



The defensibility imperative: Transforming complex DSR operations across the enterprise

Tuesday, 20 October

08:00-09:00 PDT

11:00-12:00 EST

17:00-18:00 CEST



Today's speakers



Fahad Diwan

Director of Product Marketing,
Privacy & Data Governance,
Exterro



Alan Friel

Chair, Global Data Privacy,
Cybersecurity & Digital Assets
Practice, Squire Patton Boggs



Dr. K Royal

Global Chief Privacy Officer &
Deputy General Counsel,
Crawford & Company

Exterro builds legal governance, risk, and compliance software for privacy, legal, and IT teams.

Privacy

Exterro Data Subject Rights Manager handles data subject requests from intake to audit.

E-discovery and legal hold

Teams preserve, collect, and review data for litigation.

Data governance

Teams find, classify, and manage the data they hold.

1

Welcome and introductions

Fahad Diwan, Exterro

2

The legal landscape

Alan Friel, Squire Patton Boggs

3

Operationalizing data subject rights inside the enterprise

Dr. K Royal, Crawford & Company

4

Building a defensible DSR program

Fahad Diwan, Exterro

5

Audience Q&A

All speakers



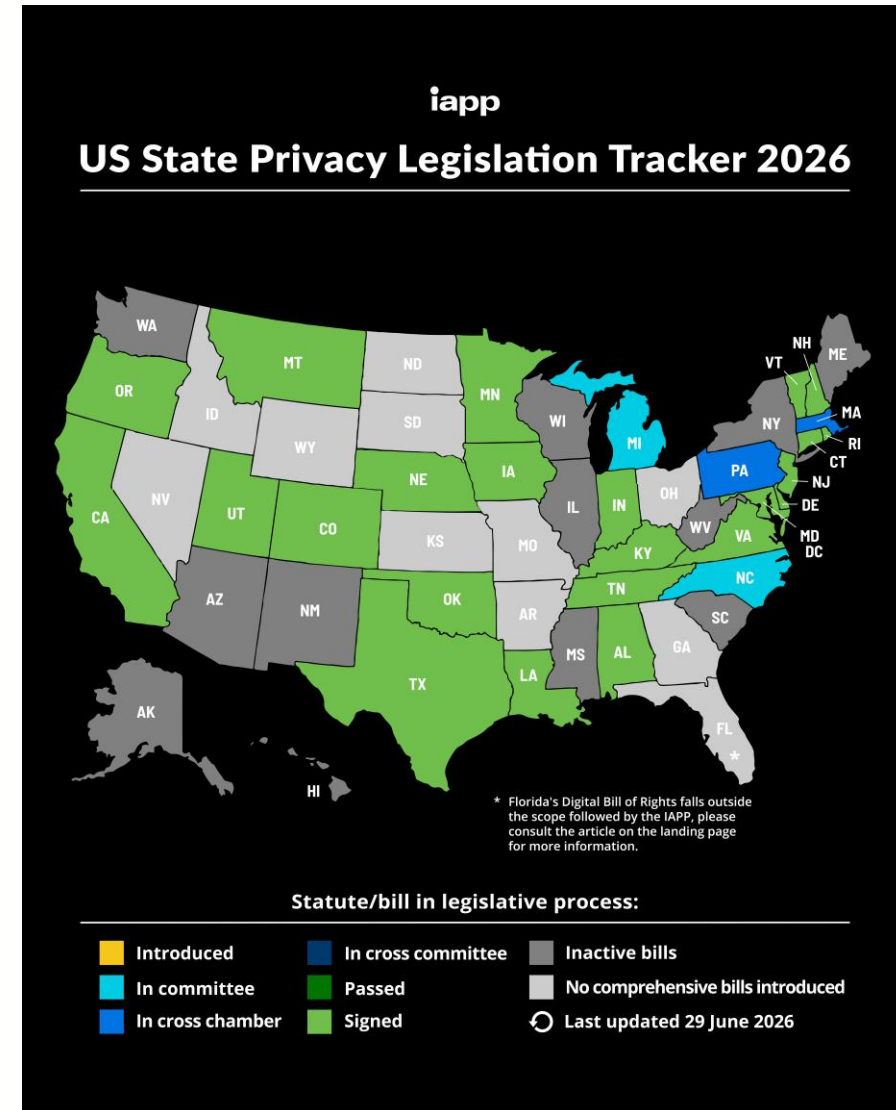
The legal landscape

Alan Friel

Squire Patton Boggs

State Consumer Privacy Laws

- **24** states have enacted omnibus privacy laws
- **20** in effect, OK, AL, LA and VT passed this year effective in 2027





What states and laws apply?

Currently Effective SCPLs

State	Consumer Privacy Law Title	Effective Date
California	California Consumer Privacy Act (CCPA)	January 1, 2020; amendments effective January 1, 2023; regulations pending
Colorado	Colorado Privacy Act	July 1, 2023
Connecticut	Connecticut Personal Data Privacy and Online Monitoring Act	July 1, 2023
Delaware	Delaware Personal Data Privacy Act	January 1, 2025
Florida	Florida Digital Bill of Rights	July 1, 2024
Indiana	Indiana Consumer Data Protection Act	January 1, 2026
Iowa	Iowa's Act Relating to Consumer Data Protection	January 1, 2025
Kentucky	Kentucky Consumer Data Privacy Act	January 1, 2026
Maryland	Maryland Online Data Privacy Act	October 1, 2025
Minnesota	Minnesota Consumer Data Privacy Act	July 31, 2025 *
Montana	Montana Consumer Data Privacy Act	October 1, 2024
Nebraska	Nebraska's Data Privacy Act	January 1, 2025
New Hampshire	Act Relative to the Expectation of Privacy	January 1, 2025
New Jersey	New Jersey Data Protection Act	January 15, 2025
Oregon	Oregon Consumer Privacy Act	July 1, 2024 **
Rhode Island	Rhode Island Data Transparency and Privacy Protection Act	January 1, 2026
Tennessee	Tennessee Information Protection Act	July 1, 2025
Texas	Texas Data Privacy and Security Act	July 1, 2024
Utah	Utah Consumer Privacy Act	December 31, 2023
Virginia	Virginia Consumer Data Protection Act	January 1, 2023

* Postsecondary institutions regulated by the Minnesota Office of Higher Education have until July 31, 2029 to comply.

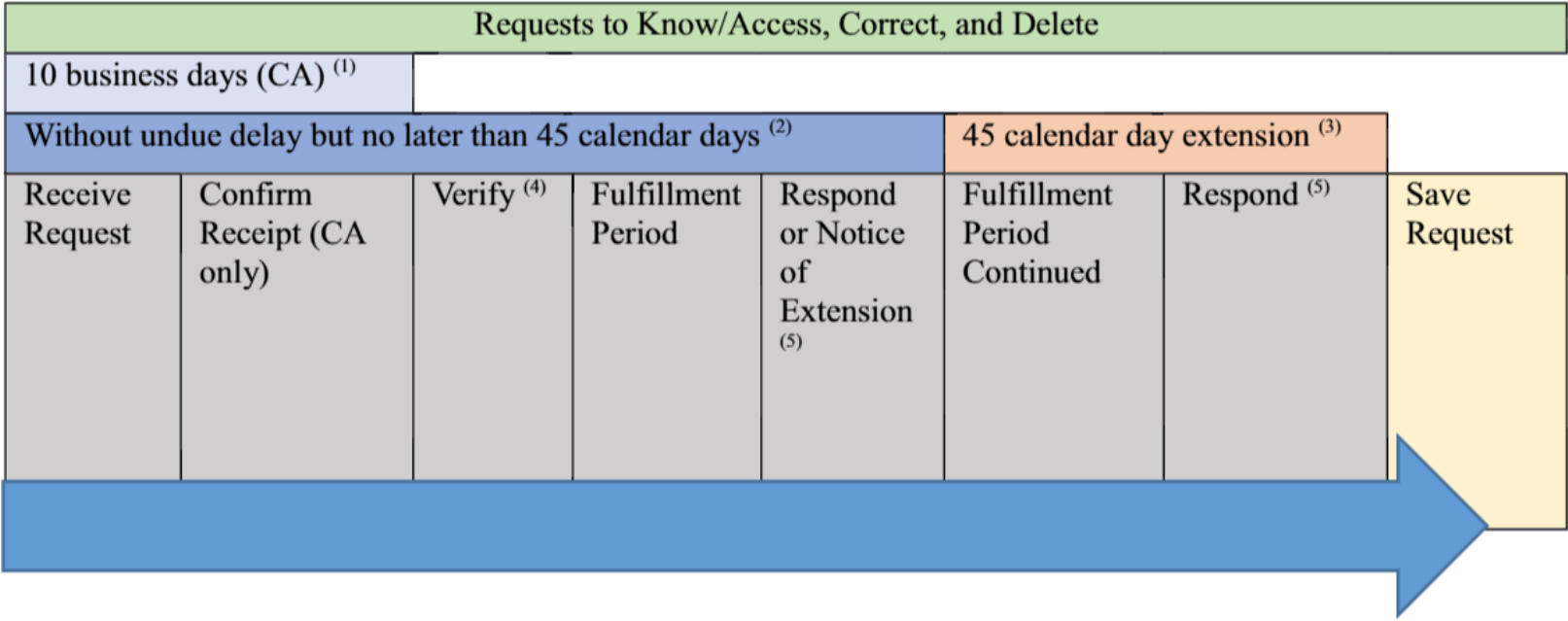
** For in-scope non-profit organizations, the effective date for OR-CPA §§1 - 9 is July 1, 2025.

- Right to **confirm whether controller is processing** the consumer's personal data and **access** the data
- Right to **correct** inaccuracies in consumer's personal data
- Right to **delete** personal data *provided by or obtained about* the consumer (varies by state)
- Right to **data portability** (provided controller not required to reveal a trade secret)
- Right to **obtain a list of (specific or categories of) third party recipients** of personal data (handful of states)
- Right to **limit the use** and **disclosure** of **sensitive personal data**
- Right to **opt-out** of the processing of the personal data for purposes of **targeted advertising** and certain **profiling**
- Right to **opt-out of sale and sharing for targeted advertising** (CA)
- Right to **opt-out / question / appeal the result of profiling** for consequential decisions
 - Some solely automated
- Right to **opt-out** of use of **automated decision-making technology** for significant decisions (CA)
 - No Human-in-the-Loop
 - No opt out if appeal right
 - Broad HR exceptions

What obligations result?

Identity Verification & Authentication

- **Timing Requirements**
 - Acknowledge receipt of the request.
 - Substantively respond within the applicable statutory timeframe.
 - Permit extensions when reasonably necessary.
 - Notify consumers if additional time is required.



Identity Verification & Authentication

- CA: Verification is required for consumer requests for information, access and copy, deletion, and correction, but notably, is not required for Do-Not-Sell/Share requests and Limit the Use and Disclosure of Sensitive PI requests. See *Honda, Todd Snyder, and Ford*.
 - A Business must verify that the requesting party is the applicable data subject, and must “establish, document, and comply with” a “reasonable” verification method.
 - A business should consider factors such as the sensitivity of the data, the potential risk of harm from unauthorized access, and the manner in which the Business interacts with Consumers.
- CO: A Controller may “authenticate” a request which means “use reasonable means to determine that a request to exercise any of the rights in Section 6-1-1306(1) is being made by or on behalf of the consumer who is entitled to exercise the rights.”
 - Applies to (1) opt out, (2) access, (3) correct, and (4) delete.
- CT: A Controller shall authenticate a request to exercise the rights to: (1) confirm processing and access PI; (2) correct inaccuracies in PI; (3) delete PI; (4) and obtain a portable copy of PI.
- UT: May authenticate a request to (1) confirm processing and access PI; (2) delete PI; (3) obtain a portable copy of PI; and (4) opt out.
- VA: May authenticate a request to (1) confirm processing and access PI; (2) correct inaccuracies in PI; (3) delete PI; (4) obtain a portable copy of PI; and (5) opt out.

What obligations result?

- **Timing & Responses:**
 - CA: confirm receipt of the request within 10 business days **and** provide information on “how the business will process the request”
 - Include a description of the verification process and the estimated time for further response.
 - May provide this confirmation in the same manner in which it received the request.
 - Verify the consumer’s identity and comply with any required disclosure or delivery within 45 calendar days of receipt (pending extensions)
- **Training:**
 - CA: Businesses that buy, receive, sell, or share for commercial purposes the PI of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA are informed of all the requirements
- **Recordkeeping:**
 - California, Colorado, and Minnesota require all businesses to maintain all records of Consumer requests as well as corresponding responses for 24 months
 - However, the statute of limitations for California AG enforcement actions is 4 years

Many state consumer privacy laws require businesses to provide consumers with an appeals process when a consumer rights request is declined, e.g., in the case of a conflict with another legal obligation or under an exemption.

Using a high-water mark approach to responding to a CRR, businesses should:

- | | | | |
|---|--|---|---|
| 1 | Inform the consumer of the request denial. | 4 | Review the appeal independently. |
| 2 | Explain the reason for denial and ability to appeal. | 5 | Respond within the applicable statutory timeframe and explain how to make a regulatory complaint. |
| 3 | Provide a mechanism to appeal. | 6 | Maintain a record of the request and response. |

Right to Delete: Scope

- Right to delete personal data about the consumer which the business has collected *[from] [about]* the consumer (California)
- Right to delete personal data *provided by* or *obtained about* the consumer (Connecticut, Delaware, Florida, Indiana, Kentucky, Nebraska, New Hampshire, Rhode Island, Tennessee, Texas, Virginia)
- Right to delete personal data *provided by* the consumer (Iowa)
- Right to delete personal data *about* the consumer (Maryland, Montana)
- Right to delete personal data *concerning* the consumer (Minnesota, New Jersey)
- Right to delete personal data *about* the consumer, including personal data the consumer *provided to* the controller, personal data the controller *obtained from* another source and *derived data* (Oregon)
- Right to delete the consumer's personal data that the consumer *provided to* the controller (Utah)

- Exceptions to Deletion Obligation
 - In some SCPLs, controller can deidentify (vs. permanently erase)
 - “A controller is not required to delete information that it maintains or uses as *aggregate or de-identified data*; provided, that such data in the possession of the controller is *not linked to a specific consumer*.” (Tennessee § 47-18-3203)
- Verification / Authentication of Deletion Request
- Contract with processor requires cooperation, including with deletion request compliance, and return/deletion of personal information after contract expires/terminates
- The California Delete Act applies to a “data broker”, which means a “business” (as defined in CCPA) that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship (Cal Civ Code §1798.99.80 et seq, as amended).
 - DROP program now in effect
 - 500k+ people have made requests

Right to Correct

- Every SCPL, excluding Iowa's, grants consumers the right to request that a covered Business / Controller correct any PI *concerning* the consumer
 - However, a Business / Controller may choose to offer Iowa Consumers such a right
- CA: applies only to individual consumer data, not household data (*i.e.*, a group of consumers cohabitating at the same residential address and sharing use of common devices or services)
 - As of January 1, 2026, a Consumer in California includes employees and individuals acting in a business-to-business context
- CA: a business may deny a consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the *totality of circumstances*
- "CA & CO: require businesses to correct the PI at issue, instruct service providers and contractors (pursuant to the written contracts) to do the same, and ensure that the information remains corrected."
- All states require an explanation to the extent a business does not honor a request

Right to Know/Access (CA)

- For PI Collected and maintained about the consumer on or after January 1, 2022, including beyond the 12-month period prior to the request (if possible):
 - The categories of personal information it has collected about that consumer.
 - The categories of sources from which the personal information is collected.
 - The business or commercial purpose for collecting, selling, or sharing that personal information.
 - The categories of third parties to whom the business disclosed that personal information.
 - The specific pieces of personal information it has collected about that consumer.
- If the business Sells/Shares or discloses PI for a business purpose:
 - The categories of personal information that the business collected about the Consumer.
 - The categories of personal information that the business sold/shared about the Consumer and the categories of third parties to whom the personal information was sold/shared.
 - The categories of personal information that the business disclosed about the Consumer for a business purpose, and for each category identified, the categories of service providers or contractors to whom it was disclosed.

Right to Know/Access (non-CA)

- Connecticut (effective July 1, 2026), Rhode Island, Minnesota, and Oregon provide for a right to know specific third parties.
 - Consumers have the right to request a list of the specific third parties to which the controller has disclosed [*sold* in CT; *sold or may sell* in RI] the consumer's PI.
 - MN & CT: if the controller does not maintain the information in a format specific to the consumer, a list of specific third parties to whom the business has disclosed any consumers' PI may be provided instead.
 - OR: the controller may choose to instead provide a list of third parties to which the controller has disclosed any personal data.
- MD & DE: require the controller to offer the right to obtain a list of categories of third parties to which the controller has disclosed the consumer's PI.
- MD: if the controller does not maintain the information in a format specific to the consumer, a list of the categories of third parties to which the controller has disclosed any consumer's personal data may be provided instead.

Right to Copy (Data Portability)

- On request, a Business / Controller must provide a verified Consumer with a copy of the PI the Business has collected about the Consumer.
- However, a Consumer could request to view it without necessarily seeking a copy.
- Information may be delivered via mail or electronically:
 - If the business provides the information electronically, “the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.”
 - If consumers have an account, disclosures and deliveries need to be available via the account.



Other Rights Issues

- Sensitive Data
- Profiling / ADMT
- Sale / Share / Targeted Advertising
- Opt-out Signals
- CIPA and ECPA Claims



Operationalizing data subject rights inside the enterprise

Dr. K Royal
Crawford & Company

Centralized or Regionalized

Common workflow, local requirements

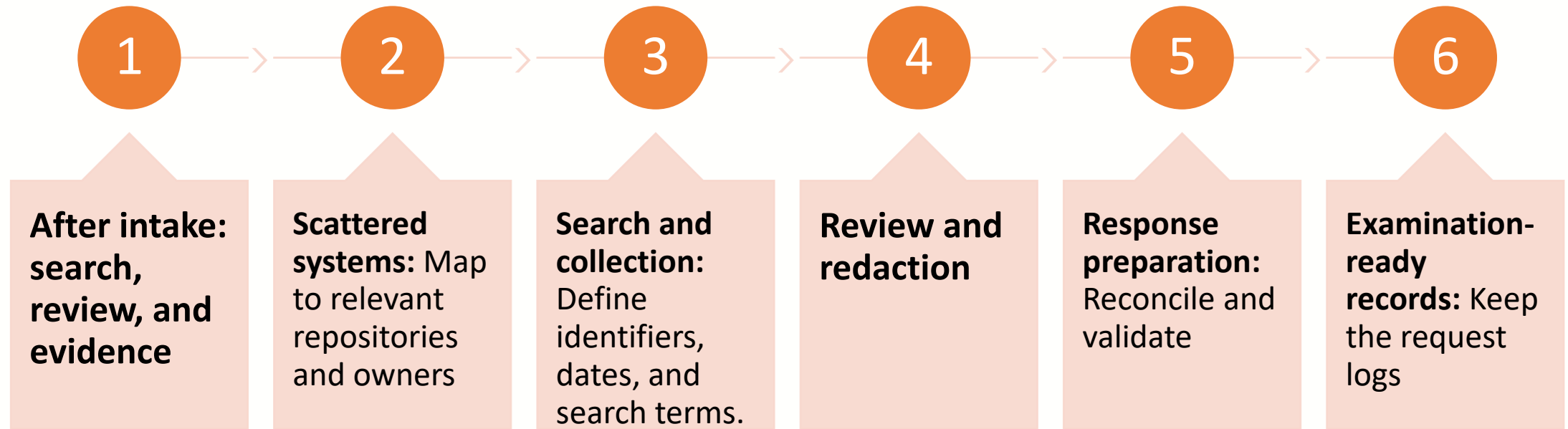
Clear accountability

Defined team roles

Upstream and downstream coordination

Shared oversight

Define the Process – Follow the Process



Employee DSRs

- Goes beyond HR file
- Carefully review for redaction material
- Coordinate grievance files, etc.
- Document



Backups



Authorities recognize the technological complexities

If in client contract, address it

If in supplier contract, address it

Keep logs to re-delete or amend as needed if restore

Backups are not archives



Building a defensible DSR program

Fahad Diwan
Exterro

Most teams can answer a request. Fewer can prove how they answered it.

Fragmented intake

Requests arrive through different forms and mailboxes for each brand.

Manual setup

Teams build backend records by hand for every request.

Risky review

Review and redaction happen in email and PDFs.

No proof

There is no single audit trail to show a regulator.

Exterro Data Subject Rights Manager carries each request through every step in one platform.

1 Intake

Branded portals for every brand, managed from one console

2 Verify

Identity verification starts when a request is submitted

3 Orchestrate

Backend records and tasks are created automatically

4 Review and redact

Inside Exterro Vault, with no export to an outside tool

5 Release and deliver

A reviewer approves every release before secure delivery

6 Delete and prove

Deletion is tracked per system and closed into the audit trail

When a regulator asks how a request was handled, the answer is already on record.

- 1 Every action is recorded**
Each step, redaction, and release is captured in the audit trail.
- 2 The record resists tampering**
Each entry is cryptographically linked to the one before it, so changes are detectable.
- 3 Nothing goes out unreviewed**
A reviewer approves every release.
- 4 Deletion is documented**
Deletion tasks are tracked for each system and closed into the record.

Questions and answers



Fahad Diwan

Director of Product Marketing,
Privacy & Data Governance,
Exterro



Alan Friel

Chair, Global Data Privacy,
Cybersecurity & Digital Assets
Practice, Squire Patton Boggs



Dr. K Royal

Global Chief Privacy Officer &
Deputy General Counsel,
Crawford & Company

Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: <https://iappwf.questionpro.com/t/AbBPvZ98ij>

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: [submit for CPE credits](#).

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

**For questions on this or other IAPP Web Conferences
or recordings please contact:**

livewebconteam@iapp.org



iapp

Appendix

Sensitive Data / Sensitive Personal Information Categories

Common categories

- Racial or Ethnic Origin
- Citizenship or Immigration Status
- National Origin
- Religious Beliefs
- Gender
- Sex Life or Sexual Orientation
- Status as Transgender or Non-binary
- Mental or Physical Health
- Medical/Health Condition or Diagnosis
- Genetic Information
- Financial Account log-in, debit card, or credit card number *in combination with* credentials permitting access to an account

GOVERNMENT ID

- Passport
- Driver's License
- Social Security number
- State Identification Card
- Other Gov't ID



PERSONAL DATA OF/FROM A KNOWN CHILD (UNDER AGE 13)



BIOMETRIC DATA

- Finger or Hand Print
- Voice Print
- Retinal Scan
- Other Unique Biological Patterns or Characteristics
- ... when used to individually identify



GEOLOCATION INFORMATION

Precise/Specific (generally within 1,750 feet (1,850 feet in CCPA))

Opt-in vs. Opt-out Consent

- **Opt-in to Sensitive Personal Information Processing**
 - Most of the SCPLs require opt-in consent but California, Iowa and Utah allow opt-out consent
- **Opt-out of Sale of Personal Data**
 - Maryland SCPL *prohibits* sale of sensitive personal data
 - Sale is an exchange of personal data for monetary or other valuable consideration *except* in Indiana, Iowa, Kentucky, Tennessee, Utah and Virginia
- **Opt-out of Targeted Advertising**
- **Opt-out of Profiling** in furtherance of decisions (or solely automated decisions in some of the SCPLs) that produce legal or similarly significant effects concerning a consumer
 - not in Iowa, Utah

- Maryland: Prohibits the sale of Sensitive PI.
 - Also prohibits the collection, processing, or sharing of Sensitive PI, except where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer.
- Oregon: Prohibits the sale of two specific types of Sensitive PI:
 - (i) PI that pertains to a consumer under the age of 16 or
 - (ii) PI that accurately identifies a consumer's location.
- Colorado: Prohibits a business from discriminating against a consumer for refusal to provide a biometric identifier or exercising the consumer's rights
- Connecticut: Prohibits the use of a geofence to establish a virtual boundary that is 1,750 ft of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data.
- California: Prohibits a business from retaliating against consumers for exercising CCPA rights
- Multiple states prohibit any sale or processing of PI from minors

Definition

In general, “profiling” means automated processing of personal data to evaluate, analyze, or predict personal aspects relating to a natural person, including, but not limited to, their personal preferences, interests, behaviors.

(Colo. Rev. Stat. s.6-1-303(20); Conn. Gen. Stat. s. 42-515(30); Va. Code Ann. s.59.1-571.)

AI is used in profiling
but not all profiling technology is AI.

Right to Opt-out

A consumer has the right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer (**LSSE**).

LSSE includes decisions resulting in provision or denial of:

- Financial or lending
- Housing
- Insurance
- Education
- Criminal justice
- Employment
- Healthcare
- Essential goods/services

iapp Opt-Out of Sale/Share and Targeting Rights

Right to Opt-Out Sale/Share/Target

- Most state privacy laws grant consumers a right to opt-out of the sale of their personal information
 - Some for \$, some any consideration
- California additionally allows consumers to opt out of the *sharing* of their personal information for “CCBA”
- The other states apply opt-out to processing for “targeted advertising”
- States vary regarding use of Opt-out Preference Signals (OOPS) or Universal Opt Out Mechanisms (UOOM)
- Cookie challenges
- Symmetry of choice
- IAB MSPA signal program
- Opt-in for “children” / “teens”

- Universal Opt-Out Mechanisms (UOOMs) are mechanisms that allow consumers to communicate an opt-out request automatically, e.g., through a browser extension, rather than submitting individual requests.
- Browser Global Privacy Controls
 - 17 states
 - CA confirm opt out (1/1/26)
- CCPA Regs: links not required if OOPS is frictionless and compliant
- OOPS controls if there is a conflict (frictionless) or if the consumer clarifies (friction)

- If there is a conflict, a conflict notice may be given in every state. However, the states sort into four groups based on how explicitly the law authorizes a conflict notice and what constraints apply (ordered from the most prescriptive to the least restrictive):
 - **California and New Jersey* (most explicit).** California and New Jersey (in draft regulations) spell out the scenarios in which notice may be given — a conflict with a business-specific privacy setting ([§ 7025\(c\)\(3\)](#); [13:45L-5.1\(c\)\(3\)](#)), a conflict with a financial-incentive/loyalty-program condition ([§ 7025\(c\)\(4\)](#); [13:45L-5.1\(c\)\(4\)](#)), and a transaction conflict when the consumer initiates an action that requires sale/share ([§ 7028\(b\)](#); [13:45L-7.5](#)). Both California and New Jersey require the signal to be honored and impose a 12-month wait before soliciting opt-in ([§ 7026\(k\)](#); [13:45L-3.4\(f\)](#)), but both still permit three types of conflict notice as not a solicitation. How the conflict resolves depends on its type.
 - California has an additional provision that may be relied on to limit the effect of sale/share opt-outs via an OOPS or any other sale/share opt-out (e.g., ones received via the consent management platform or CRR form). [Section 7026\(h\)](#) of CCPA Regulations provides that in responding to an opt-out of sale/share request, a business may present the consumer with the choice to granularly limit the scope of the opt-out as long as a single option to opt-out of all sale or sharing of all personal information is also offered (which under § 7004 must be at least as prominent and no more burdensome than the granular carve-outs). However, by doing so, a business would lose the frictionless safe harbor benefits.
 - Alabama, Connecticut, Delaware, Maryland, Minnesota, Montana, New Hampshire, and Oregon (and Vermont, once effective) — the express conflict-notice states. These states have an express statutory provision: the controller must honor the signal but may notify the consumer of a conflict with an existing setting or loyalty enrollment and offer the chance to confirm or consent (see, e.g., Conn. Gen. Stat. § 42-520(e)(1)(B)). If the consumer does not respond, the opt-out controls — even if that ends loyalty participation. None impose a 12-month opt-in solicitation wait; opting back in need only be no easier than opting out, and no dark patterns. Alabama is a partial exception worth flagging—it does not impose a standalone duty to recognize an opt-out preference signal in the first place (that recognition requirement was removed before the Act passed), and the Act does not take effect until May 1, 2027.
- **Colorado.** Colorado permits conditioning loyalty-program participation on consent to sale/targeted advertising ([Rule 6.05](#)) but has no express conflict-notice provision, so notice is governed by its general consent and dark-pattern rules ([Rules 7.03, 7.05, 7.10](#)).
- **Texas, Nebraska, and Louisiana (silent).** These GPC states do not address conflict notices at all, so the only constraint is the general prohibition on dark patterns.

- **California Invasion of Privacy Act (CIPA) (CA Penal Code §§ 630-638.55)**
 - § 631 (Wiretapping): Prohibits the interception of an electronic communication in transit. Since one party cannot intercept its own communication, the theory is a publisher aids and abets its vendors' and partners' interception.
 - § 632 (Eavesdropping): Prohibits intentionally using an electronic device to overhear or records a "confidential communication" without consent of all parties. Often used in chatbot / customer service claims.
 - § 632.7 (Cellular / Cordless): Prohibits the interception of cellular or cordless calls, including by a party to the call, without consent.
 - § 638.51 (Pen Register/Trap and Trace): Prohibits installing devices or software processes that capture routing, addressing, or signaling information without a court order or explicit user consent.
 - **Statutory Damages:** \$5,000 per violation, or 3x actual damages
- **Compare PA (WESCA) and FL (FSCA)**
- **Defenses**
 - Substantive (e.g., not a communication / call, not a third party (i.e., agent); not routing/signal info; no interception in transit)
 - Consent; Disclose third-party access

Wiretapping Litigation:

Electronic Communications Privacy Act (ECPA)

- Crime/Tort exception overcomes 1 party consent defense
 - Criminal violations of laws
 - HIPAA/CMIA; GLBA; DOJ Bulk Data Rule; Protecting Americans' Data from Foreign Adversaries Act. (PADFAA)
 - Tort arising out of privacy deception
 - \$100 a day / \$10,000
- Courts split over the interpretation of “intercepted for the purpose of committing any criminal or tortious act”
 - Does the interception require a criminal or tortious purpose? (i.e., separate from interception)
 - Does the interception result in some form of criminal or tortious act? (i.e., not separate from interception)
- ECPA cases initially focused on more sensitive personal data, but demands have alleged that the same theory applies to tracking technologies collecting routine internet data (e.g., search history on a retail website).