

Privacy Law 101

2022 Privacy & Technology Law Forum

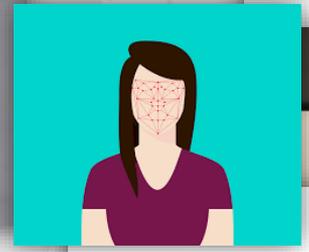
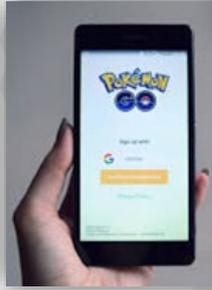
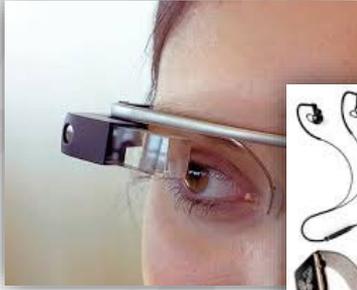
March 23, 2022

*Privacy & Technology Section of the State
Bar of Georgia*

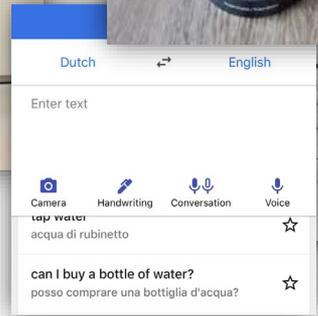
Amelia Vance
Founder and President
Public Interest Privacy Consulting
avance@pipc.tech
www.pipc.tech
[@ameliaivance](https://twitter.com/ameliaivance)



In the past decade...



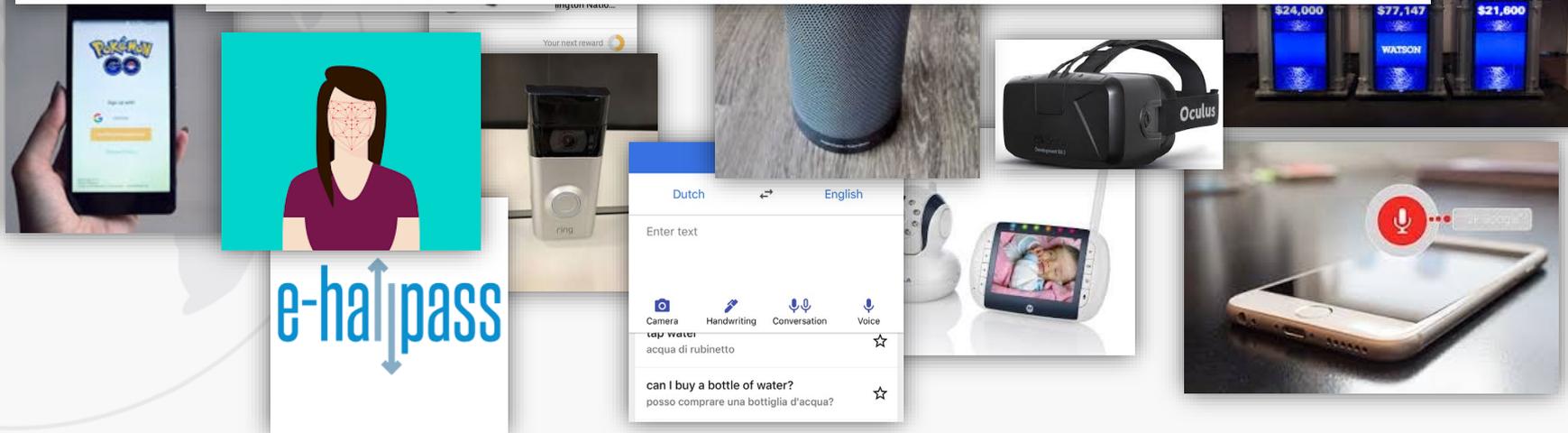
e-hai|pass



In the past decade...



This is the decade that computers became the boss of you.



e-hai|pass

Data in our day - to - day lives



Wake Up

Information we collect

“Geolocation data. Physical location or movements. Sensory data. Audio, electronic, visual, or similar information. Commercial information. Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies”

Apalon Alarm Clock Privacy Policy

https://www.apalon.com/privacy_policy.html



Attend a work meeting

How we use personal data

“We manually review short snippets of a small sampling of voice data we have taken steps to de-identify to improve our speech services such as recognition and translation.”

Microsoft (Teams) Privacy Policy

<https://privacy.microsoft.com/en-gb/privacystatement>



Go for a run

Information you provide us

“To help improve your experience or enable certain features of the Services, you may choose to provide us with additional information, like your logs for food, weight, sleep, water, or female health tracking; an alarm; and messages on discussion boards or to your friends on the Services.”

FitBit Privacy Policy

<https://www.fitbit.com/global/us/legal/privacy-policy>



Pay for your groceries online

We personalize your experience

“We can customize the organization of stories we present to you by considering our knowledge of your interests within the NYTimes: eg., what articles you have visited, which NYT newsletters you’re subscribed to, and which columnists you follow. We believe your reading history is a powerful indicator of stories and topics that are important to you.”

New York Times Personalization FAQ

<https://help.nytimes.com/en-us/articles/360003965994-Personalization>



Take a moment and meditate

Tracking technologies

“Our third party partners may use technologies such as cookies to gather data about your activities within the Products to deliver such advertising to you, such as retargeting ads. We are not always able to respond to do-not-track signals.”

Headspace privacy policy

<https://www.headspace.com/privacy-policy>



Read the news



How do we process personal data?

“We may also associate information that we learn about you through your and your contacts’ use of the Services, and information you and others provide, to suggest people you may know or may want to transact with through our Services.”

Paypal Privacy Policy

<https://www.paypal.com/webapps/mpp/ua/privacy-full>



Watch a funny video

The types of personal data we use

“We also collect information regarding your use of the Platform, e.g. how you engage with the Platform, including how often you use the Platform and how you interact with content we show you, the ads you view, videos you watch and problems encountered, the content you like, the content you save to “Favourites”, the words you search and the users you follow.”

TikTok Privacy Policy

<https://www.tiktok.com/legal/privacy-policy>

What does this mean for real people?



How an internet mapping glitch turned a random Kansas farm into a digital hell

 Kashmir Hill
4/10/16 10:00am • Filed to: REAL FUTURE ▾

Tech

FEB 16, 2012 @ 11:02 AM 3,368,630

The Little Black Book of Billionaire Secrets

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

 Netflix US @netflix Follow ▾

To the 53 people who've watched A Christmas Prince every day for the past 18 days: Who hurt you?

WHAT HAPPENS WHEN AN ALGORITHM CUTS YOUR HEALTH CARE

By Colin Lecher | @colinlecher | Mar 21, 2018, 9:00am EDT
Illustrations by William Joel; Photography by Amelia Holowaty Krates

Street Bump About



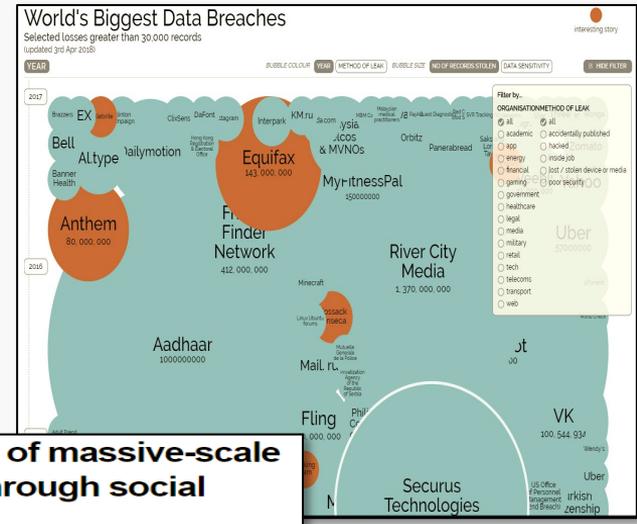
Help keep your streets smooth

RECORD A TRIP

MY TRIPS

The Intersect

You've probably never heard of this creepy genealogy site. But it knows a lot about you.



Experimental evidence of massive-scale emotional contagion through social networks

Adam D. I. Kramer, Jamie E. Guillory and Jeffrey T. Hancock
PNAS June 17, 2014. 111 (24) 8788-8790; published ahead of print June 2, 2014.
<https://doi.org/10.1073/pnas.1320040111>

 TIME

Orbitz Shows Higher Prices to Mac Users

By Martha C. White | June 26, 2012

Los Angeles Times

Dad gets OfficeMax mail addressed 'Daughter Killed in Car Crash'

January 19, 2014 | By Matt Pearce

So how did we get here?





Defining Privacy



Privacy is not one thing, but a cluster of many distinct yet related things. Privacy involves the control, use, and disclosure of personal information. It involves issues such as surveillance, online gossip, identity theft, data security, online behavioral advertising, Big Data, access to records, use of cloud computing services, and much more.

- Daniel Solove

Carnegie Mellon Privacy Illustrated



<http://cups.cs.cmu.edu/privacyillustrated/>

Being alone and creating private spaces

*Me hiding under the covers
in my bedroom*

- Age 5



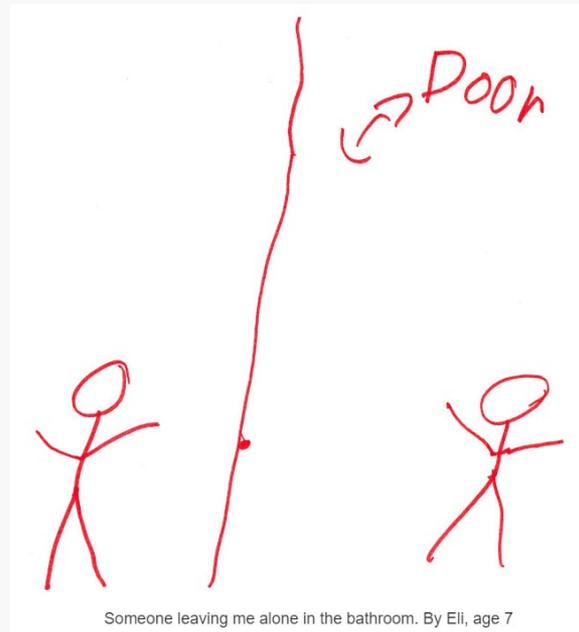
Me hiding under the covers in my bedroom. Age 5

<http://cups.cs.cmu.edu/privacyillustrated/>

Having space around you or between you and other people

*Someone leaving me alone
in the bathroom*

- Eli, age 7



Privacy from physical exposure

My sister knocking at my door when I'm changing

- Lucinda, age 8



<http://cups.cs.cmu.edu/privacyillustrated/>

Privacy of thoughts and ideas

If people could read your thoughts that would be creepy

- Elizabeth, age 11

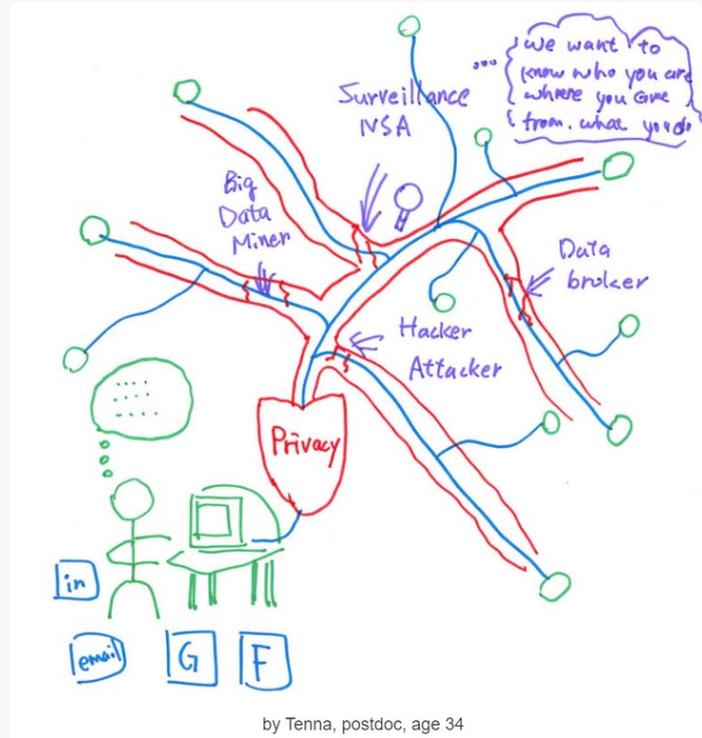


If people could read your thoughts that would be creepy, by Elizabeth, age 11

<http://cups.cs.cmu.edu/privacyillustrated/>



Surveillance

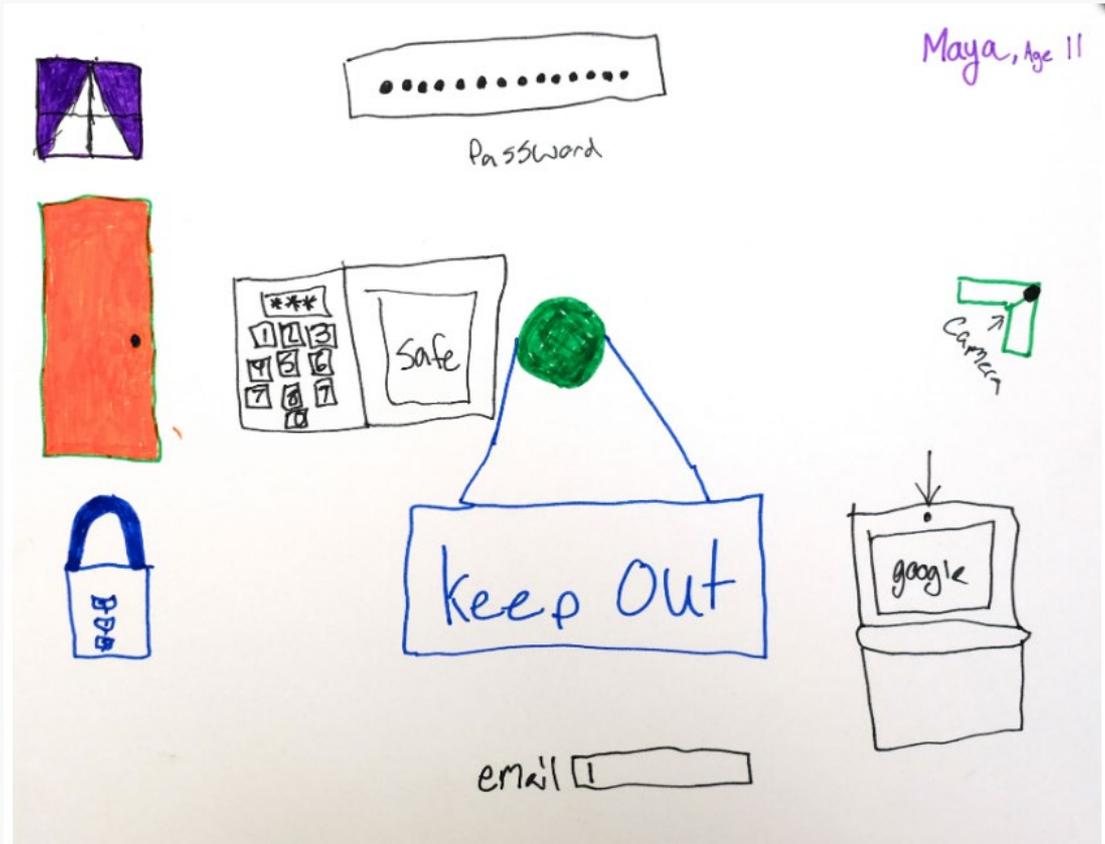


by Tenna, postdoc, age 34

<http://cups.cs.cmu.edu/privacyillustrated/>

Online privacy

Maya, age 11



<http://cups.cs.cmu.edu/privacyillustrated/>

What are the ways that others define privacy?

We can find various definitions or approaches to defining privacy in...

- Fundamental rights frameworks
- Laws and regulations
- Principles
- Social sciences
- Conceptual theories & scholarship
- Surveys
- Experiments
- Mathematics
- Technical standards
- (and more)



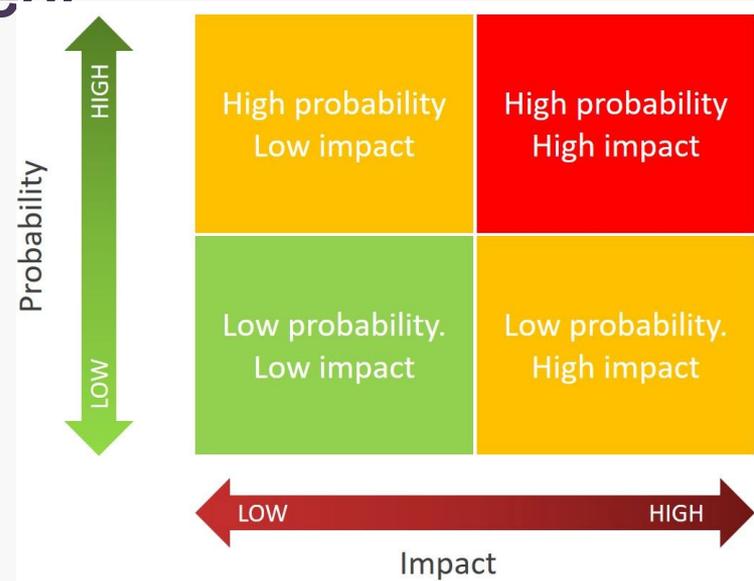
Privacy was once misconstrued as being about hiding and secrecy. Now it's understood to be something much more pressing: power dynamics between the individual, the state and the market. [Data protection] must seek to mitigate the inherent power imbalances between people —and those that collect, process and profit off their data.

- Frederike Kaltheuner

Privacy Risks Are Often Not Immediately Apparent

Privacy risks can be...

- Incremental
- Unequal
- Not obvious
- Intrusive





*Whether a particular problem is classified
as one of privacy is not as important as
whether it is recognized as a problem*

- Daniel Solove

Defining Privacy Through Harms



Harm	Description	
Physical Harms	Result in bodily injury or death	
Economic Harms	Monetary losses or a loss in the value of something	
Reputational Harms	Injuries to an individual's reputation and standing in the community (whether information is accurate or inaccurate)	
Psychological Harms	Emotional Distress	Includes a wide range of emotions, including annoyance, frustration, fear, embarrassment, anger, and various degrees of anxiety.
	Disturbance	Unwanted intrusions that disturb tranquility, interrupt activities, sap time, and otherwise serve as a nuisance.
Relationship Harms	Causing damage to important relationships—whether personal, professional, or organizational—that are important for one's health, well-being, life activities, and functioning in society because someone did not maintain the confidentiality of information they were given and therefore damaged trust.	

Defining Privacy Through Harms



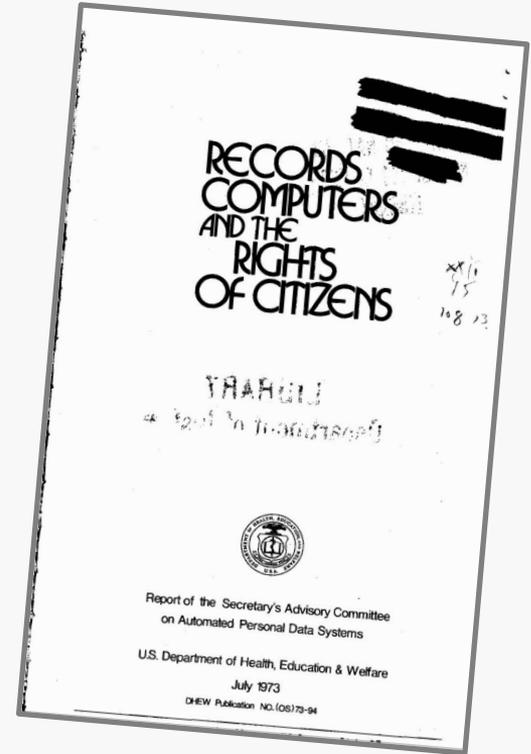
Harm	Description	
Autonomy Harms Restricting, undermining, inhibiting, or unduly influencing people's choices	Coercion	Impairment on people's freedom to act or choose
	Manipulation	Undue influence over people's behavior or decision-making
	Failure to Inform	Failure to provide people with sufficient information to make decisions
	Thwarted Expectations	Information collection, use, or sharing that undermines people's choices
	Lack of Control	Inability to make meaningful choices about one's data or prevent the potential future misuse of it
	Chilling Effects	Inhibiting people from engaging in lawful activities
Discrimination Harms	Entrenching inequality and disadvantaging people based on gender, race, national origin, sexual orientation, age, group membership, or other characteristics or affiliations. Can involve curtailment of autonomy, but also involves unequal treatment that creates shame and stigma and the societal consequence of further entrenching disadvantages.	

Defining Privacy

Not security or secrecy

Basic Principles

- Transparency
- Purpose Limitation
- Focused Collection
- Respect for Context
- Access and Control (including Deletion)
- Security
- Accountability





The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

- Fourth Amendment, U.S. Constitution

A faint background image showing silhouettes of several people walking on a globe. The globe is positioned in the lower-left quadrant, and the silhouettes are scattered across the top and middle of the frame, suggesting global movement and connectivity.

In order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies

- Privacy Act of 1974

Consumers need stronger laws to place them on a more equal footing when negotiating with businesses in order to protect their rights. Consumers should be entitled to a clear explanation of the uses of their personal information, including how it is used for advertising, and to control, correct, or delete it, including by allowing consumers to limit businesses' use of their sensitive personal information to help guard against identity theft, to opt out of the sale and sharing of their personal information, and to request that businesses correct inaccurate information about them.

- California Privacy Rights Act of 2020

Common Law Foundations

Warren & Brandeis' seminal article "The Right to Privacy" (1890):

- Privacy as the "right to be let alone"
- Inspired by new technologies (instant Kodak cameras) & business models (newspaper enterprise)
- Grounded in tort law (civil injuries/wrongs) - not contract, trusts, IP/moral rights, property rights, trade secrets



A man records in a letter to his son, or in his diary, that he did not dine with his wife on a certain day. No one into whose hands those papers fall could publish them to the world, even if possession of the documents had been obtained rightfully; and the prohibition would not be confined to the publication of a copy of the letter itself, or of the diary entry; the restraint extends also to a publication of the contents. What is the thing which is protected? Surely, not the intellectual act of recording the fact that the husband did not dine with his wife, but that fact itself. It is not the intellectual product, but the domestic occurrence.

- Warren & Brandeis



A right to privacy is neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information...

- Helen Nissenbaum, *Privacy in Context*



Privacy was once misconstrued as being about hiding and secrecy. Now it's understood to be something much more pressing: power dynamics between the individual, the state and the market. [Data protection] must seek to mitigate the inherent power imbalances between people —and those that collect, process and profit off their data.

- Frederike Kaltheuner

Today's Privacy Landscape



Privacy Safeguards in Law, Code, and Norms

- Broad legal protections against unfair or deceptive use of data, violation of reasonable expectations of privacy
- Specific laws provide heightened protection for sensitive information (e.g., health, financial, kids)
- Technical measures reduce risk of unauthorized access (e.g., encryption, anti -scraping policies)
- Social norms constrain organizations and individuals who might otherwise use data in unexpected ways

U.S. Patchwork of Privacy Laws

- 4th Amendment (search)/14th Amendment (due process) and state constitutional protections
- State and local law – torts for invasion of privacy, FOIA laws, surveillance ordinances
- Broad consumer protection laws
 - FTC – Section 5 of FTC Act, prohibits unfair or deceptive uses of data
 - State AGs – Unfair & Deceptive Acts and Practices laws (UDAP)
 - Self-regulation (binding commitments)
- Sectoral laws provide heightened protection for sensitive information (e.g., health, financial, kids) -- COPPA, HIPAA, FCRA, GLBA, FERPA, VPPA, DPPA, WireTap Act, etc.



Many Recent Changes

(more about this later)

- EU General Data Protection Regulation
- California Consumer Privacy Act (and CPRA)
- Additional state consumer privacy laws
- Proposed federal legislation

U.S. Patchwork of Privacy Laws

- “Code is law” – organizations design technical measures into devices and data flows that have much the same force as written laws
- Privacy by design (PbD) and privacy by default
 - Technical measures that protect privacy and security
 - Demonstrate good faith, intent to respect privacy, comply with data protection laws
- Design of devices and interfaces influences consumer choices
- Increasingly technical protections are implemented by end users or by platforms (e.g., app stores)

For example...

- Encryption
- Local processing
- Differential privacy
- MAC randomization (iOS 8+)
- Device permissions
- Ad blockers and anti-tracking software
- Do Not Track signals
- Anti-scraping tools



Evolving Privacy Norms

- Social norms constrain organizations and individuals who might otherwise use data in unexpected ways
 - Creepy or cool?
 - Cultural and generational differences?
 - Where do we stand in an elevator?
- Influenced by a confluence of factors, including design choices and expectations about legal protections
- Norms exist at all levels of information exchange – from interpersonal, individual - organizational, societal
 - New business models often impact more norms than they intend to. “Contextual integrity” is key

Controversial...



Cool!



Commonplace?





What's Next?

U.S. Consumer Privacy Law

(Torts - *very* rarely pursued, vary by state)

Sectoral laws : cover some sectors or types of data, but not all

FTC & state UDAP laws : limited to unfair & deceptive practices, not all entities

Missing: substantive comprehensive consumer privacy laws

- All sectors/types of data
- Specific obligations on organizations

Law	Sector/Type of Data	What is <u>Not</u> Covered:
HIPAA	Healthcare institutions	<i>sensitive health data collected by fitness apps, wearable devices, and real-world data</i>
GLBA	Financial institutions	<i>data brokers, proxies for financial health</i>
COPPA	Data from children <13	<i>data from teenagers</i>
VPPA	Video rental records	<i>data from mobile apps, web browsing history</i>
FTC Act (Section 5)	(All) Commercial Data*	<i>non-profits, government entities, exempt industries</i>

Changing Expectations

“Patchwork” of privacy laws leaves gaps

- Certain sectors/data types not covered by privacy laws
- Privacy harms that aren’t legally enforced/enforceable
- Consumer confusion and resignation

“Notice & Consent” laws also under pressure

- N&C model of privacy regulation: as long as consumers have an opportunity for notice and consent, their privacy is protected
- Reality: No one reads privacy policies, and no one can negotiate for better practices
- Concern:
 - Puts the burden of protecting privacy onto individual consumers;
 - Leaves businesses uncertain about what practices are acceptable (or not)

GDPR’s influence

- Comprehensive data protection obligations - far beyond “Notice & Consent”
- Mega privacy fines & extraterritorial scope
- C-suite attention to data protection



Changing Expectations

Response: New generation of proposed privacy laws that are:

- Comprehensive (all sectors/data)(almost all organizations)
- Put clear, proactive obligations on companies to protect personal data
- Adopt many (not all) GDPR concepts (controllers, processors, etc.)
- Create new* substantive rights for individuals
 - Access
 - Correction
 - Deletion (/erasure/Right to be Forgotten)
 - Portability
 - Restrict processing - e.g., opt- out of sale/sharing, targeted advertising, profiling



Changing Expectations

California Consumer Privacy Act (CCPA):

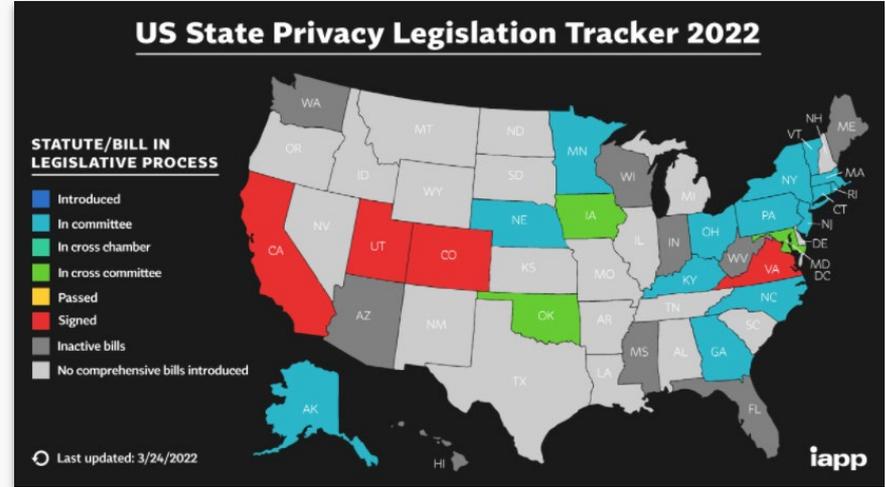
- Economy size + extraterritorial scope = de facto US law
- First introduced as a ballot initiative spearheaded by privacy activists, following Cambridge Analytica and GDPR coming into effect
- “Do Not Sell My Personal Information” + basic access, deletion, and transparency requirements
- Amended in Nov. 2020 by ballot initiative: California Privacy Rights Act (CPRA) - some new protections for sensitive data, and established a state privacy agency



Changing Expectations

Hundreds of bills introduced in states:

- 38 states introduced more than 160 consumer privacy related bills in 2021 (compared to 30 states in 2020 and 25 in 2019), with comprehensive privacy legislation introduced in 25 states.
- Proposed state legislation in 28 states this session (including Georgia - SB 394)
- Four have become law: California, Virginia, Colorado, and Utah



- “California model” - similar to CCPA, with “Do Not Sell” provisions
- “Washington model” - similar to (failed) Washington State efforts, with broader individual rights, risk assessments, and GDPR-like definitions

Changing Expectations

Dozens of federal bills

- 116th Congress (Jan 2019 - Jan 2021): 20+ comprehensive bills introduced in the Senate and House (none passed); the most significant legislation was introduced by leading Democratic and Republican leaders in the Senate Commerce Committee
- 117th Congress (Jan 2021 to present): 30+ bills introduced so far; greater variety of issues (e.g. content moderation, anti-trust)
- Stuck on two key issues: enforcement & preemption

Bills in Both Chambers (117th Congress)					State law pre-emption	Private right of action	Sponsor
House number	Senate number	Key provisions	State law pre-emption	Private right of action	Sponsor		
HR.651	S.1111	Use and disclosure of COVID-19 test data.	⊗	✓	Rep. Eshoo, Anna; Sen. Blumenthal, Richard		
HR.778	S.1111		N/A	N/A	Rep. Speier, Jackie; Sen. Schatz, Brian		
HR.847	S.1111				Sen. Stevens		

House of Representatives Bills (117th Congress)					State law pre-emption	Private right of action	Sponsor
Number	Title	Key provisions	State law pre-emption	Private right of action	Sponsor		
HR.674	Protecting Consumer Information Act				Sen. Blumenthal, Richard		

Senate Bills (117th Congress)					State law pre-emption	Private right of action	Sponsor
Number	Title	Key provisions	State law pre-emption	Private right of action	Sponsor		
S.24	Protecting Personal Health Data Act	Directs Department of Health and Human Services to regulate consumer devices, services, apps and software that collect or use personal health data.	✓	N/A	Sen. Blumenthal, Richard		
S.47	APP ACT	Requires operators from specified countries that make their software available to U.S. consumers to disclose to the Federal Trade Commission and Department of Justice certain information, including any data protection measures in place.	✓	⊗	Sen. Rubio		
S.103	BROWSER ACT of 2021	Prohibits data collection from U.S. users if the operator complies with requests from specified foreign governments to disclose U.S. consumer data.	✓	⊗	Sen. Blumenthal, Richard		
S.300	Stop Marketing And Revealing The Weaknesses And Trackers Consumer Health Data Act	Requires covered entities to obtain users' opt-in approval to use their sensitive information.	⊗	⊗	Sen. Cassidy, Bill		
S.319	Data Care Act of 2021	Prohibits the transfer or sale of consumer health information collected from a "personal consumer device" to entities whose primary business function is to collect or analyze consumer information for profit, unless it obtains the consumer's informed consent.	⊗	⊗	Sen. Schatz, Brian		
S.344	Mind Your Own Business Act of 2021	Imposes certain responsibilities on online service providers with respect to their handling of identifying data, including limiting it from unauthorized access and preventing harm.	⊗	✓	Sen. Wyden, Ron		
S.376	Consumer Data Privacy and Security Act of 2021	Requires assessments, periodic reporting and opt-out processes by covered entities that operate high-risk or automated decision-making information systems, such as AI or machine learning.	✓	⊗	Sen. Moran, Jerry		
S.383	Children and Teens' Online Privacy Protection Act	Imposes criminal penalties for false certification of annual reports by corporate officers.	⊗	⊗	Sen. Markle, Edward		
S.362	Social Media Privacy Protection and Consumer Rights Act of 2021	Provides consumers with rights to access, correct and delete their data.	⊗	⊗	Sen. Markle, Edward		
S.2052	Facial Recognition and Biometric Technology Moratorium Act of 2021	Requires businesses to implement data security programs.	⊗	⊗	Sen. Blumenthal, Richard		
S.238	Data Protection Act of 2021	Prohibits collection without consumer consent.	⊗	⊗	Sen. Blumenthal, Richard		
S.209	Setting an American Framework to Ensure Data Access, Transparency and Accountability Act	Extends primary protections to children aged 13-16, including the provision of notice and consent.	⊗	⊗	Sen. Blumenthal, Richard		
		Grants users of online platforms the right to opt out of data collection and tracking, providing users with the right to access, requires "plain English" terms of the right to access, and mandates establishment of privacy and security programs.	⊗	✓	Sen. Markle, Edward		
		Prohibits biometric surveillance by the federal government without explicit statutory authorization.	N/A	N/A	Sen. Gillibrand, Kirstin		
		Establishes an independent federal "Data Protection Agency" to regulate high-risk processing and use of personal data.	✓	⊗	Sen. Wicker, Roger		
		Requires companies to publish privacy policies, appoint privacy and data protection officers, implement customer's rights to correction and deletion, and maximize the data they collect.					

Senate Bills (117th Congress)					State law pre-emption	Private right of action	Sponsor
Number	Title	Key provisions	State law pre-emption	Private right of action	Sponsor		
S.1111			N/A	N/A	Sen. Blumenthal, Richard		
S.1111			N/A	N/A	Rep. Lieu, Ted		
S.1111			N/A	N/A	Rep. Walberg, Tim		
S.1111			✓	⊗	Rep. DeBene, Suzan		
S.1111			N/A	N/A	Rep. Bishop, Dan		
S.1111			N/A	N/A	Rep. Biggs, Andy		
S.1111			N/A	N/A	Rep. Jackson Lee, Sheila		



Federal Legislative Roadblocks



	Businesses and Conservatives prefer:	Advocates and Liberals prefer:
Preemption: How far will a federal law preempt, or nullify, state laws?	Strong preemption (nullify most state privacy laws, such as CCPA) – single standard, legal uniformity, impracticalities of complying with inconsistent standards across state lines (particularly for online and mobile data)	Less or no preemption – concerns over a weak national law preventing further progress in states; desire to allow states to continue innovating, raising the bar, and responding to new technology
Enforcement: Should individuals be permitted to challenge violations of the law in court?	FTC Enforcement only – single national standard, legal predictability and uniformity compared to federal court system, costs, concerns over abusive or meritless class action litigation	FTC Enforcement + Strong Private Right of Action – incentivizes compliance, codifies the right of the individual to have their “day in court,” parallels to anti-discrimination law in US history

California Consumer Privacy Act (CCPA) + California Privacy Rights Act (CPRA)

- **Key procedural features:**
 - Complicated legislative history (ballot initiatives, amendments, AG regulations, oh my!)
 - Complicated oversight - AG rulemaking, new privacy agency CPPA
 - CCPA **already** in effect; some CPRA provisions **already** in effect, some come into effect in 2023
 - 6 months between going into effect & enforcement
- **Numerous exemptions (including publicly available information), scope limited to for-profit businesses of a certain size** -
- **Key substantive rights:**
 - Transparency; Right to Access (in portable format); Right to Delete;
 - “Do Not Sell My Personal Information” button
 - “Personal information” and “sell” defined broadly (CPRA extends to “sell or share”)
 - Right to limit use of sensitive personal data
 - Non-discrimination/retaliation against consumers who exercise their rights
 - Regulations promulgated by the California AG:
 - prohibit “dark patterns” in responding to opt-out requests
 - require companies to honor global opt-out signals sent by browser plug-ins or similar tools (a subject of ongoing dispute)

Virginia Consumer Data Protection Act (passed 2021; in effect 2023)

- **Key procedural features:**
 - Derived from the 2019 Washington Privacy Act (bill, didn't pass)
 - Enforcement by Attorney General
 - No rulemaking
 - Definitions align more closely with GDPR - e.g. Controller/Processor distinction
- **Numerous exemptions (including publicly available information), scope limited to for-profit businesses of a certain size**
- **Key substantive rights:**
 - Transparency; Right to Access (in portable format); Right to Delete
 - Rights to Opt - Out of Sale, Targeted Advertising, and/or Profiling in Furtherance of Legal or Similarly Significant Effects
 - “Sale” defined more narrowly than CCPA
 - Controllers must conduct data protection risk assessments for high-risk processing
 - Affirmative consent required to collect “sensitive data” (revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship, or immigration status; genetic or biometric data; precise geolocation data).

Colorado Privacy Act (passed 2021; in effect 2023)

- **Key procedural features:**
 - Similarities to both CCPA and VCDPA
 - Enforcement by Attorney General
 - Additional rulemaking from Attorney General will provide further specificity
- **Numerous exemptions (including publicly available information), scope limited to for-profit businesses of a certain size**
 - *Includes non -profits!*
- **Key substantive rights:**
 - Consumer rights to access, delete, correct data, and to opt-out broadly to sale, targeted advertising, and profiling (like VCDPA)
 - Controllers must conduct data protection risk assessments for high-risk processing
 - Affirmative consent required to collect “sensitive data” (revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis, sex life or sexual orientation, or citizenship or citizenship status; genetic or biometric data; personal data collected from a known child)
 - Beginning in 2024, controllers will be required to allow consumers to exercise their right to optout through a "user-selected universal opt-out mechanism that meets the technical specifications established by the Attorney General”
 - Companies must establish appeals procedures for denials of consumer rights

Utah Consumer Privacy Act (passed 2022; in effect December 2023)

- **Key procedural features:**
 - Similarities to Colorado and Virginia laws
 - Enforcement by Attorney General
 - Additional rulemaking from Attorney General will provide further specificity
- **Key substantive rights:**
 - Consumer rights to access, delete, and to opt -out broadly to sale and targeted advertising. It does not include a right to correct inaccurate personal data or to opt -out of significant profiling decisions, and also does not include affirmative, opt -in consent for the collection and processing of sensitive data.
 - Covered businesses have transparency requirements and new data security obligations (no data protection risk assessments required)
- **Enforcement:**
 - Delegates exclusive enforcement authority to the Utah Attorney General but would require a consumer complaint process prior to initiating an enforcement action.



Some Key Differences between the State Laws

- **Which organizations are covered by the law**
 - Non-profits in Colorado, but not VA or CA
 - Control or process data of 50,000 consumers (CA) vs. 100,000 consumers (VA, CA) annually; etc.
- **What constitutes sensitive data**
 - California, unlike Virginia or Colorado, includes “union membership,” “philosophical beliefs”, “sex life”, “genetic data,” “contents of a consumer’s mail, email, and text messages”, government ID numbers
 - Virginia and Colorado, unlike California, includes: “citizen or immigrant status” and data from a “known child”
- **Compliance specifics...**
 - What has to go into your privacy policy
 - What triggers a data protection assessment
 - How to respond to access requests (DSARs); etc.

Push on Enforcement: FTC

US Federal Trade Commission

- **Background**

- Independent agency with consumer protection & antitrust missions
- May initiate an enforcement action using either an **administrative** or **judicial** process;
 - If a company violates a final order, it is liable for a civil penalty for each violation.
 - Can refer to U.S. Dep't of Justice for criminal penalties
- Rulemaking authority (*akin to implementing acts/decisions of the European Commission, but broader*)

Novelties

- Innovative enforcement toolbox (deletion of proprietary algorithms)
- Lina Khan (antitrust scholar) appointed as Chair
- Non-traditional Rulemaking detailing Section 5 (unfair & deceptive commercial practices) on the horizon

Push on Enforcement: State AGs

Notable recent enforcement by State Attorneys General (“AGs”) under e.g. the Children’s Online Privacy Protection Act (“COPPA”)

Google hit with new antitrust lawsuit from 38 state attorneys general

It is the third major antitrust suit against Google since October.

By **Catherine Thorbecke** and **Aaron Katersky**

December 17, 2020, 2:59 PM • 6 min read



State AGs plan to fight court dismissal of their antitrust claims against Facebook

PUBLISHED WED, JUL 28 2021-11:20 AM EDT

Lauren Feiner
@LAUREN_FEINER



KEY POINTS

- State attorneys general who accused Facebook of illegal monopolization will fight a court's dismissal of their claims, according to a Wednesday court filing.
- The Federal Trade Commission has until August 19 to file an amended complaint against Facebook.

This Month in Privacy...

JD SUPRA[®] MENU

March 24, 2022

Buyers Beware: the FTC's Case Against CafePress Highlights Privacy and Data Security Risks in Corporate Transactions

Newsletters Shows DONATE

MARKETPLACE[™]

Consumer privacy is being decided state by state

MARKETPLACE TECH

KIMBERLY ADAMS AND JESUS ALVARADO

Consumer privacy is being decided state by state

iapp News Connect Train Certify Resources Conferences Join STORE

The Privacy Advisor

Biden's State of the Union remarks put children's privacy front and center

EFF

About Issues Our Work Take Action Tools Donate

Stop Invasive Remote Proctoring: Pass California's Student Test Taker Privacy Protection Act

SCOTT IKEDA · MARCH 29, 2022

CCPA Data Privacy Trends Report: Data Subject Requests Indicate California Consumers Are Quick To Assert Their Privacy Rights

SCOTT IKEDA · MARCH 29, 2022

LAW & GOVERNMENT PUBLIC SAFETY

Apple digital driver's license in Arizona raise privacy concerns

BY: JEROD MACDONALD-EVOY - MARCH 2022

Ad industry worried about expansion of Apple's iPhone privacy features

Mike Peterson | Mar 28, 2022

abc NEWS

US, EU Tentatively Agree on Trans-Atlantic Data Privacy Framework

by Mark Rasch on March 30, 2022

Irish regulator fines Facebook for privacy law violations

Ireland's privacy watchdog has...

Meta, 17

Utah Consumer Privacy Act Newest State Privacy Act Signed into Law

March 15, 2022, 11:15 AM · 1 min

Could Congress fix AI bias with privacy rules?

By BRENDAN BORDELON | 03/29/2022 10:00 AM EDT

JD SUPRA[®]

Wyoming Enacts Genetic Data Privacy Act

March 11, 2022

Linn Freedman

Genetic Data Privacy + Security

Medical Economics

Privacy group issues warning about danger to patient information

March 25, 2022

Todd Shryock

The New York Times

How California Is Building the Nation's First Privacy Police

PLAY THE CROSSWORD



Questions?

Amelia Vance
Founder and President
Public Interest Privacy Consulting
avance@pipc.tech
www.pipc.tech
[@ameliaivance](https://twitter.com/ameliaivance)

