpenArchive, is a mobile app designed to help people securely archive, verify, and encrypt their mobile media and preserve it on the Internet Archive and decentralized web storage.

https://www.eff.org/deeplinks/2025/01/executive-order-state-department-sideswipes-freedom-tools-threatens-censorship

Last time

- Privacy as a civil right

Today

- Some more legal background on privacy
- Privacy and Regulation

Important Principles from last class

- Reasonable Expectation of Privacy
- Third-Party Doctrine
- Mosaic Theory

Florida v Riley

- **Background**: Sheriff office received tip that Riley was allegedly growing marijuana on his property. Officers were unable to see inside a greenhouse while investigating the tip. They decided to use a helicopter to circle over the property and from this aerial vantage point were able to see what looked like marijuana growing inside.

- Does this constitute a search protected under 4A?

US v Miller

- **Background**: Upon suspecting a warehouse leaser of running an undocumented whiskey distillery, investigators had local banks provide Miller's bank records without a warrant or notifying Miller. With the evidence these records provided, Miller was arrested.

- Does this constitute a search protected under 4A?

Riley v California

- Background: Riley was pulled over for having expired registration tags. Policy was that in this case the car is impounded and a inventory search is conducted. Two hidden handguns were found and Riley was placed under arrest. During this, officers performed a warrantless search of his phone, and information they found was used to charge Riley in connection to a gang shooting. As per *Diaz*, officers are entitled to perform a search of an individual's clothes during an arrest.

- Does this constitute a search protected by the 4A?

Can you be compelled to unlock a phone?

Can you be compelled to unlock a phone?

- It depends

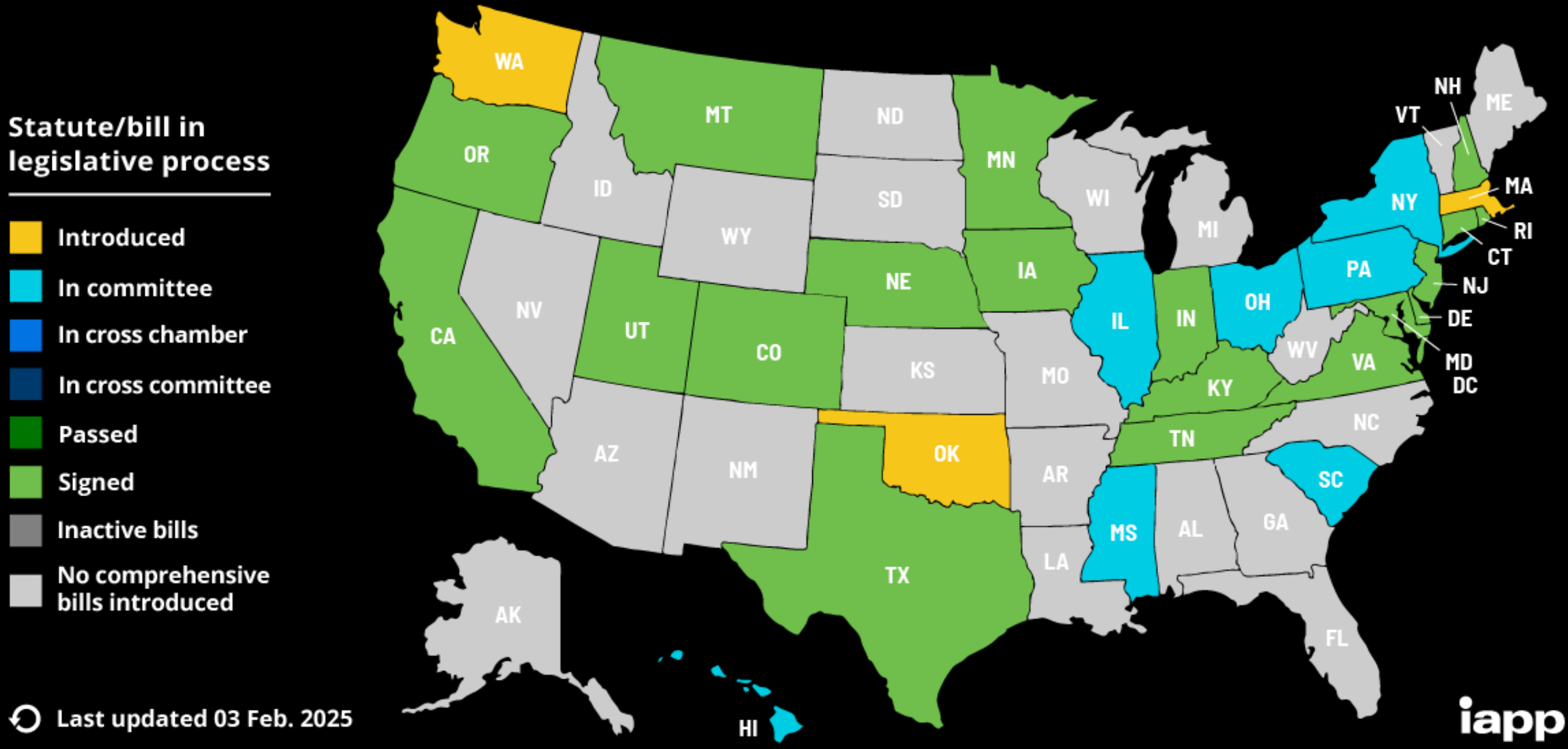
Can you be compelled to unlock a phone?

- It depends
- 5A protects against compelled self incrimination

Can you be compelled to unlock a phone?

- It depends
- 5A protects against compelled self incrimination
- Three caveats:
  - Only protects testimony (“something you know”)
  - “Foregone conclusion” exception
  - Border Exception

US State Privacy Legislation Tracker 2025



Open Legal Questions

- *Burrows v. Supreme Court*: REP for bank records under California Constitution
- *US v Warshak*: Appeals court ruling that there is REP for email
- *Maryland v Andrews*: Lower court ruling that stingrays violate REP
- *Alasaad v Duke*: Is there a REP at the border?
- Judge Stephen Smith ruling: Are NITs permissible?

What does this look like in terms of Regulation?

What does this look like in terms of Regulation?

- Governing how data is used in practice vs where privacy rights are derived from

- What should be the goals of regulation?
  - Who is being regulated?
  - What exactly is being regulated?
  - What does enforcement look like?

Principles of Privacy Regulation

- Data Minimization
- Purpose limitation
- Consent and User Rights
- Transparency and Accountability

Types of Regulations

- Most regulations fall under a few categories:
  - Medical Privacy
  - Financial Privacy
  - Consumer Data Privacy

The Federal Trade Commission (FTC)

- One of the most important regulatory agencies in the US
- Established in 1914 by the Federal Trade Commission Act
- Focused on antitrust and consumer protection
- Section 5 of the FTC Act is used to require companies to safeguard personally identifiable information (PII)
- Enforcement is through fining violators

FTC Impact

- Drove adoption of privacy policies by companies
- Primarily focuses on “broken promises”
- Requires certain types of disclosure to be included in policies

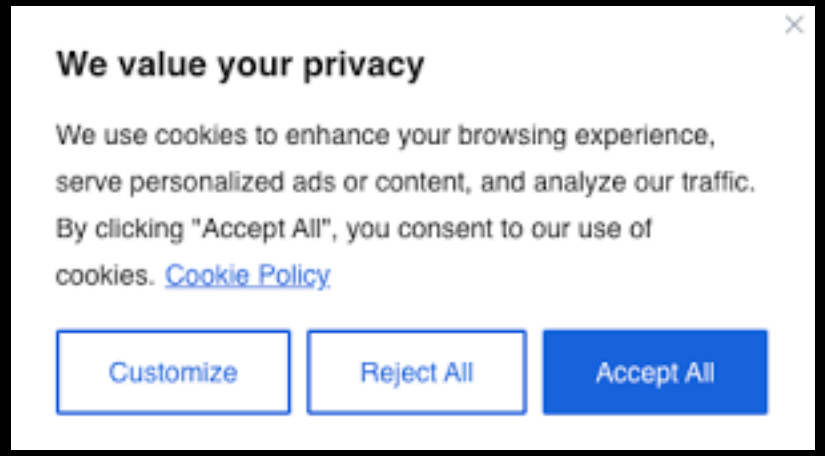
Privacy Act of 1974

- Codified the Fair Information Practice Principles (FIPP) for the federal government regarding its storage and use of PII
- Intended to mitigate fears about federal agencies compiling large databases of records
- Requires consent except in cases of a routine, investigative, archival, administrative purpose

Important US Data Privacy Laws

- Family Educational Rights and Privacy Act
- Children’s Online Privacy Protection Act
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act
- Fair Credit Reporting Act
- Video Privacy Protection Act
- Electronic Communications Privacy Act
- Stored Communications Act

GDPR


We value your privacy
We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies. Cookie Policy
Customize
Reject All
Accept All

GDPR

- The General Data Protection Regulation (GDPR) is an important component of EU privacy law that was implemented in 2016
- One of the most impactful privacy regulations alongside the CCPA
- Core Principles:
  - Lawful processing of data
  - Purpose Limitation
  - Data Minimization
  - Accuracy
  - Storage Limitation
  - Integrity and Confidentiality

GDPR – Lawful Processing of Data

- According to Article 6, lawful purposes for data processing are:
  - Data subject has given consent
  - To fulfil contractual obligations
  - To comply with legal obligations
  - To protect vital interests of the data subject
  - To perform a task in the public interest
  - For legitimate interests of the data controller as long as those are overridden by the interests of the data subject

GDPR Rights of the Data Subject

- Transparency
- Accessing of data and information about how it is processed
  - Portability of data
- Erasure
- Right to Opt-out
- Right to compensation

Problem Solved?

A Large-Scale Study of Cookie Banner Interaction Tools and Their Impact on Users' Privacy

Nurullah Demir
Institute for Internet Security
KASTEL Security Research Labs
Karlsruhe Institute of Technology

Tobias Urban
Institute for Internet Security
secunet Security Networks AG

Norbert Pohlmann
Institute for Internet Security

Christian Wressnegger
KASTEL Security Research Labs
Karlsruhe Institute of Technology

A Study on Subject Data Access in Online Advertising After the GDPR

Tobias Urban[1,2(✉)], Dennis Tatang[2], Martin Degeling[2], Thorsten Holz[2], and Norbert Pohlmann[1]

Maggie Van Nortwick and Christo Wilson

Setting the Bar Low: Are Websites Complying With the Minimum Requirements of the CCPA?

An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites

Hana Habib, Yixin Zou†, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, Florian Schaub†
Carnegie Mellon University & †University of Michigan
{htq, ajannu, nksridha, cswoopes, acquisti, lorrie, ns1}@andrew.cmu.edu
{yixinz, fschaub}@umich.edu

GDPR Reality Check – Claiming and Investigating Personally Identifiable Data from Companies

Fatemeh Alizadeh, *University of Siegen*
Timo Jakobi, *University of Siegen*
Alexander Boden, *Fraunhofer Institute*
Gunnar Stevens, *University of Siegen*
Jens Boldt, *University of Siegen*

GDPR: When the Right to Access Personal Data Becomes a Threat

Luca Bufalieri, Massimo La Morgia, Alessandro Mei, Julinda Stefa
Department of Computer Science, Sapienza University of Rome, Italy

Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy?

Zengrui Liu
Texas A&M University
College Station, Texas, USA
lzr@tamu.edu

Umar Iqbal
Washington University in St. Louis
St. Louis, Missouri, USA
umar.iqbal@wustl.edu

Nitesh Saxena
Texas A&M University
College Station, Texas, USA
nsaxena@tamu.edu

Do Cookie Banners Respect my Choice?

Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework

Célestin Matte
Université Côte d'Azur, Inria
France
celestin.matte@inria.fr

Nataliia Bielova
Université Côte d'Azur, Inria
France
nataliia.bielova@inria.fr

Cristiana Santos
Research Centre for Justice and Governance
School of Law, University of Minho
cristianasantos@protonmail.com

Personal Information Leakage by Abusing the GDPR "Right of Access"

Mariano Di Martino[1], Pieter Robyns[1], Winnie Weyts[2], Peter Quax[1,3], Wim Lamotte[1], and Ken Andries[2,4]
[1] *Hasselt University/tUL, Expertise Centre for Digital Media*
[2] *Hasselt University - Law Faculty*
[3] *Flanders Make*
[4] *Attorney at the Brussels Bar*
{mariano.dimartino,pieter.robyns,peter.quax,wim.lamotte,ken.andries}@uhasselt.be
winnie.weyts@student.uhasselt.be

What exactly is PII?

NIST: *(1) Any information that can be used to distinguish or trace an individual's identity, such as a name, social security number, date and place of birth, mother's maiden name, or biometric records. (2) Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.*

GDPR: *Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

HIPAA

- Privacy rule applies to:

1. Names
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if…
3. Dates (other than year) directly related to an individual
4. Phone Numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

What exactly is PII?

- Potentially a lot of different things
- Context-sensitive
- Processing dependent
- What isn’t captured by this notion of PII?

Next time

- Understanding Privacy Harms