2023 Privacy Update

New Year, New Laws

Lay of the Land

- 5 New State Laws:
  - California, Virginia, Colorado, Connecticut, and Utah
- CA and VA already in effect
- Headlines:
  - Sensitive personal data
  - Opt-out signals
  - Data Protection Assessments
  - HR data (in CA)

?

Lay of the Land

	CA	CO	CT	UT	VA
Disclose Retention Period	✅	X	X	X	X
Affirmative Consent for Sensitive PI	X	✅	✅	🔄	✅
Opt Out of Profiling	☑	✅	✅	X	✅
Right to Appeal	X	✅	✅	X	✅
Risk Assessment	☑	✅	✅	X	✅
HR Data Covered	✅	X	X	X	X

✅ Required
☑ Pending regulatory clarity
X Not required
🔄 Requires opt-out choice

Opt-Out Preference Signals

California provides some much needed clarity, but questions remain

What Are Opt-Out Preference Signals?

- Signal sent by “platform, technology, or mechanism” on behalf of a consumer that communicates the choice to opt-out of sale/sharing
  - Most commonly sent by browsers or browser extensions
- California provides very little guidance on exactly what types of signals businesses should look for
  - Must be in a format “commonly used and recognized by businesses” such as “an HTTP Header field or JavaScript object; and
  - Must make clear to the consumer that the “use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information”

What should you do when you get an OOPS?

- It’s easy, just treat the signal as any other opt-out request
  - Stop selling/sharing covered data within 15 days of receipt
  - Notify all third-parties business has sold to or shared with
- Information disclosed to Service Providers or Contractors pursuant to a written contract does not qualify as sale/sharing

Who is opting-out?

- It can be hard to tell who is sending an OOPS, especially if they are using a new device/browser
- Businesses must opt-out the specific browser/device that sent the signal and any consumer profiles associated with the browser/device
  - If known, must opt-out the consumer as well
- MAY ask for additional information to facilitate opt-out
  - If the consumer does not provide that info, still must process opt-out

What if you get an OOPS that conflicts with a consumer's privacy settings?

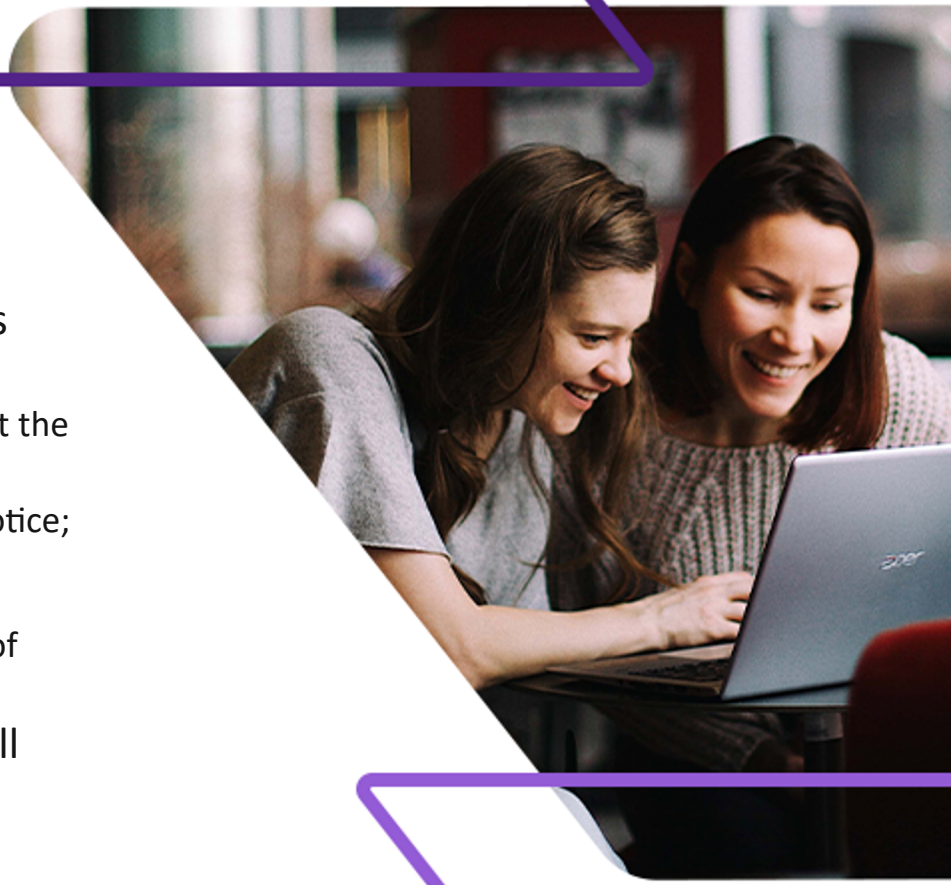
- It depends on what the opt-out signal conflicts with
- If it is a user's business-specific privacy settings:
  - Must process the opt-out
  - Can inform the consumer about the conflict and give them the chance to consent to continued sale/sharing
- If it is a financial incentive program the user has signed up for:
  - May just process the opt-out; OR
  - Inform the consumer about the conflict and ask them to "affirm" decision to opt-out of the incentive program

“Frictionless Processing”

- **Cannot charge a fee or other consideration**
  Must process Opt-Out Preference Signals without compensation from consumer
- **Cannot “change the consumer’s experience”**
  Must give consumers who use signals the same products/services that you give to other consumers
- **Cannot display a pop-up or other “interstitial content” in response to Opt-Out Preference Signal**
  Two exceptions to this requirement

But wait, there's more:

- Even with frictionless processing, a business must also:
  - Allow consumers to submit both DNS and Limit the Use requests via signals;
  - Include additional information in its Privacy Notice; and
  - Allow opt-out preference signals to "fully effectuate the consumer's request to opt-out of sale/sharing"
- Can only forego providing required links if all four requirements are satisfied



Colorado: Joining the Opt-out Signal Party Soon!

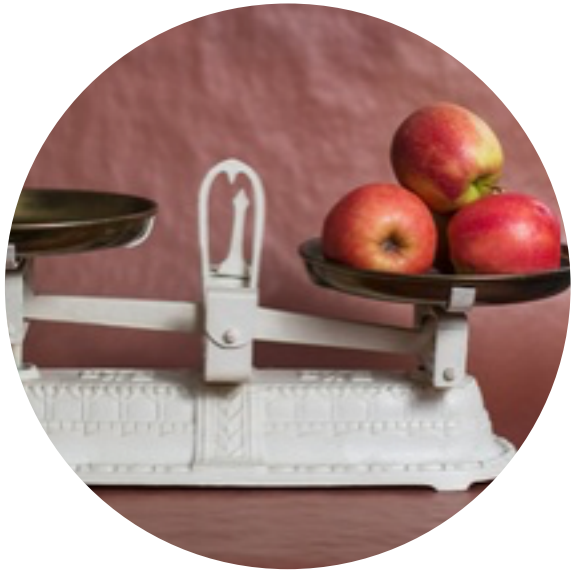
- Regulations deadline: July 1, 2023
  - Universal opt-out mechanism
  - Mandatory starting July 1, 2024
- Signals can opt out of both sales and targeted ads, or just one
- Can’t be default setting
- AG keeps list of standards
  - Initial list: January 1, 2024

Data Protection Assessments

Data Protection Assessments

- Risk Assessments (CPRA) or Data Protection Impact Assessments (GDPR)
- Internal analysis weighing pros and cons
- Triggered by “risky” activities from a data privacy persp
- Available on request by regulators

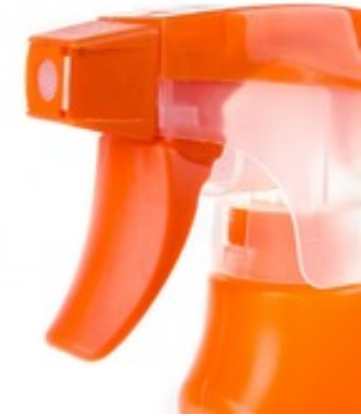
Weighing Pros and Cons



- Overview of types of questions:
  - Describe the processing activity and the context of its use
  - Describe the safeguards to protect the data
  - Balance the benefit of processing with the risk of causing harm
- Things to consider:
  - What is your organization's relationship with the data subjects?
  - Do the data subjects need special protection?
  - Benefits to consumers, stakeholders, your organization, and the public

DP Assessments: Triggers

- Triggered by “risky” activities from a data privacy perspective
  - Targeted advertising
  - Selling Personal Data
  - Sensitive Personal Data
  - Risky Profiling
  - Catch-all for “heightened risk” uses
- SixFifty tool walks through these



DP Assessments: Audience

- Available on request by regulators
  - May need to be proactively filed with the CPPA in CA periodically (regs pending)
- Your own organization
  - Prompt privacy policy improvements
- Can be reused

California Employee Data

Whose Data?

- When we say “employee” it’s very broad, and includes:
  - Members of the board
  - Covered dependents
  - Contract workers
  - Job applicants
  - Current and past employees
- Data Exceptions:
  - Publicly available information
  - Deidentified data
  - FCRA (Credit reports)
  - GLBA (Financial institutions)
  - HIPAA & CMIA (Health data)

Obligations for Employee Data

- Provide notice to employees
  - Place where employees will have access to it
  - Recommended that it is different from consumer notice
- Respond to rights requests
  - The same as consumer requests
- Exceptions
  - The same as consumer requests but generally more applicable

Examples of Exceptions

- Request to delete
  - Can’t because of the states record retention requirements
- Request to access
  - Don’t because records contain trade secrets
  - Don’t because records contain another person’s private information
- Request to amend
  - Don’t because the information is subjective, just one person’s opinion, and not fact.

CPRA Regulations

Approved by the CPPA on February 3

Timeline

- CCPA charged the AG & CPPA with implementing wide variety of regulations to flesh out the statute
- Despite initial deadline of July 1, 2022, CPPA approved regulations on February 3, 2023
  - Only addresses some of the issues referred by statute
- Expected to take effect later this spring

Key Points

- Opt-Out Preference Signals
- The Alternative Opt-Out Link
- Clarified “Disproportionate Effort” Standard
- Data Minimization Principles
- Requirements for Designing “Choice Architecture”
- Service Providers and Contractors
- Enforcement & Record-Keeping Requirements

Required Links

Do Not Sell/Share My Personal Information

- Required for all businesses that sell/share PI
- Must be located in the header/footer of the business' homepage

AND

Limit the Use of My Sensitive Personal Information

- Required for businesses that process sensitive PI for non-exempt purposes
- Must be located in the header/footer of the business' homepage

OR

Alternative Opt-Out Link

- "Your [California] Privacy Choices"
- Must direct consumers to explanation of both rights and mechanism to exercise them

“Disproportionate Effort”

- Used several places in the context of responding to consumer requests
  - Allows businesses not to comply with certain requirements if doing so would be unreasonably difficult or costly
- Applies when the “time and/or resources expended” by the business “significantly outweighs the reasonably foreseeable impact to the consumer” of not complying with a given requirement
  - Generally required to explain facts to consumer when claiming disproportionate effort
- Another area to monitor for development as enforcement begins

Data Minimization

- Businesses must conduct a set analysis to ensure privacy practices are in line with minimization obligations
- Two discrete tests –
  - One to ensure a purpose is appropriate and consistent with consumer expectations
  - Another to ensure data collection/processing are reasonably necessary and proportionate to that purpose

Factors to Consider

- Purpose Test:
    1. The relationship between the consumer(s) and the business.
    2. The type, nature, and amount of personal information that the business seeks to collect or process.
    3. The source of the personal information and the business's method for collecting or processing it.
    4. The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information.
    5. The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s).

- Necessary/Proportionate Test:
    1. The minimum personal information that is necessary to achieve the purpose.
    2. The possible negative impacts on consumers posed by the business's collection or processing of the personal information.
    3. The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers

“Choice Architecture”

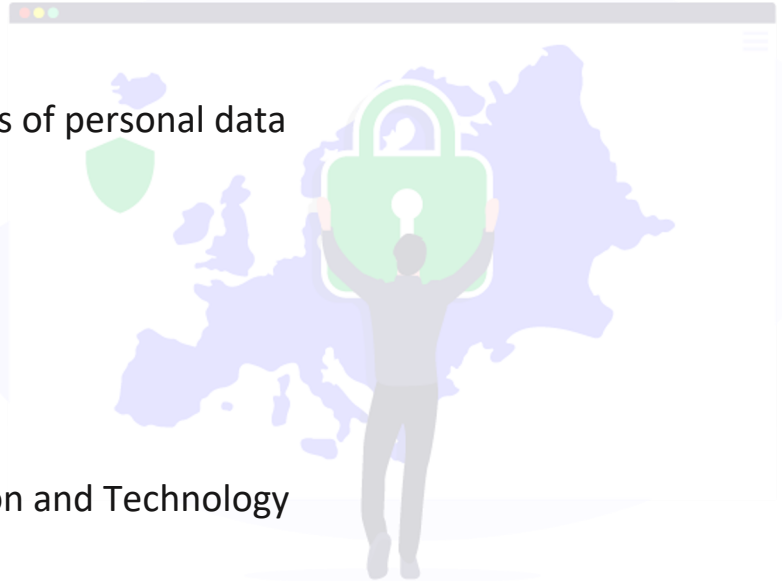
- Detailed requirements for how to offer consumers privacy choices
  - For example, when a business asks for consumer consent, how should that look?
- Emphasizes simplicity, symmetry, and ease of use
- Methods shall:
  - Be easy to understand;
  - Be symmetrical in choice;
  - Avoid confusing language or interactive elements;
  - Avoid impairing consumer ability to choose; and
  - Be easy to execute

Service Providers and Contractors

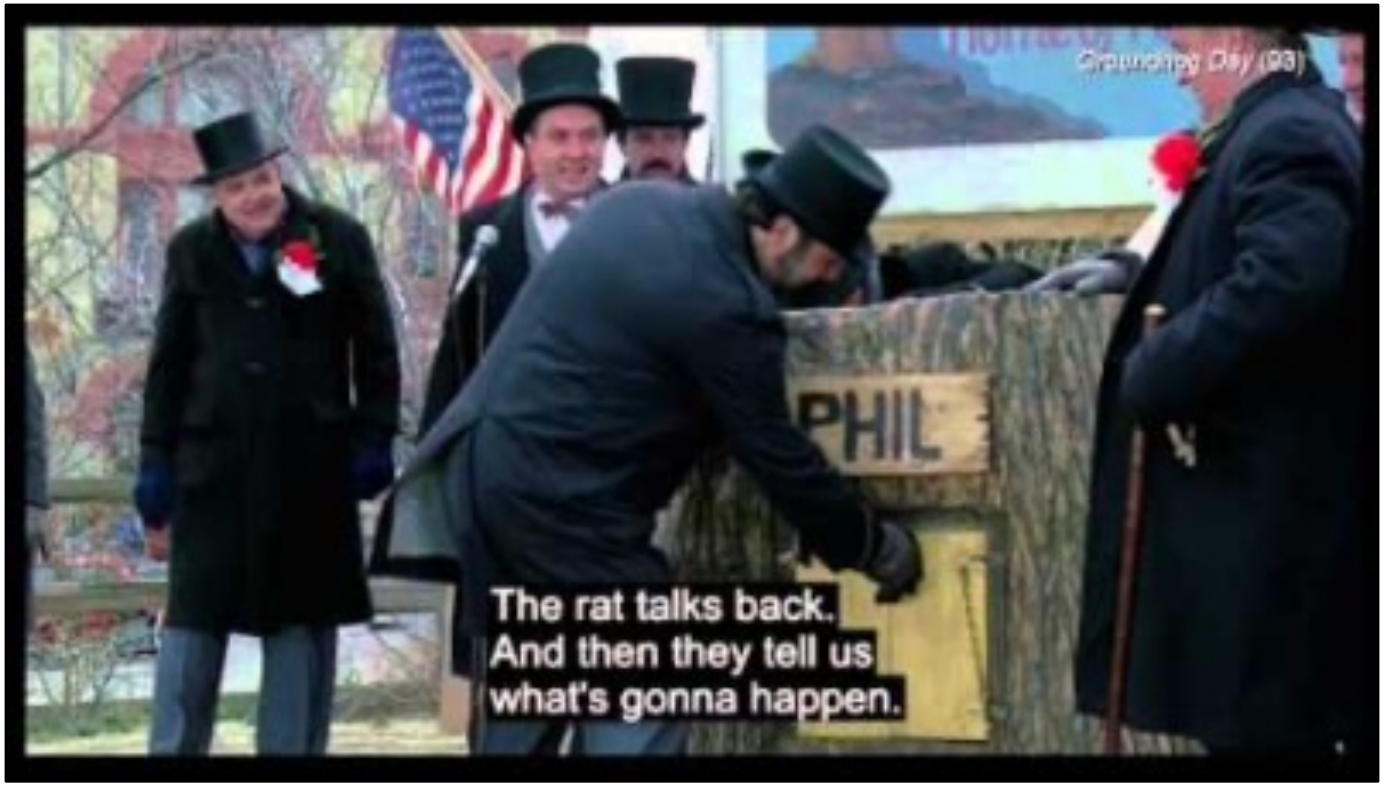
- Data disclosed to these entities is not “sold” or “shared”
- Both are defined by required written contract with the business
  - Service Providers must “process Personal Information on behalf of a business”
- Written contract must contain several required provisions
  - Must set forth the specific Business Purposes for which data is disclosed, and require the SP/C to only use disclosed data for those purposes;
  - Must require SP/C to comply with CCPA; and
  - Must grant business the right to monitor compliance and take remedial action
- CANNOT contract to provide targeted advertising

Dispatches from Europe

- CJEU decision re GDPR access requests
  - Must provide specific identities of the recipients of personal data
- EU–US data transfers
  - EU considering adequacy decision with US
- UK
  - International Data Transfer Agreement
  - Created new Department for Science, Innovation and Technology



Privacy Prognostications

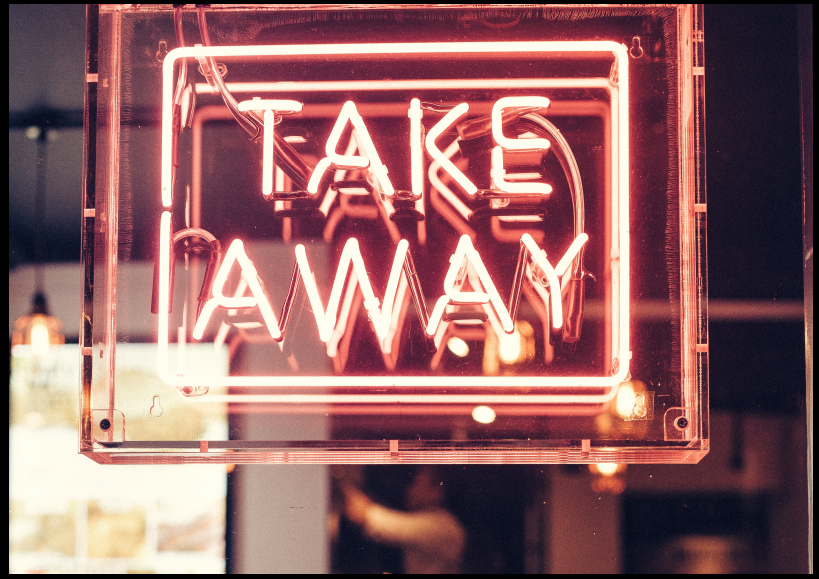


Privacy Prognostications

- New states?
- Federal action?
- More clarity?
- Areas to focus on?

Key Takeaways

- 5 New State Laws
- Opt-out Signals
- Data Protection Assessments
- HR Data (in California)
- Global Privacy Issues
- Can’t-miss prediction: More change



Q&A

sixfifty.com/all-us

All-US Privacy

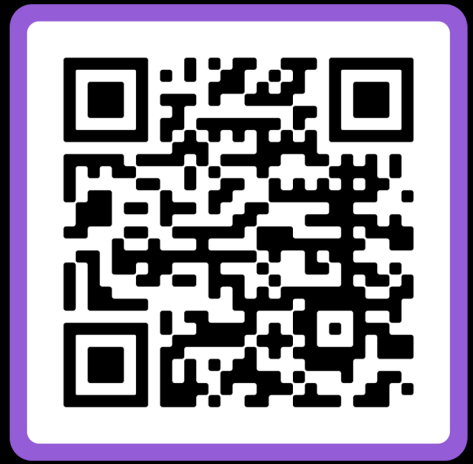
With All-US Privacy by SixFifty, you get coast-to-coast privacy coverage with a single set of customized compliance documents.

Schedule a demo Do you need to comply?

Future-proof your data privacy program

California, Colorado, Virginia, Utah, and Connecticut have all passed data privacy regulations in the past five years. As more laws pass, all new regulations will be added to your All-US Privacy subscription. At no extra cost!

Thank you!



Connect with us

on social media