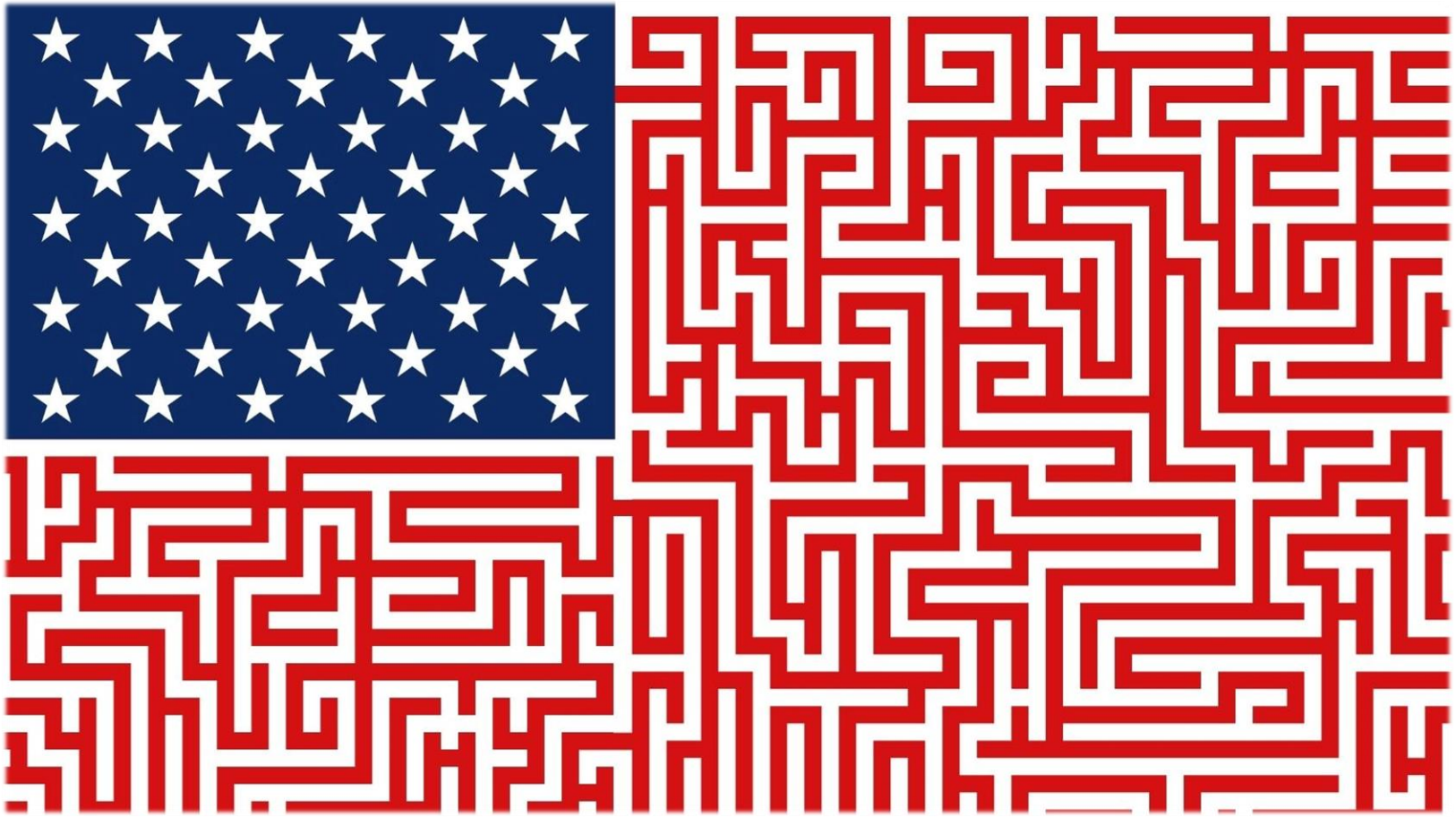
Navigating the Labyrinth of U.S. Privacy Laws: Building a Compliance Program

Ieuan Jolly
Partner, New York

Kris Ekdahl
Senior Associate, Chicago

9 November 2021



Understanding the Complexity and Risk Profile of U.S. Privacy Frameworks Compared to the GDPR

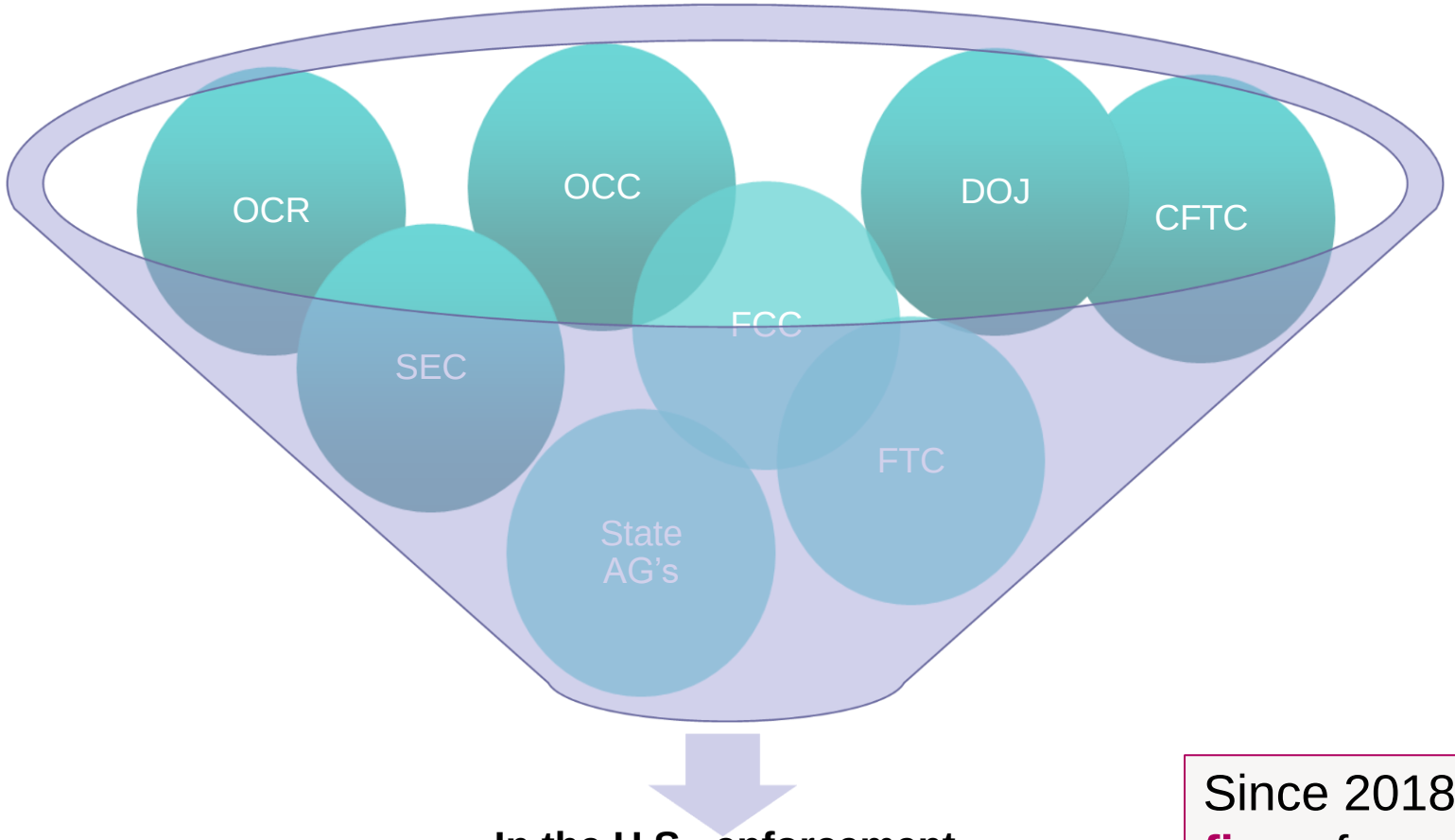
GDPR fines (up to 4% of global annual turnover) issued are typically far less than U.S. fines.

The GDPR creates a comprehensive set of privacy requirements, but the U.S. has novel features that go above and beyond the GDPR.

Class Action Lawsuits in the U.S. create a more litigious environment in which to operate.

The U.S. has many more privacy laws to navigate than the EU.

Penalties Under U.S. Privacy Laws are Consistently High



In the U.S., enforcement is brought by multiple regulators

Recent U.S. Examples:

> FTC – Facebook ($5 billion)

> CFPB / FTC / 48 State AG's – Equifax ($700 million)

> OCC – Citibank ($400 million)

> FCC – Telemarketers ($225 million)

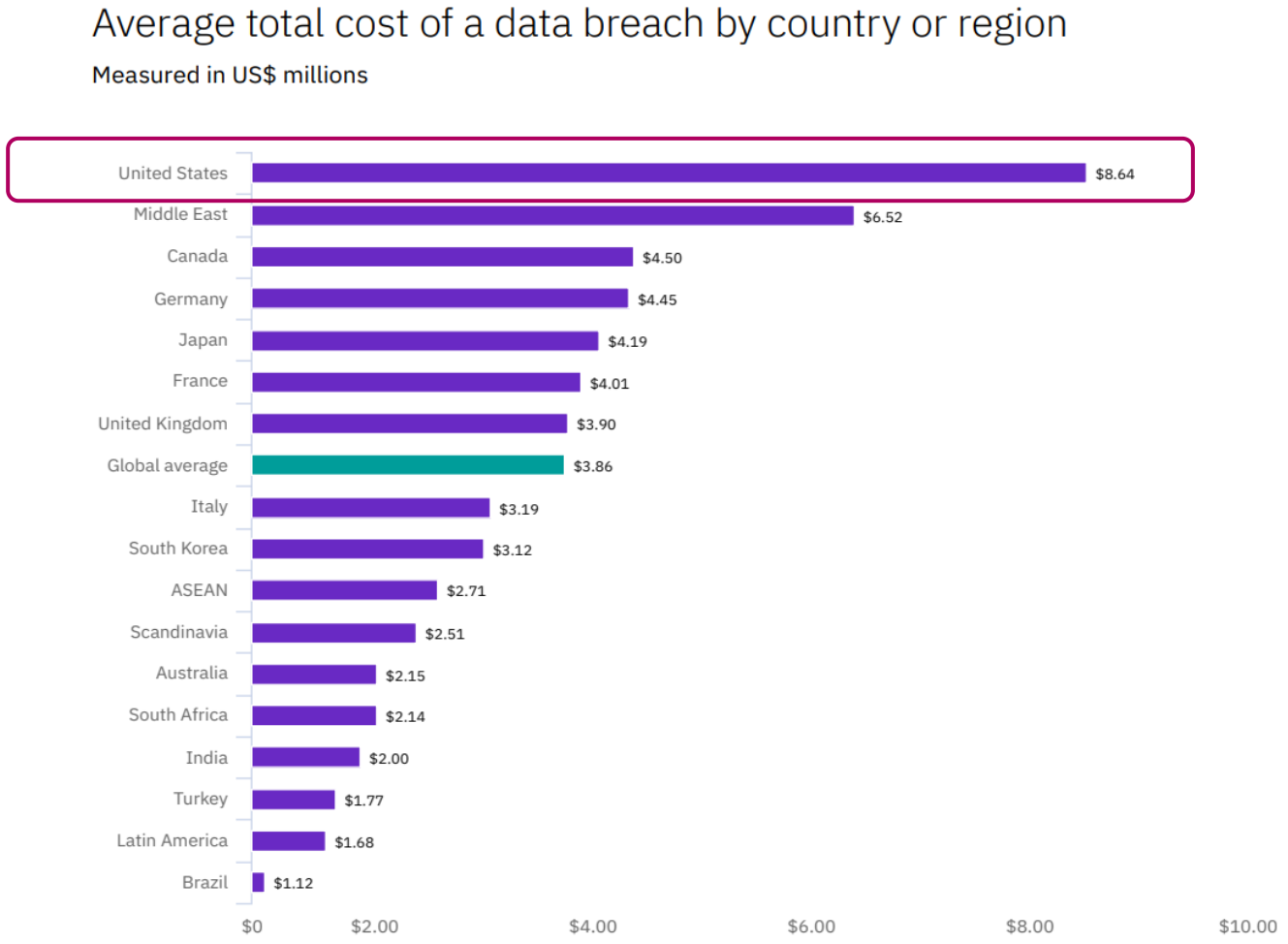
> DOJ – DISH ($210 million)

> SEC – Facebook ($100 million)

> 48 State AG's – Uber ($148 million)

Since 2018 (worldwide) **seven of the ten largest fines** for privacy and data protection breaches came from **U.S. regulators.**

Data Breaches in the U.S. are the Costliest in the World



Source: IBM Security, “Cost of a Data Breach Report 2020” https://www.ibm.com/security/digital-assets/cost-data-breach-report/

Private Lawsuits Culminating in Class Actions are Prolific in the U.S.

> The GDPR has not caused a tsunami of private litigation, as feared in 2018.

> In contrast, private litigation, in the form of class actions, is **prolific** the U.S.

$92M TikTok Privacy Deal Gets Ill. Judge's Early OK

By **Lauraann Wood**

Law360 (October 1, 2021, 9:13 PM EDT) -- An Illinois federal judge has given his early blessing to a $92 million settlement resolving biometric and other data privacy claims against TikTok and its parent company, finding the deal fair despite several objections over its value to class members.

11th Circ. Leaves Equifax Data Breach Deal Mostly Intact

By **Rosie Manins**

Law360 (June 3, 2021, 10:21 PM EDT) -- The Eleventh Circuit upheld all but one element of the $425 million settlement over the 2017 Equifax data breach Thursday over the objections of several class members, cutting only the service awards to class representatives.

Zoom Users' $85M Deal Ending 'Zoombombing' Suits Gets OK

By **Lauren Berg**

Law360 (October 22, 2021, 5:38 PM EDT) -- A California federal judge Thursday gave the initial thumbs-up to Zoom users' $85 million deal resolving privacy and data security claims against the videoconferencing provider, months after the court questioned the claims over data sharing and "Zoombombing" disruptions.

T-Mobile faces growing list of lawsuits in US over recent data breach

26 Aug 2021 | 20:38 GMT | **Insight**

By Mike Swift and Amy Miller

Since acknowledging a data breach last week that exposed the Social Security numbers, driver license numbers and other personal data of current, former and prospective customers, T-Mobile has been hit with at least 16 lawsuits in federal and state courts across the US, and the list of litigation filed against the Number 2 wireless carrier continues to grow each day.

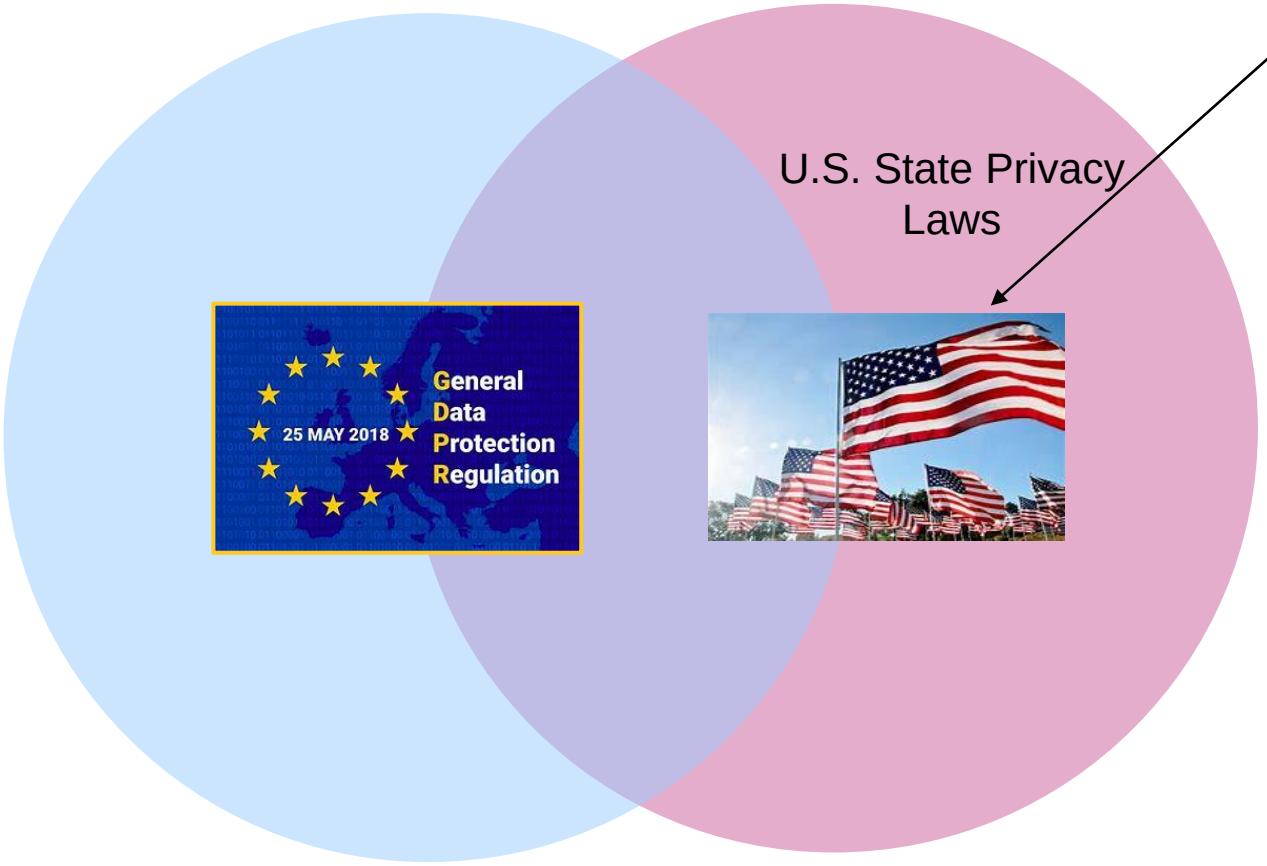
From the Atlantic to Pacific coasts in the US, T-Mobile faces an ever-lengthening list of lawsuits that claim the wireless carrier was negligent and violated state privacy and consumer protection laws by failing to prevent a data breach that exposed the personal information of more than 50 million people.

Altaba To Allot $400M To Verizon For Yahoo Settlement Appeal

By **Leslie Pappas**

Law360 (October 12, 2021, 6:39 PM EDT) -- A Delaware Chancery judge has ruled that the liquidating former owner of Yahoo Inc. must set aside $400 million to cover the appeal of a national $117.5 million class action settlement stemming from the internet provider's data breaches.

U.S. Laws Have New Requirements Above and Beyond those of GDPR



U.S. privacy law concepts that go above and beyond the GDPR:

> Right to opt-out of the "sale" of personal information *[plus a requirement to add a "Do Not Sell My Personal Information" **link** to website/apps].*

> Right to opt-out of *targeted advertising [plus a requirement to add a "Do Not Share My Personal Information for Cross-Context Behavioral Advertising" **link** to website/apps].*

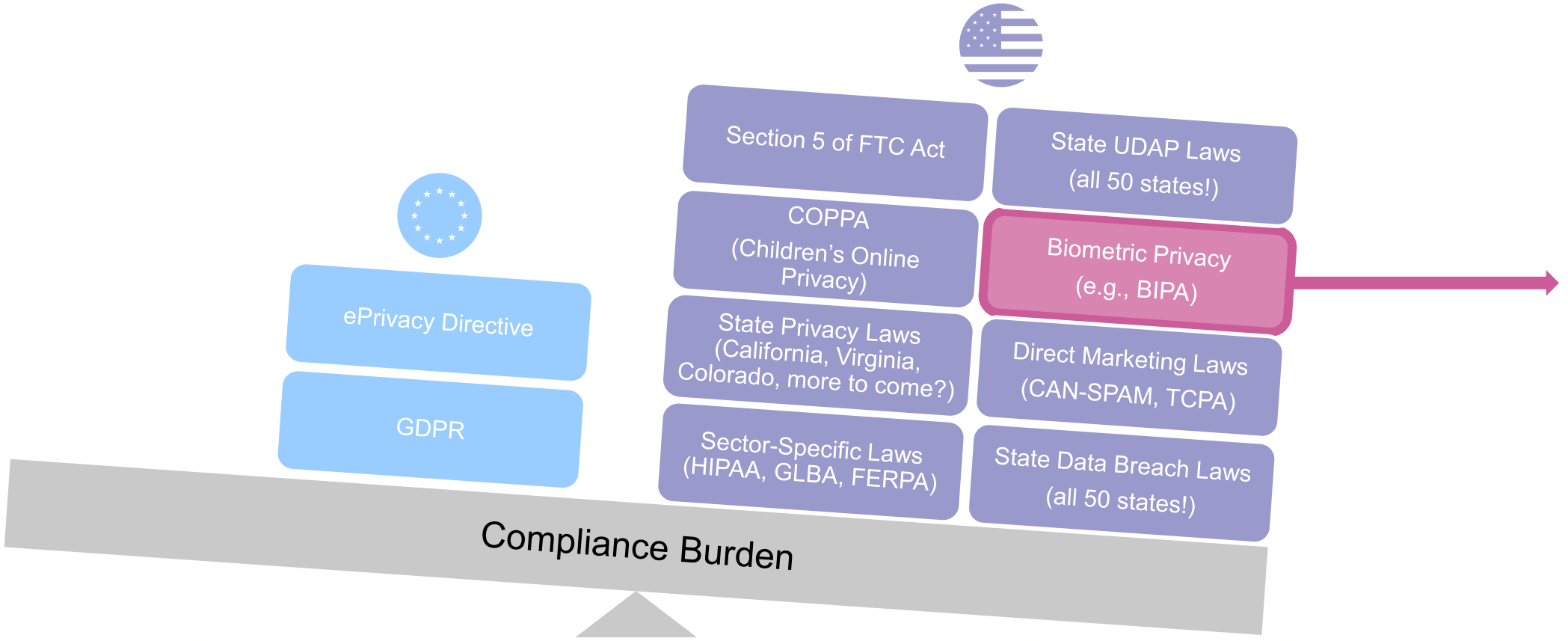
> Right to limit certain use and sharing of *sensitive personal information [plus a requirement to add a "Limit the Use of my Sensitive Personal Information" **link** to website/apps].*

> *Opt-in consent* required prior to offering financial incentives for data processing *[and prior notice detailing the key terms].*

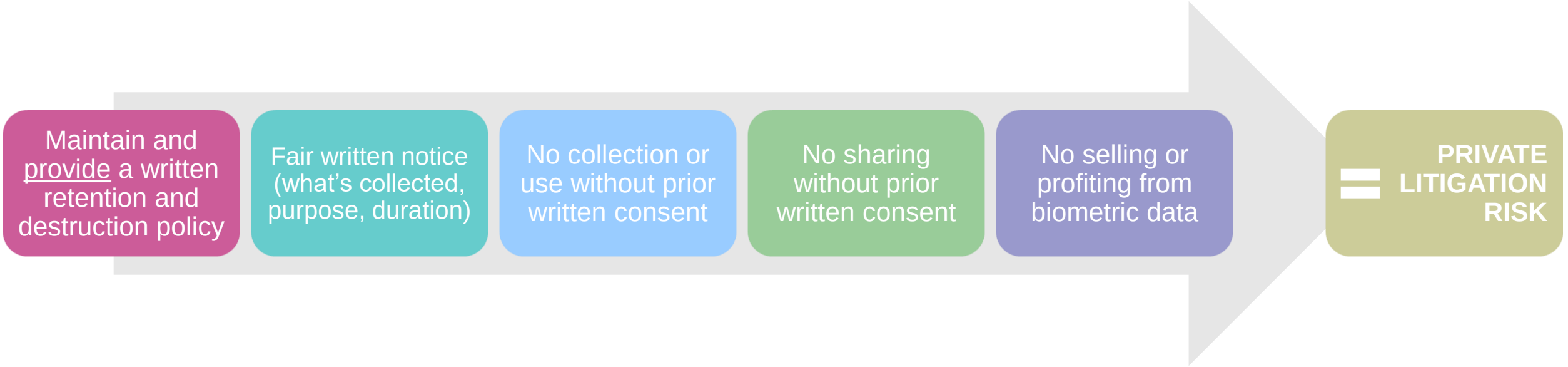
> Specific *contract language* required for *service providers*, distinct from the requirements of Art. 28.

Navigating the Labyrinth of U.S. Privacy Laws

U.S. compliance is made challenging by a dizzying patchwork of sector-specific and state-by-state laws that overlap – and sometimes conflict – with each other.



Illinois Biometric Privacy Act (BIPA)

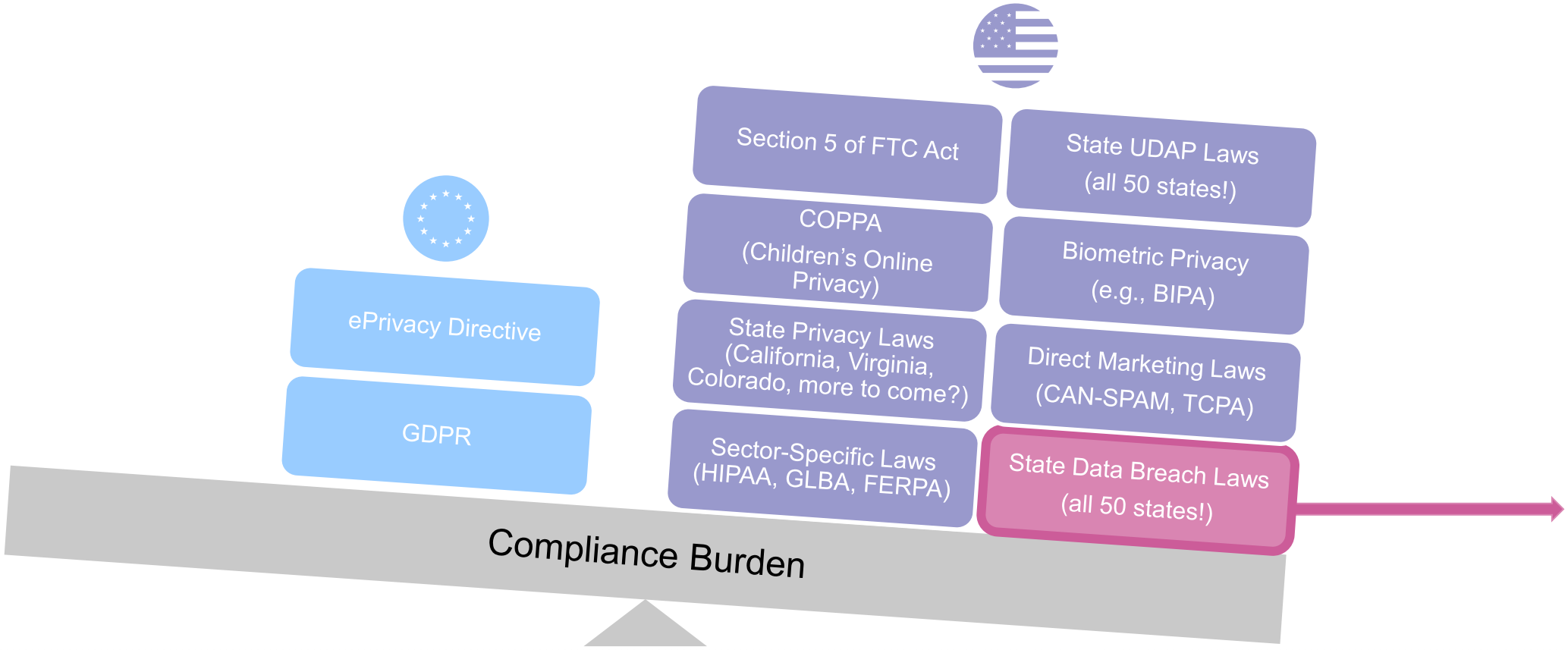


Up to $1,000 for each negligent violation, or up to $5,000 for each intentional violation

- Over 1,000 BIPA suits filed in recent years.
- Six Flags Entertainment – **$36 million** settlement with private class of plaintiffs.
- TikTok – **$92 million** settlement with private class of plaintiffs.
- Facebook – **$650 million** settlement with private class of plaintiffs.

Navigating the Labyrinth of U.S. Privacy Laws

U.S. compliance is made challenging by a dizzying patchwork of sector-specific and state-by-state laws that overlap – and sometimes conflict – with each other.



50 States, 50 Different Data Breach Laws

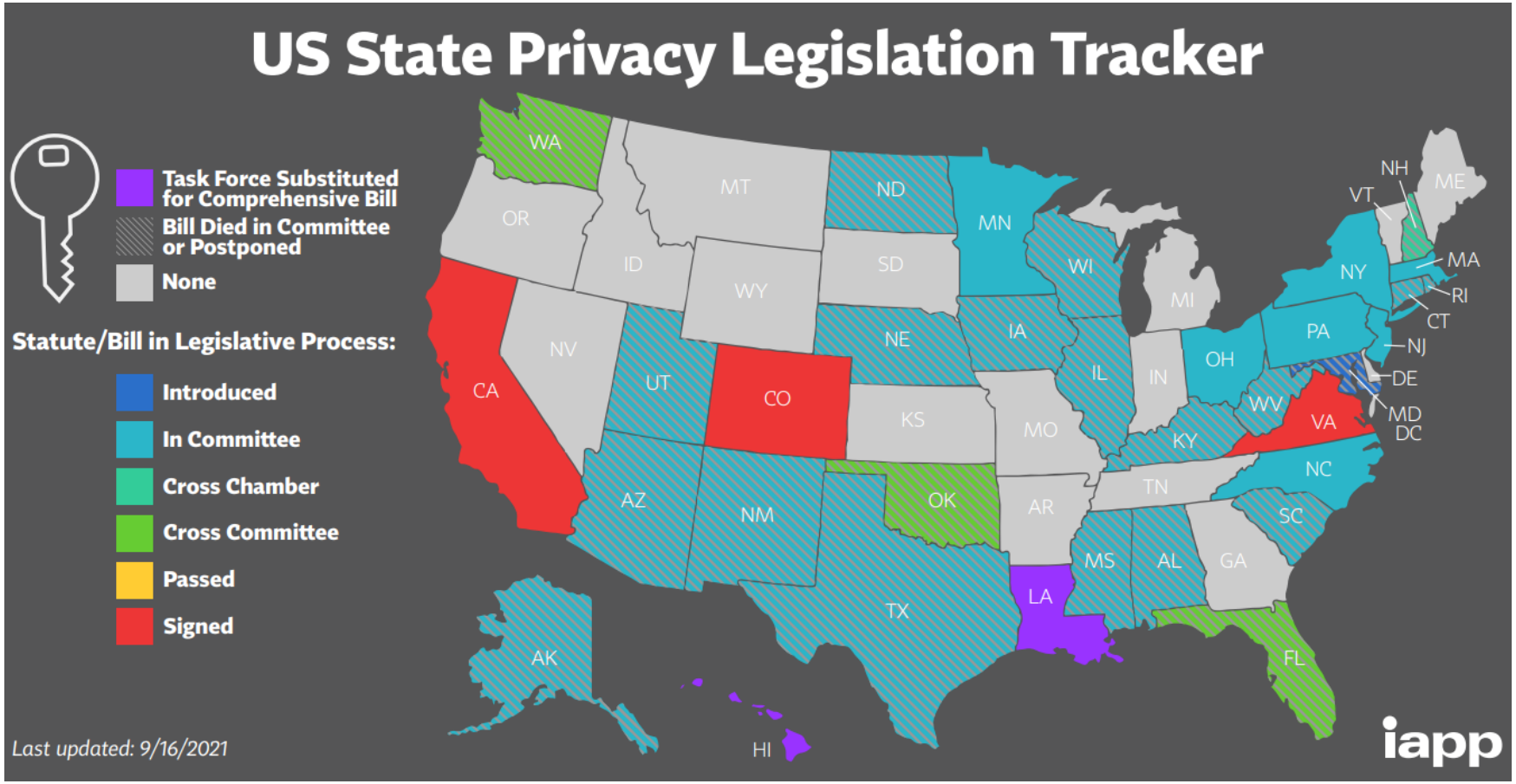
Much overlap, but important differences on a range of topics

> What types of personal information are triggering
> Acquisition vs. Access
> Notification deadlines for regulators
> Notification deadlines for individuals
> Sequencing of notifications
> Exceptions for likelihood of harm analysis
> Private right of action
> Security requirements

Comprehensive written information security program

> Designate an employee to maintain and implement WISP.
> Data mapping of all instances of personal information.
> Identify and evaluate reasonably foreseeable risks.
> Evaluate effectiveness of safeguards against those risks.
> Regular ongoing employee training.
> Disciplinary measures for violators.
> Means for detecting and preventing security failures.
> Policies for when/how records should be kept and transported.
> Protocols for terminating server/system access to employees once they are terminated or quit.
> Vetting of third-party service providers.
> Contractual requirements on third-party service providers.
> Data minimization (duration and volume).
> Data access limited by “need to know”.
> Physical security requirements (locked cabinets, key cards, etc.).
> Post-incident reviews and root cause analysis.
> Secure authentication protocols for IDs/passwords.
> Block access after multiple unsuccessful login attempts.
> Encrypt all personal information transmitted across public networks, or transmitted wirelessly.
> Encrypt all personal information stored on portable devices.
> End-point detection and active monitoring.
> Up-to-date antivirus, anti-malware, and firewall protections.

Absent a Comprehensive National Law, States are Filling the Vacuum



California Consumer Privacy Act ("**CCPA**")

California Privacy Rights Act ("**CPRA**")

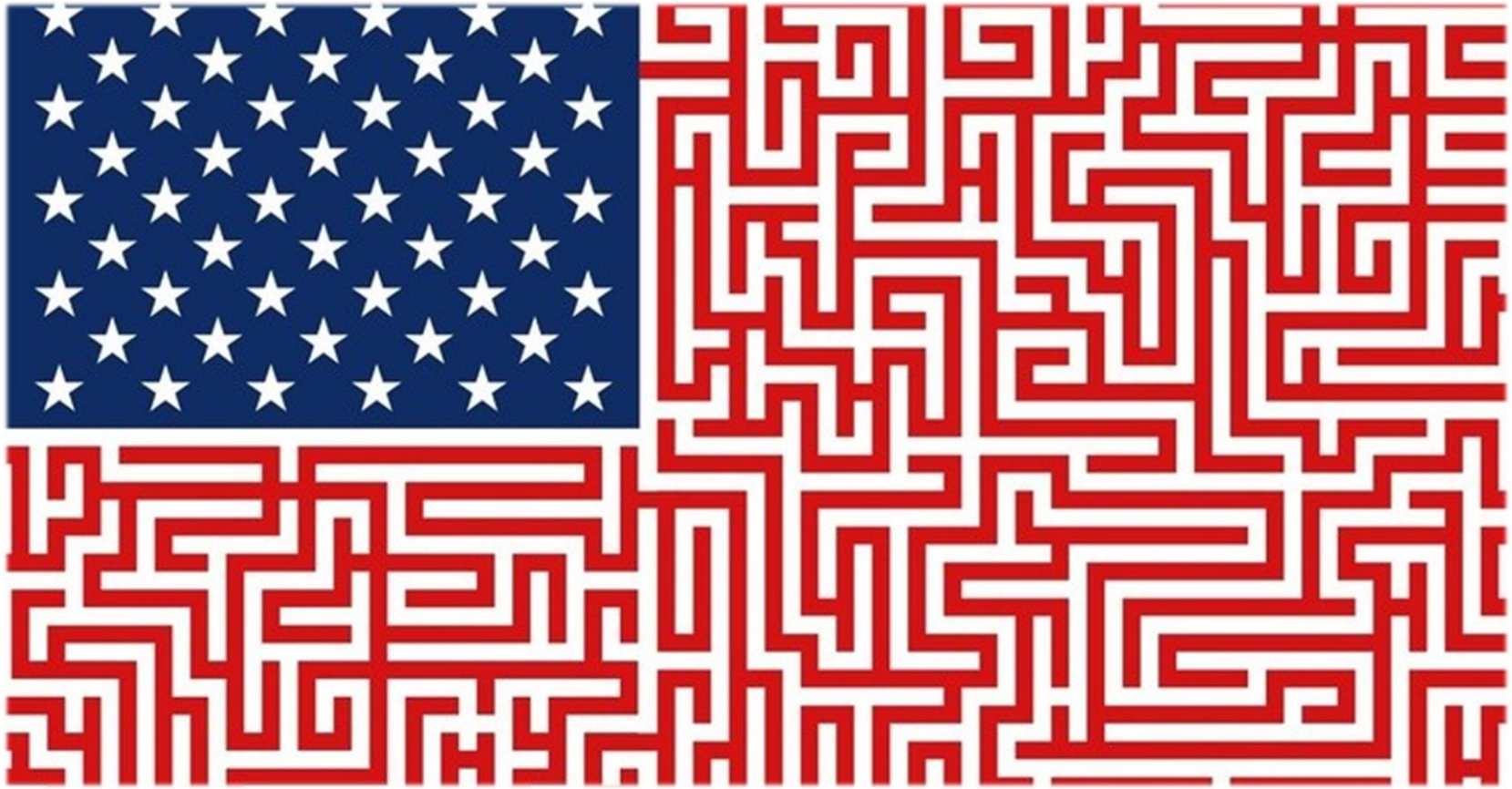
Virginia Consumer Data Protection Act ("**CDPA**")

Colorado Privacy Act ("**CPA**")

More to come soon?

Source: International Association of Privacy Professionals, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

How can Companies Navigate the Labyrinth of U.S. Privacy Laws?



Take a **single streamlined approach** based on the *highest common denominator* among the laws, and only make state-specific adjustments if a material difference would significantly lessen your compliance burden.

Foundations of a Streamlined U.S. Privacy Program

Fair Information Processing

- ❑ Special rules for sensitive personal information
- ❑ Special rules for precise geolocation data
- ❑ Profiling, automated decision-making
- ❑ Children's personal information
- ❑ De-identification (anonymization), aggregation, pseudonymization
- ❑ Financial incentives
- ❑ Non-discrimination for exercising data rights

Data Security / Data Breaches

- ❑ Requirements for specific physical, technical, and administrative safeguards
- ❑ Incident Response Plan ("IRP") / Business Continuity Plan ("BCP")
- ❑ Tabletop exercises to prepare for a data breach
- ❑ What constitutes a data breach under applicable laws (type of info, access vs. acquisition, etc.)
- ❑ Notification obligations to individuals (timing, method, content)
- ❑ Notification obligations to regulators (timing, method, content)
- ❑ Additional remediation required (e.g., credit monitoring)

Vendor Management

- ❑ Due diligence, security questionnaires
- ❑ Data Processing Agreements ("DPAs")
  - Specific security requirements
  - Usage restrictions
  - Assistance in responding to data subject requests
  - Deletion requirements at end of Term
  - Assistance in responding to governmental or regulator inquiries
- ❑ If selling personal information, no onward sales without explicit notice to consumer

Consumer Rights / Managing Requests

- ❑ Methods for submitting requests
- ❑ Verification requirements
- ❑ Deadlines to acknowledge and respond to requests
- ❑ Right of access
- ❑ Right of portability
- ❑ Right to correct
- ❑ Right to delete
- ❑ Right to opt out of sales or personal information / behavioral advertising

Consumer Choice

- ❑ Conditions for consent
- ❑ Cookie consent; cookie banners
- ❑ Direct marketing practices (privacy first; opt-in vs. opt-out)
- ❑ Opt-in for collection of sensitive personal information
- ❑ Opt-out for processing sensitive personal information
- ❑ Opt-out for sales of personal information
- ❑ Opt-out for behavioral advertising
- ❑ Opt-out for automated decision-making

Privacy Governance

- ❑ Data mapping / Data inventory
- ❑ Privacy Risk Assessments ("PRA") / Data Protection Impact Assessment ("DPIA")
- ❑ Privacy by design (data minimization, retention schedules)
- ❑ Staying current with new developments

Privacy Notices

- ❑ Notice at the point of collection
- ❑ Categories of data processed
- ❑ Purpose of processing for each category of data
- ❑ Categories of data shared with third parties
- ❑ Categories of third parties with whom data is shared (or sold)
- ❑ Consumer rights & how consumers may exercise those rights
- ❑ Annual reviews and updates

Employee Management

- ❑ Training requirements
- ❑ Testing (e.g., phishing tests)
- ❑ Binding confidentiality / non-disclosure agreements

U.S. Privacy Compliance Program: Matrix of Applicable Laws

PRIVILEGED & CONFIDENTIAL

Privacy Domain	Requirement	GDPR	California (CCPA) + (CPRA)	Virginia (CDPA)	Colorado (CPA)
Law Applicability + Key Definitions	**Law Effective Date**	May 25, 2018	CCPA already in effect; CPRA takes effect Jan. 1, 2023 (enforcement begins July 1, 2023)	Jan. 1, 2023	July 1, 2023
	Threshold for Applicability	Applies to both: (1) companies established in the EU that process PD of EU individuals, and (2) non-EU companies that process PD of EU individuals in relation to offering them goods or services, or monitoring	Either: (a) $25M in annual gross revenue; (b) processes PI of 50,000 CA residents per year [beginning Jan. 1, 2023, threshold raises to 100,000]; or (c) derives more than 50% of revenue from sales of PI	Either: (a) processes PD of 100,000 VA residents per year; or (b) derives more than 25% of revenue from sales of PD (and collects PD from at least 25,000 VA residents)	Either: (a) processes PD of at least 100,000 CO residents per year; or (b) derives revenue or receives a discount on the price of goods or services from the sale of PD (and collects PD from at least 25,000 CO
	Terminology and Types of Entities	"**Controller**" the entity that, alone or jointly with others, determines the purposes and means of the processing of PD. Art. 4(7). "**Processor**" an entity that processes PD on behalf of the controller. Art. 4(8).	"**Business**" the covered entity that, alone or jointly with others, determines the purpose and means of the processing of PI. 1798.140(c). "**Service Provider**" a for-profit legal entity that processes PI on behalf of a business and to which the business discloses a consumer's PI for a business purpose pursuant to a written contract (containing certain prohibitions). 1798.140(v). "**Third Party**" any entity that processes PI from the Business, other than the consumer, the business, or a service provider. 1798.140(w). "**Contractor**" (beginning Jan. 1, 2023) an entity to whom the business makes available a consumer's PI for a business purpose	"**Controller**" the entity that, alone or jointly with others, determines the purposes and means of the processing of PD. 59.1-571. "**Processor**" an entity that processes PD on behalf of the controller. 59.1-571. "**Third Party**" any entity that processes PD from the Controller, other than the consumer, controller, processor, or an affiliate of the processor or the controller. 59.1-571.	"**Controller**" the entity that, alone or jointly with others, determines the purposes and means of the processing of PD. 6-1-1303(7). "**Processor**" an entity that processes PD on behalf of the controller. 6-1-1303(19). "**Third Party**" any entity that processes PD from the Controller, other than the consumer, controller, processor, or an affiliate of the processor or the controller. 6-1-1303(26).
	Definition of Personal Information / Personal Data	Personal Data ("**PD**") = information relating to an identified or identifiable natural person. An identified or 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	Personal Information ("**PI**") = any information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household. PI does not include de-identified or aggregated information or publicly available information.	Personal Data ("**PD**") = any information that is linked or reasonably linkable to an identified or identifiable natural person. PD does not include de-identified data or publicly available information. 59.1-571.	Personal Data ("**PD**") = information that is linked or reasonably linkable to an identified or identifiable individual. PD does not include de-identified data or publicly available information. 6-1-1303(17).
	Covers Employee or Job Applicant Data?	Yes, and data privacy program must integrate data privacy into hiring and HR practices.	Not until Jan. 1, 2023 - though it remains possible that the CCPA exemption for employee/applicant PI will be extended by the	No, but data privacy program should still integrate data privacy into hiring and HR practices.	No, but data privacy program should still integrate data privacy into hiring and HR practices.
	Covers B2B Data?	Yes	Not until Jan. 1, 2023 - though it remains possible that the CCPA exemption for B2B PI will be extended by the California legislature.	No	No
Data Subject Rights + Data Subject Requests	**Methods for Submitting Requests**	There are no limitations on how a data subject may submit a data request, so any request made via any means could start the one-month deadline to respond. Modalities should be provided for facilitating the exercise of the data subject's rights under the GDPR. The controller should also provide means for requests to be made electronically, especially where PD are processed by electronic means. Rec. 59. Acceptable methods may include web forms, email address, toll-free phone, postal mail, or through an online account.	A business that operates exclusively online and has a direct relationship with a consumer from whom it collects PI shall only be required to provide an email address for submitting requests to know. All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number. 999.312(a). A business shall provide two or more designated methods for submitting requests to delete. 999.312(b). A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. If the business interacts with consumers in person, the business shall consider providing an in-person method. 999.312(c). A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous	A controller shall offer one or more secure and reliable means for consumers to submit a request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. 59.1-584(E). Acceptable methods may include web forms, email address, toll-free phone, postal mail, or through an online account.	A controller shall offer one or more methods for consumers to submit a request, taking into account the ways in which consumers normally interact with the controller. Controllers shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. 6-1-1306. Acceptable methods may include web forms, email address, toll-free phone, postal mail, or through an online account.
	Verification Requirements Prior to Fulfilling DSRs	A controller should use all reasonable measures to verify the identity of a data subject who requests access to PD, subject to the principle of data minimization, purpose limitation, and fairness. Rec. 64.	Businesses must verify the identity of the consumer prior to fulfilling an access request or deletion request. For requests to access specific pieces of information, the business may use the consumer's password-protected account with the business (if one already exists) or must require up to 3 pieces of matching information. 999.325(c). For deletion requests, the business shall require 2 or 3 pieces of matching information, depending on the nature of the data to be deleted. 999.325(d). If a business can't verify the requester's identity, the business may deny the request and explain the reasoning to the	A controller must use reasonable means to authenticate the identity of an individual prior to fulfilling any rights requests. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a consumer request and may request that the consumer provide additional information reasonably necessary to authenticate the consumer. 59.1-573(B)(4). If an authorized agent submits a request on someone's behalf, the business should also verify the agent's identity and confirm that such person is actually authorized.	A controller must use reasonable means to authenticate the identity of an individual prior to fulfilling any rights requests. A controller is not required to comply with a request if the controller is unable to authenticate the request, in which case the controller may request additional information reasonably necessary to authenticate. 6-1-1306(2)(d). If an authorized agent submits a request on someone's behalf, the business should also verify the agent's identity and confirm that such person is actually authorized.

Streamlining Compliance: Data Subject Rights

	CCPA (in effect)	**CPRA** (Jan. 1, 2023)	**CDPA** (Jan. 1, 2023)	**CPA** (July 1, 2023)
Right of access	X	X	X	X
Right of portability	X	X	X	X
Right of rectification		X	X	X
Right of deletion	X	X	X	X
Right to opt-out of sales	X	X	X	X
Right to opt-out of targeted advertising		X	X	X
Right to opt-out of automated decision-making		X	X	X
Right to limit to processing of sensitive personal information		X*		

Managing Consumer Rights Requests

Submission methods

> Must provide two ways for consumers to submit requests (e.g., webforms, email address, toll-free phone, postal mail, or through an online account.

> Can't require someone to create a new account just to submit a request, though.

> California: Requires a toll-free phone number if you have in-person data collection.

> California: Requires a webform as one method for "Do Not Sell" requests.

> California: **"Do Not Sell My Personal Information"/"Do Not Share My Personal Information"** links required in website footer and in privacy policy (can be combined).

> California: **"Limit the Use of My Sensitive Personal Information"** link required in website footer if you process sensitive personal information.

Deadline to respond

> **45 days** from date of request. If necessary due to complexity of the request, you may take up to an additional 45 days (for total of 90), but must provide notice and explanation to the consumer.

> California: 15 business days to honor sale opt-outs.

> California: Must acknowledge receipt of all requests within 10 business days.

Managing Consumer Rights Requests

Authentication

- Must authenticate the requester's identity through reasonable means (such as requiring two or three matching pieces of information, or using an existing password-protected account):
  - Authentication standards can scale up/down depending on sensitivity of the request.
  - Do not collect sensitive or unnecessary information in order to authenticate.
  - Do not use this information for other purposes.

Tracking

- Keep records of all requests and how you responded to them:
  - TIP: Compliance is easier if you have a process for tracking the date of receipt of a request, so as to avoid missing a deadline.
  - TIP: Many businesses have template communications to streamline the process.

Access and Portability Rights

You must give consumers the ability to:

1. **Confirm whether you are processing their personal information**
   - > Access to specific pieces of personal information;
   - > Access to the categories of personal information collected, the categories of sources the personal information was collected from, the purpose for collecting the personal information, and the categories of third parties the personal information is shared with;
   - > Upcoming: Requirement to disclose how long personal information and sensitive personal information will be kept.

2. **Obtain copies of their personal information in a portable and readily usable format**
   - > Must ensure secure transmission to avoid wrongful disclosure
     - > For instance, password-protected files
   - > Never provide copies of sensitive personal information (e.g., credit card number, passport number)
     - > Rather, just acknowledge which categories of sensitive personal information you have

Right of Rectification

Requirement to give consumers the ability to correct inaccuracies in the personal information retained about the consumer.

✔ **Tip:**	Many companies already offer this right, even though it is not legally required until 2023.
✔ **Tip:**	Create a self-service portal online to facilitate and streamline these requests.

Right of Deletion

You must give consumers the ability to request deletion of personal information that you (or your service providers or contractors) maintain about the consumer.

The deletion right is **not absolute**.* For example, you can retain personal information to the extent it is **necessary** to:

- Comply with laws or with a government investigation or court order (e.g., subpoena), or cooperate with law enforcement.
- Provide the product or service specifically requested by the consumer.
- Perform a contract to which the consumer is a party (e.g., fulfilling the terms of a warranty).
- Debug an error, or prevent / detect / protect against / respond to illegal activity or data incidents.
- Use for solely internal uses that are reasonably aligned with the expectations of the consumer and compatible with the context in which the consumer provided the information.
- (Virginia) to establish, exercise, prepare for, or defend legal claims.
- (Virginia) to take immediate steps to protect an interest that is essential for the life or safety of someone.

California: You must **"downstream"** the request to all recipients with whom you shared the personal information.

(*) **Colorado:** At present, Colorado does **not recognize any** exceptions to a deletion request, but this distinction may be changed through amendment or rule-making before the law takes effect in July 2023.

Right to Opt-Out of "Sales" of Personal Information

You must give consumers the ability to opt-out of the "sale" of their personal information

"Sale" is construed broadly as the:

exchange of personal information *[or making personal information available – Cal.]*

in exchange for monetary *[or other valuable – Cal., Col.]* consideration.

"Sales" do **not** include:

(1) transfers to a service provider or contractor who processes PI on your behalf (and is bound by specific contract language), or

(2) transfers to third parties at the specific direction of the consumer.

Consensus under CCPA that allowing third party ad cookies on your website is a sale.

CDPA and CPA have narrower definitions of "sale" so the analysis could be different, but those laws include opt-outs for Behavioral Advertising.

Cookie Consent Management

Consider implementing a cookie banner or cookie consent management platform

> Unlike in the EU, cookie banners and cookie consent management platforms are not (yet) required on your website under U.S. law.

> However, more companies are starting to add them to help with CCPA “Do Not Sell” compliance.

> Will also be helpful for operationalizing behavioral advertising opt-outs under CPRA, CDPA, and CPA.

> You need a way to block third-party ad cookies, to fully comply with Do Not Sell requests.

> It is insufficient to just refer consumers to the NAI / DAA behavioral advertising opt-out tools.

Right to Opt-Out of Cross-Contextual Behavioral Advertising

Requirement to give consumers the ability to opt out of having their personal information processed or shared for "cross-contextual behavioral advertising" / "targeted advertising"

Defined as the targeting of advertising to a consumer based on the personal information obtained from that consumer's activities over time and across non-affiliated websites / applications, to predict such consumer's preferences or interests.

New right under CPRA, CDPA, and CPA

But, general consensus is that targeted advertising is a "sale" under the CCPA and is therefore already subject to opt-out rights.

Right to Opt-Out of Profiling and Automated Decision-Making

Requirement to give consumers the ability to opt-out of profiling and automated decision-making

> Profiling is the automated processing of personal information to evaluate, analyze, or predict aspects related to a consumer's economic situation, health, personal preferences, interests, reliability, behavior, location, performance at work, or movements.

> In California, this opt-out rights applies without any sort of materiality threshold. But in Virginia and Colorado, this opt-out right only applies where the automated decision-making will produce **legal or other similar significant effects** on the person.

> In California (CPRA), you must also be prepared to provide information about your profiling activities, if requested by a consumer.

Sensitive Personal Information: New Definitions & Categories of Data

	California	Virginia	Colorado
Social security number	X		
Driver's license/passport/state ID	X		
Financial account/credit card #	X		
Precise geolocation	X	X	
Information about a child under 13		X	X
Genetic data	X	X	X
Biometric data	X	X	X
Mental or physical health diagnosis		X	X
Sexual orientation		X	X
Racial/ethnic origin	X	X	X
Religion	X	X	X
Union membership	X		
Contents of mail/email/SMS	X		
Citizenship or immigration status		X	X

Sensitive Personal Information: Opt-in vs. Opt-out

You may need opt-in consent before collecting sensitive personal information.

Virginia and Colorado (opt-in)

> Affirmative **opt-in consent** is required before collecting sensitive personal information.

> Freely given, specific, informed, and unambiguous.

California (limited opt-out)

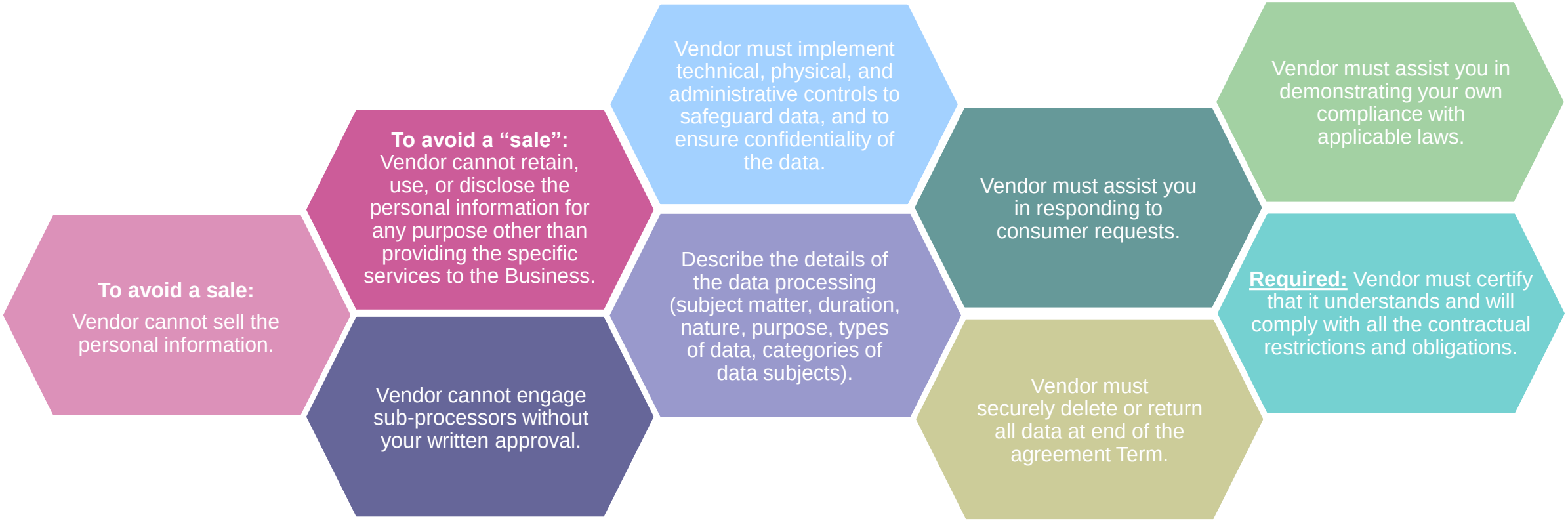
> Consumers can limit the use and disclosure of their sensitive personal information to only those uses that are "necessary" for you to provide the services or goods to the consumer (i.e., **opt-out right**).

> **"Limit the Use of my Sensitive Personal Information" link on websites and mobile apps**.

Vendor Management

You should develop a template Data Processing Agreement ("DPA") to use with any vendor that will process personal information on your behalf.

The template agreement should address the following points:



Data Retention Schedule

Requirement to implement and maintain a data retention / deletion schedule

> (California) Data retention schedule will be explicitly required under the CPRA.
>
> Privacy policy will also need to describe retention periods for each category of personal information and for each category of sensitive personal information

> Not explicitly required under CDPA or CPA.
>
> But a data retention schedule will be helpful in complying with obligations to minimize data storage and ensure secure destruction of personal information once no longer needed.

Privacy Risk Assessments / Data Protection Impact Assessments

Requirement to conduct (and document) a PRA or DPIA before undertaking high-risk data processing activities

- High-risk processing includes: (i) using personal information for targeted advertising, (ii) selling personal information, (iii) using personal information for automated decision-making, and (iv) processing sensitive personal information.
- Your PRA / DPIA should identify the benefits of the processing and weigh them against the risks, and identify measures to mitigate such risks.
- In California (CPRA), you must conduct an annual cybersecurity audit if doing high-risk processing.
- In California (CPRA), you must submit copies of PRA's / DPIA's to regulators on a regular basis.
- In Colorado and Virginia, you only need to submit copies of assessments when requested by the Attorney General.

Financial Incentives

Financial incentives must be reasonably related to the value of the consumer's personal information, and the consumer must affirmatively opt-in.

You may offer a consumer discounts, benefits, or other perks to let you collect or retain their personal information, as long as…

- The perks are reasonably related to the value of the personal information
- You provide a notice of the key terms at the point of collection or enrollment
- You obtain the consumer's prior opt-in consent
- You allow a consumer to opt-out at any time without penalty

(Compliance is driven by California. CDPA and CPA are silent on this issue).

Workstreams for Building a U.S. Privacy Program

- Consumer Rights
- Consumer Choice
- Data Security / Data Breaches
- Privacy Governance
- Privacy Notices
- Employee Management
- Vendor Management
- Fair Information Processing

IDEAS The Boston Globe

Massachusetts has a chance to clean up our national privacy disaster

A bill pending on Beacon Hill would be the most revolutionary data-privacy legislation in the United States.

By Woodrow Hartzog Updated October 7, 2021, 3:00 a.m.

April 21, 2021

North Carolina Proposes Expansive Consumer Privacy Protections

LinkedIn Facebook Twitter Send Embed

Ohio Personal Privacy Act Equips Consumers with Tools to Protect their Data

July 13, 2021

Ohio Lt. Governor Jon Husted, Director of InnovateOhio, today was joined by State Representative Rick Carfagna (R-Genoa Twp.); State Representative Thomas Hall (R-Madison Twp.); Deputy Director of InnovateOhio Carrie Kuruc; and Chair of the CyberOhio Advisory Board Kirk Herath for a press conference to announce the introduction of landmark data privacy legislation.

New York Law Journal

New York Privacy Act Makes Progress, but Hurdles Remain

In the 2021 session, the New York legislature considered no fewer than four major data protection proposals.

June 28, 2021 at 12:45 PM By F. Paul Greene

Questions?

Linklaters LLP

Ieuan Jolly

Partner, New York

Tel: +1 212 903 9574

ieuan.jolly@linklaters.com

Kris Ekdahl

Senior Associate, Chicago

Tel: +1 212 903 9415

kris.ekdahl@linklaters.com

1290 Avenue of the Americas

New York, NY 10104

Tel: +1 212 903 9000

Fax: +1 212 903 9100

Linklaters Delivering legal certainty in a changing world.

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of Linklaters LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ, England or on www.linklaters.com. This document contains confidential and proprietary information. It is provided on condition that its contents are kept confidential and are not disclosed to any third party without the prior written consent of Linklaters. Please refer to www.linklaters.com/regulation for important information on our regulatory position. Linklaters offices in the Americas are located at 1290 Avenue of the Americas, New York, New York 10104; 601 Thirteenth Street N.W., Washington, D.C. 20005; and Avenida Horácio Lafer 160, 6° andar, 04538-080 Itaim Bibi, São Paulo. Linklaters operates in São Paulo through an affiliate, LCDE (Linklaters Consultaores em Direito Estrangeiro / Direito Inglês). Attorney Advertising: Prior results do not guarantee a similar outcome.