

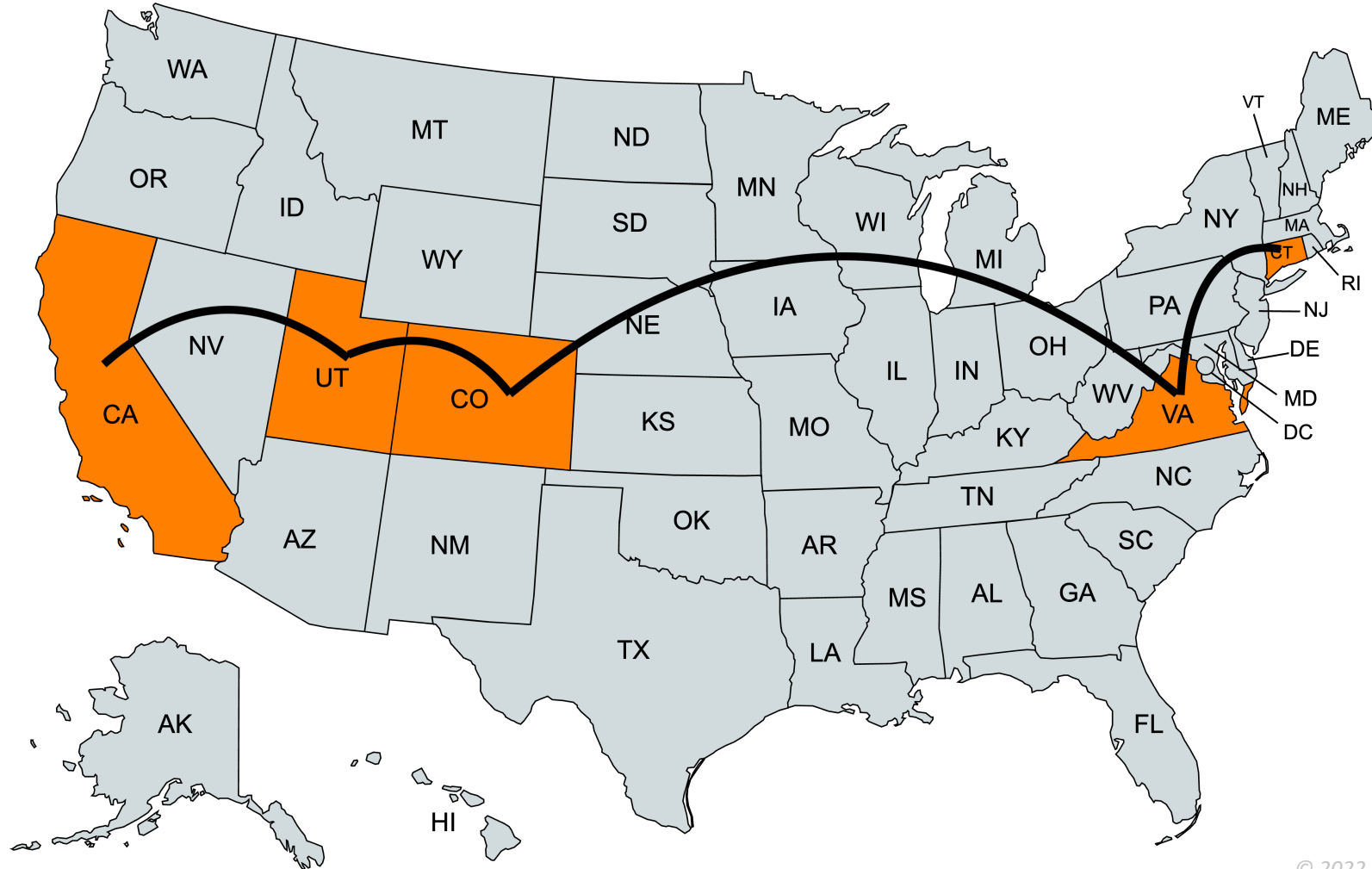


US Privacy Road Trip Session 1

September 15, 2022

* Although we will be providing legal information during this webinar, we will not be providing legal advice.

US Privacy Road Trip



California Changes



Consumers' Rights

- Notice
- Deletion
- Right to Know
 - Specific Information
 - Category Information
- Correction
- Port
- Opt-Out of Selling
- Opt-Out of Sharing
- Limit Use & Disclosure of Sensitive PI



Responding to Requests to Know

- CPRA expands the look-back period
- Instead of the previous 12 months, businesses will have to disclose information beyond that for any PI processed on or after January 1, 2022,
- UNLESS providing it for more than 12 months is:
 - Impossible or
 - Would involve a disproportionate effort
- Regs will need to address what would qualify for that exception

what's the
opposite of
disproportionate?



proportionate, balanced, equal,
even, proportional, moderate,
reasonable, relative,
corresponding, per capita



 Thesaurus.plus

Correction

- Responses
 - Verification (to prevent fraud)
- Exemptions
 - Impossible
 - Disproportionate level of effort
 - Information is accurate
- Consumer right to submit an addendum if correction request is denied

Right to Opt-Out of Selling or **Sharing**

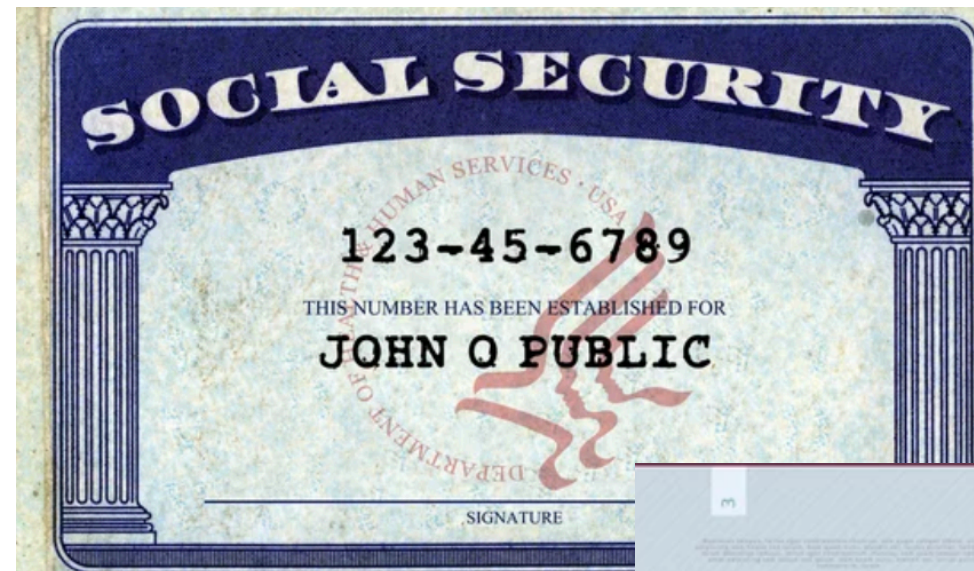
- CPRA expands on CCPA to include opting out of the **sharing** of PI
- Sharing means cross context behavioral advertising
- Must have link(s) on your website!
- Rules need to identify:
 - Requirements & tech specs for an opt-out preference signal to indicate a consumer's intent to opt out or to limit the use/disclosure:
 - Tech specs for an opt-out signal specifying the consumer is less than 13 or is at least 13 but less than 16
 - How to process rights exercised through preference signals



Sensitive Information

Sensitive PI

- Includes:
 - Biometrics
 - Communications
 - Finances
 - Genetics — genetic data
 - Precise Geolocation
 - Government ID
 - Health
 - Race, religion and union membership
 - Sex Life



Limit the Use of Sensitive Data

- Provide Notice
- Link to “Limit the Use of My Sensitive Personal Information”
- Minimize -- keep it no longer than ‘reasonably necessary’
- Future Regulations on recognizing platform, technology or other mechanism such as
 - Browser plug-in
 - Privacy Setting
 - Other user-enabled mechanism



California Website Link Examples

Do Not Sell My Personal Information

Do Not Share My Personal Information



Do Not Sell or Share My Personal Information

Limit the Use of My Sensitive Personal Information

Do Not Sell or Share My Personal Information and
Limit the Use of My Sensitive Personal Information

Service Provider and Contractor Obligations

- a prohibition on selling or sharing the PI
- a prohibition on retaining, using or disclosing the personal information outside of the direct business relationship with the business
- a prohibition on combining PI from different sources;
- a requirement to notify the business of sub-processors;
- a mandate to bind sub-processors by written contract to the same obligations;
- provisions regarding monitoring of compliance/oversight
- certify their understanding of and compliance with these contractual requirements (contractors, not SP)



Data Protection Assessments

- CPRA calls them "risk assessments"
- Submit to the CPPA on a regular basis
- *At least* triggered by processing sensitive personal information
- Contents
 - Weighing benefits and risks to various audiences
 - Goal: Restrict processing if the risks to the consumer outweigh the benefits to all stakeholders



Audits

- Contractor & Service Provider terms to allow business to monitor their CCPA compliance
- Terms include, not limited to, at least once a year:
 - Manual reviews
 - Automated scans
 - Regular assessments, audits, or other technical and operational testing
- For businesses whose processing presents a significant risk:
 - Annual independent cybersecurity audit
 - Risk to be determined by CPPA regulations:
 - Size and complexity of the business and
 - Nature and scope of the processing

Utah



Utah Consumer Privacy Act (UCPA) Overview

- Comprehensive consumer privacy
- Passed on 24 March 2022
- Effective date: 31 December 2023
- Broadly based on Virginia's Consumer Data Protection Act
 - ... with a few business-friendly tweaks



UCPA Applicability

Three requirements*:

1. Conducting business in UT/targeting Utahns;
2. Annual revenue of \$25M; and
3. Either (i) processing personal data of 100k+ Utahns **OR** (ii) deriving >50% of revenue from sale of personal data and processing personal data of 25k+ Utahns

* Some exceptions apply



Sensitive Data

- Definition
 - Racial or ethnic origin
 - Religious beliefs
 - Sexual orientation
 - Citizenship or immigration status
 - Medical history, mental or physical health conditions, treatments and diagnoses
 - Genetic and biometric data used to identify an individual
 - Specific geolocation data (within 1/3 mile)
- Processing
 - Only requirements are to first (i) present consumer with “clear notice” and (ii) provide an opportunity to opt out of the processing
 - This opt-out right is not mentioned anywhere else in the UCPA, so details are hazy



Utah Consumer Rights

- Notice
- Confirmation & Access
- Deletion*
- Portability*
- Opt-out of targeted ads and sales
- Non-discrimination for exercising privacy rights



Photo by [Icons8 Team](#) on [Unsplash](#)

What's Not There?

- No regulation of profiling/automated decision-making
- No data protection impact assessments
- No appeal process for denied rights requests
- No authorized agents
- Implementing regulations*



Enforcement

Utah: People Working Together!

Unique, two-tiered process:

1. Department of Commerce's Division of Consumer Protection
 - Receives consumer complaints
 - May investigate
 - Substantial evidence of violation → refer to Attorney General
2. Attorney General
 - Upon referral, AG may initiate enforcement action



Enforcement

- Cure provision
 - 30 days to fix the violation and promise not to do it again
- Fines up to \$7,500 per violation
 - No requirement that violation be intentional to reach that amount
- Can also recover actual damages to affected consumers



Colorado





Colorado Privacy Act (CPA)

- Effective date: July 1, 2023
- Coverage:
 - Any business (including nonprofits) that intentionally produces or delivers products or services to the state's residents AND either:
 - Controls or processes personal data of 100k+ the state's residents; or
 - Sells ANY personal data and controls or processes the data of 25k+ Coloradans
- Exempted
 - Employee and B2B Data
 - HIPAA Covered Entities
 - FCRA & GLBA Data
 - De-identified data & publicly available information
- Violation of CPA = Deceptive Trade Practice
 - Up to \$20,000 per violation, not to exceed \$500,000 in total; or
 - \$10,000 per violation if the consumer is 60 years old or older, with no cap





Consumers' Rights

- Notice
- Deletion
- Right to Know
- Correction
- Port
- Appeal
- Opt-Out of Selling
- Opt-Out of Targeted Advertising
- Opt-Out of Profiling with Significant Effects





Sensitive Information



Sensitive PI

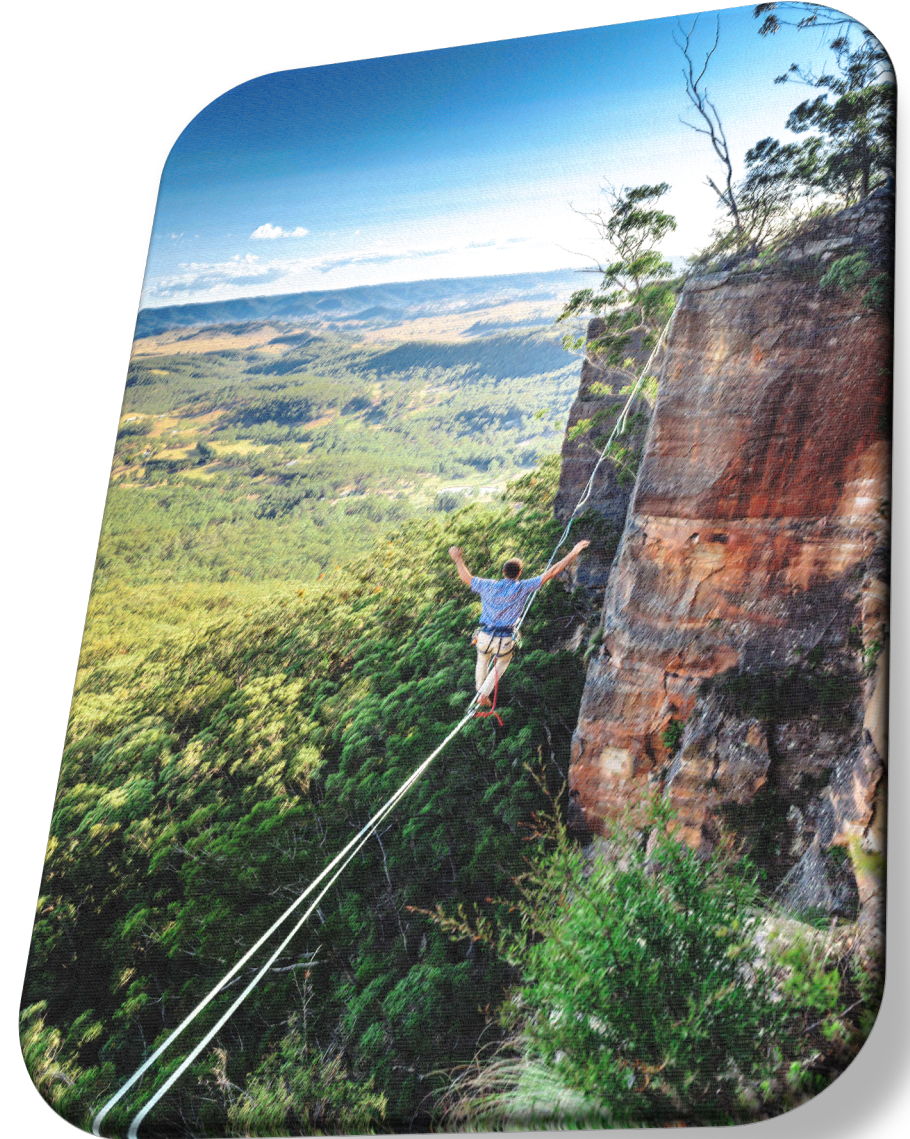
- Includes:
 - Racial or ethnic origin
 - Religious beliefs
 - Genetic or biometric data for the purpose of identifying a person
 - Personal data collected from a known child
 - Mental or or physical health condition or diagnosis
 - Sex life or sexual orientation
 - Citizenship or citizenship status
- Affirmative Consent
- Data Processing Assessment





Data Protection Assessments

- Analogous to GDPR's Data Protection Impact Assessments
- Triggered by:
 1. Processing sensitive data;
 2. Processing Personal Data for targeted advertising;
 3. Selling Personal Data;
 4. High-risk profiling;
 5. Other processing activities that present a heightened risk of harm to consumers
- Contents
 - Weighing benefits and risks to various audiences
 - Goal: Restrict processing if the risks to the consumer outweigh the benefits to all stakeholders



Virginia



Virginia Consumer Data Protection Act (VCDPA)

- Effective date: January 1, 2023
- Unique mix of CCPA, GDPR, and other privacy concepts
- Compliance is generally a bit simpler for businesses than the CCPA
- However, on a few key issues it is stricter



What Businesses Are Covered?

- Two thresholds for the VCDPA to apply:
 - Controlling or processing the personal data of 100,000 or more Virginia residents in a calendar year
 - Controlling or processing the personal data of 25,000 or more Virginians and deriving over 50% of gross revenue from sale of personal data
- All organizations subject to HIPAA or Gramm–Leach–Bliley exempt
- Non-profits and institutes of higher education exempt



Special Categories of Data

- **De-identified data:** take reasonable measures to ensure it cannot be linked to anyone; publicly commit to keep it de-identified; and contractually obligate recipients to comply with the VCDPA
- **Publicly available information:** government records or widely distributed information (e.g., media, or public sharing by consumer)
- **Pseudonymous data:** data that isn't linked to anyone, but could be with other information, maintained separately
- **Sensitive data:** (i) race, ethnicity, religion, health diagnoses, sexual orientation, citizenship, immigration status; (ii) biometric data for identification; (iii) known children's data (under 13); and (iv) precise geolocation data (within 1,750 feet, or ~1/3 mile)



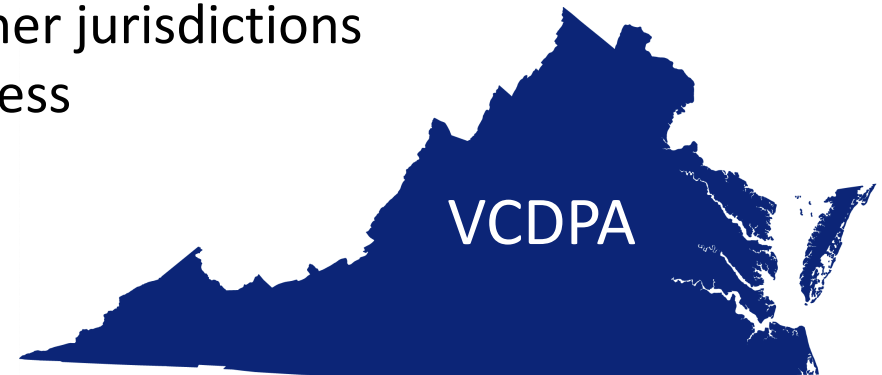
Controller Obligations: Opt-in for Processing Sensitive Data

- Controllers cannot process sensitive data without consent of the consumer
 - Sensitive data = protected classes, biometric data, children's data, precise geolocation data
- Consent means “a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data”
- For children's sensitive data, must comply with COPPA
 - A child is anyone under 13



Data Protection Assessments

- Required: (i) targeted advertising; (ii) selling personal data; (iii) profiling consumers in a way that presents a reasonably foreseeable risk of negative impact; (iv) sensitive data; or (v) “a heightened risk of harm to consumers”
- Assessments must weigh benefits and risks, as mitigated by safeguards
- Can re-use assessments done to comply with other jurisdictions
- Don’t need to make them public, but AG can access



Enforcement

- No private right of action
- AG enforcement only: injunctions and fines
- Fines up to \$7,500 per violation (plus attorney fees)
- 30-day cure period
- Money collected goes into Consumer Privacy Fund to support AG enforcement efforts



Connecticut



Connecticut Personal Data Privacy and Online Monitoring Act

- Effective date: 1 July 2023
- Penalties: \$2k – \$10k*
- Similar to Virginia and Colorado
- Key differences:
 - Consumers whose data used for payment processing excluded
 - Authorized Agent
 - Global opt-out in 2025
 - Can't be default setting
 - 60-day cure period
 - Optional in 2025



Applicability



Topic	CA	CO	CT	UT	VA
Number of Data Subjects	100,000 or	100,000 or	100,000* or	100,000 or	100,000 or
Sale/Sharing Revenue	50% of revenue, or	25,000 + any revenue or discount due to sale	25,000 + 25% of revenue	50% of revenue, and	25,000 data subjects + 50% of revenue
Worldwide Revenue	\$25 million	N/A	N/A	\$25 million	N/A

Exemptions



Topic	CA	CO	CT	UT	VA
Employee/ B2B Data	X*				
Nonprofits		X			
HIPAA	Data & Institutions	Data	Data & Institutions	Data & Institutions	Data & Institutions
GLBA	Data	Data & Institutions	Data & Institutions	Data & Institutions	Data & Institutions
FCRA	Data	Data	Data	Data	Data
Other	Vehicle info	Air carriers State universities*	Universities	Indian tribes Universities Air carriers	Universities

Basic Notice



Topic	CA	CO	CT	UT	VA
Categories Collected					
Purpose of Processing					
Data Retention		X	X	X	X
Consumer Rights					
Categories of 3d Parties					

Notice of Higher-risk Processing



Topic	CA	CO	CT	UT	VA
Selling					
Targeted Advertising					
Profiling	X*	*	*	X	*
Sensitive Data		+	+	+	+
Incentives		X	*	X	X

Basic Consumer Rights



Topic	CA	CO	CT	UT	VA
Know & Access		X			
Correction				X	
Deletion					
Data Portability					
Appeal	X			X	

Opt-out Rights



Topic	CA	CO	CT	UT	VA
Selling					
Sensitive Data	Limit Use & Disclosure*	Opt In	Opt In	Opt in	Opt In
Profiling	X*	*	*	X	*
Targeted Advertising	Cross Context Behavioral Advertising				

Risk Assessments



Topic	CA	CO	CT	UT	VA
Sensitive Data				X	
Sale	?			X	
Targeted Advertising	?	*		X	
Profiling	?	*	*	X	*
Heightened Risk	?			X	
Reciprocity	?	?		X	

Enforcement




Topic	CA	CO	CT	UT	VA
Cure Period	X	60 days (until 2025)	60 days* (until 2025)	30 days	30 days
Amount	\$2,500 – \$7,500	\$2,000 – \$20,000*	\$2,000 – \$10,000*	\$7,500	\$7,500
Enforcer	CPPA	AG + 22 DAs	AG	Dept. of Comm. ⇔ AG	AG
Private Right of Action	Security breaches	X	X	X	X

Other



Topic	CA	CO	CT	UT	VA
Effective Date	1 Jan. 2023*	1 July 2023	1 July 2023	31 Dec. 2023	1 Jan. 2023
Children	Under 13; 13–16	Under 13	Under 13; 13–16	Under 13	Under 13
Global Privacy Signal	Allegedly	July 1, 2024	January 1, 2025		
Regulatory Action	CPPA	AG	None	None	None*

Global Privacy Control is  for this website

Nationwide Privacy Made Simple

With All US Privacy by SixFifty, you get coast-to-coast privacy coverage with a single set of customized compliance documents.

GET A DEMO



Do you know when current laws go into effect?

