CPRA Law + Tech: Understanding Data, Decisionmaking, and Design

February 25, 2022
Session 2

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

FUTURE OF PRIVACY FORUM

About This Series

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM

About This Series

What do privacy lawyers need to know about the **technologies and data practices** at the heart of emerging legislation? Informational webinars from Feb. 25 to Apr. 1 will bring academic, technical, and business experts to share **technological basics for privacy lawyers.**

	Topic	**Dates (2022)**
1	CPRA and Emerging US Privacy Laws	*Video available*
2	Sensitive Data: Health Conditions, Demographics, and Inferences	**Today!**
3	Basics of Online Advertising	Friday, Mar. 4
4	“Dark Patterns” and Manipulative Design	Friday, Mar. 11
5	Universal Opt-Outs and Global Privacy Controls	Friday, Mar. 25
6-7	*Coming soon!*	Friday, Apr. 1

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM

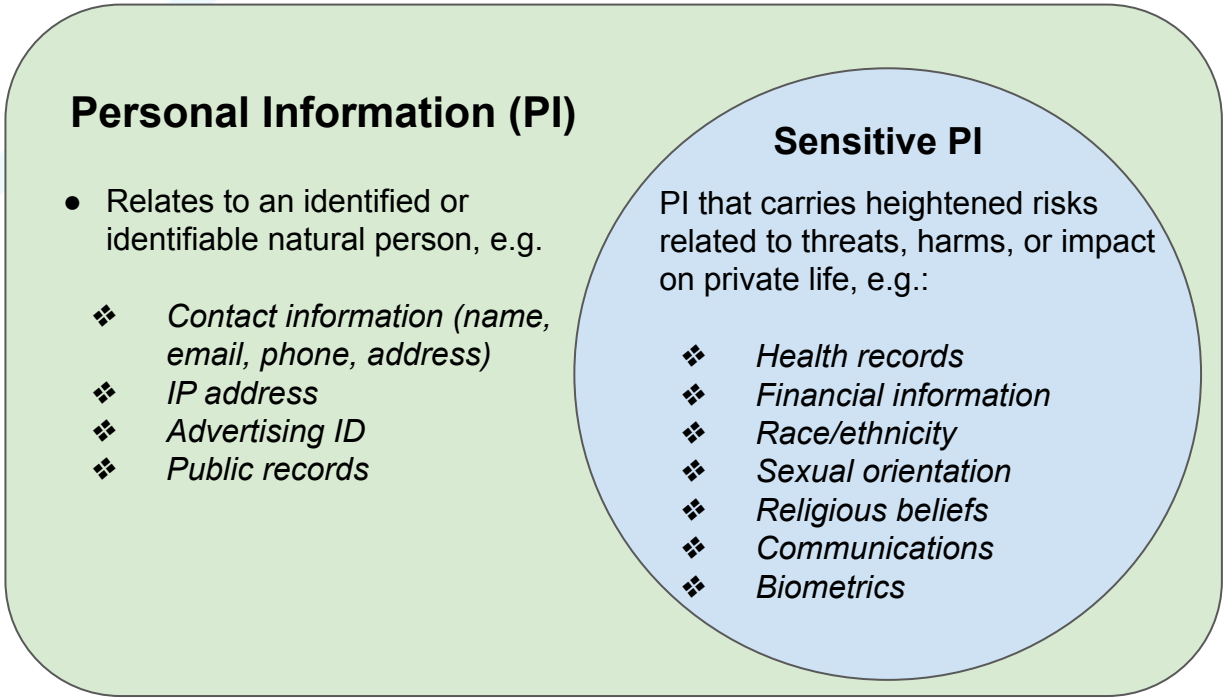
Today's Agenda

- Introduction: What is "sensitive data"?
- Emerging legislative definitions and requirements
- Case Studies: Non-HIPAA Health, Fitness, and Wellness Data
- Discussion

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM

Sensitive Data vs. Personal Data

"What's the difference?"



Non-PI

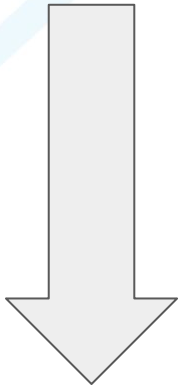
- Unrelated to persons (e.g. factory sensor data, environmental data)
- Related to groups
- Sufficiently aggregated, or anonymized (e.g. statistics)

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM

Emerging Legislative Definitions – Sensitive Data

		California Privacy Rights Act	Virginia VCDPA	Colorado CPA
	Category	**"Sensitive Personal Information"**	**"Sensitive Data"**	**"Sensitive Data"**
"personal information that reveals…" (CPRA) / "Personal data revealing…" (VA, CO)	SSN, Government ID	**Yes**	No	No
	Financial account info	**Yes,** credentials or access to	No	No
	Geolocation	**Yes** ("personal information that reveals… a consumer's precise geolocation")	**Yes** ("precise geolocation data")	No
	Racial or ethnic origin	**Yes**	**Yes**	**Yes**
	Religious beliefs	**Yes,** "religious or philosophical"	**Yes**	**Yes**
	Union membership	**Yes**	No	No
	Communications	**Yes**, content of	No	No
	Genetic data	**Yes**	**Yes**, "for the purpose of uniquely identifying a natural person"	**Yes,** "that may be processed for the purpose of uniquely identifying an individual"
and	Biometric data	**Yes,** "for the purpose of uniquely identifying a consumer"	**Yes**, "for the purpose of uniquely identifying a natural person"	**Yes,** "that may be processed for the purpose of uniquely identifying an individual"
	Health	**Yes** "personal information collected and analyzed **c**oncerning a consumer's health;	**Yes,** "personal data revealing mental or physical health diagnosis"	**Yes,** "personal data revealing … a mental or physical health condition or diagnosis"
	Sexual orientation	**Yes "**personal information collected and analyzed concerning a consumer's sex life or sexual orientation"	**Yes,** "personal data revealing . . . sexual orientation"	**Yes,** "personal data revealing … … sex life or sexual orientation"
Additional Categories	Citizenship status	No	**Yes,** "personal data revealing . . . citizenship or immigration status"	**Yes,** "personal data revealing . . . citizenship or immigration status"
	Children's data	No	**Yes,** "known child"	**Yes,** "known child"
	Marital status	No	No	No
	Political opinion	No	No	No

Legal requirements vary:



- Notice requirements - CA
- Reasonable security standards - Most/All
- “Limit use and disclosure” (Opt-Out) - CA
- Affirmative Consent (Opt-In) - VA, CO
- “Explicit Consent” - GDPR
- Prohibition (or prohibition as default) - GDPR

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM

Summaries of New Requirements – Sensitive Data

	California Privacy Rights Act	Virginia VCDPA	Colorado CPA
Summary of New Requirements	**Consumer right to direct a business, at any time, to "limit the use and disclosure of my Sensitive PI"** • … to that which is "necessary to perform the services or provide the goods reasonably expected by an average consumer … to perform the services set forth in paragraphs (2), (4), (5), and (8)* of subdivision (e) of Section 1798.140, and as authorized by regulations …" • (*security and integrity; short-term transient use (non-personalized ads); performing basic services, such as customer service or payment processing; and quality/safety") • "Sensitive Personal information that is collected or processed **without the purpose of inferring characteristics about a consumer**, is not subject to this Section, as further defined in regulations…" **New Disclosures** • categories, purposes, and whether the sensitive PI is sold or shared (at or before the point of collection) **Heightened Security** • Data sensitivity is typically a factor in assessing whether a business has violated its "duty to implement and maintain reasonable security procedures and practices **appropriate to the nature of the information** . . ." **Upcoming Regulations (1798.185) will include:** (19)(C) … determining any additional purposes … the scope of activities permitted… and "ensuring that the exemption … for sensitive personal information applies to information that is collected or processed **incidentally, or without the purpose of inferring characteristics about a consumer,** while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under Section 1798.121."	**Opt-in Consent** • "A controller shall … Not process sensitive data concerning a consumer **without obtaining the consumer's consent …**" • "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. **Data protection assessments** • "A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data: […] 4. The processing of sensitive data"	**Opt-In Consent** • "A controller shall not process a consumer's sensitive data without first obtaining consent …" • "Consent" means "a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement … The following does not constitute consent: (a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (b) hovering over, muting, pausing, or closing a given piece of content; and (c) agreement obtained through dark patterns." **Data protection assessments** • "A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities…[including] processing sensitive data."

Non-HIPAA Health

“What does non-HIPAA, non-CMIA health mean?”

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM

HIPAA Health Information

Background: Health Insurance Portability and Accountability Act

Consideration 1: Does HIPAA apply?

Applies only to "Covered Entities" ("CEs") and their "Business Associates" ("BAs"). CEs are:

(i) health plans,
(ii) healthcare providers that engage in certain electronic transactions, and
(iii) healthcare clearinghouses.

BA is a person or entity that provides services to a CE involving the use or disclosure of "protected health information" ("PHI"). A BA may not use or disclose PHI in any way that would be impermissible by the CE. A subcontractor of a BA providing services indirectly to the CE involving PHI is also subject to HIPAA.

HIPAA Privacy

Consideration 2: How can PHI be used?

Privacy Rule - Defines and limits when an individual's PHI may be used or disclosed by a CE. A CE can only use or disclose PHI either:

(i) as the Privacy Rule permits or requires; or
(ii) as the subject of the information (or personal representative) authorizes in writing.

Permitted Uses and Disclosures. - Without an individual's authorization:

(i) for Treatment, Payment, and Health Care Operations;
(ii) Incident to an otherwise permitted use and disclosure;
(iii) Public Interest and Benefit Activities; or
(iv) Limited Data Set for the purposes of research, public health or health care operations.

CE can rely on professional ethics and best judgment in deciding which uses and disclosures to make.

Confidentiality of Medical Information Act (CA)

Medical Information - Individually identifiable information, in possession of, or derived from a *provider of healthcare*, pharmaceutical company, health plan or their contractor regarding patient medical history, mental or physical condition.

Provider of Healthcare - Includes, any business organized for the purpose of maintaining medical information to make the information available to a patient OR to a health care provider (at the request of a patient or provider) to allow the patient to manage his own medical information, or diagnosis or treatment of the patient.

- A "provider of healthcare" under CMIA includes software, hardware and mobile apps and devices designed to maintain medical information for those purposes.

Case Studies: Non-HIPAA Health, Fitness, and Wellness Data

Case Study 1: Consumer health testing kits (spit, skin, blood tests)
Case Study 2: Fitness mobile app

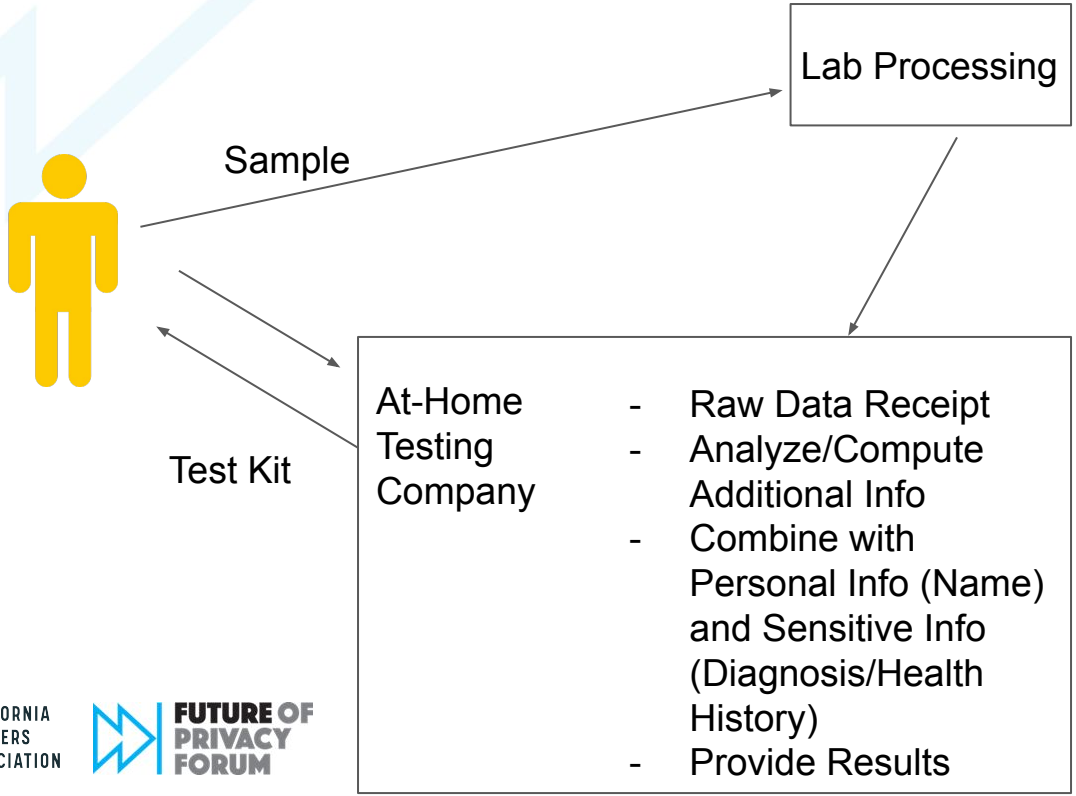
Case Study 1

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

FUTURE OF PRIVACY FORUM

At-Home Lab Testing: No Provider

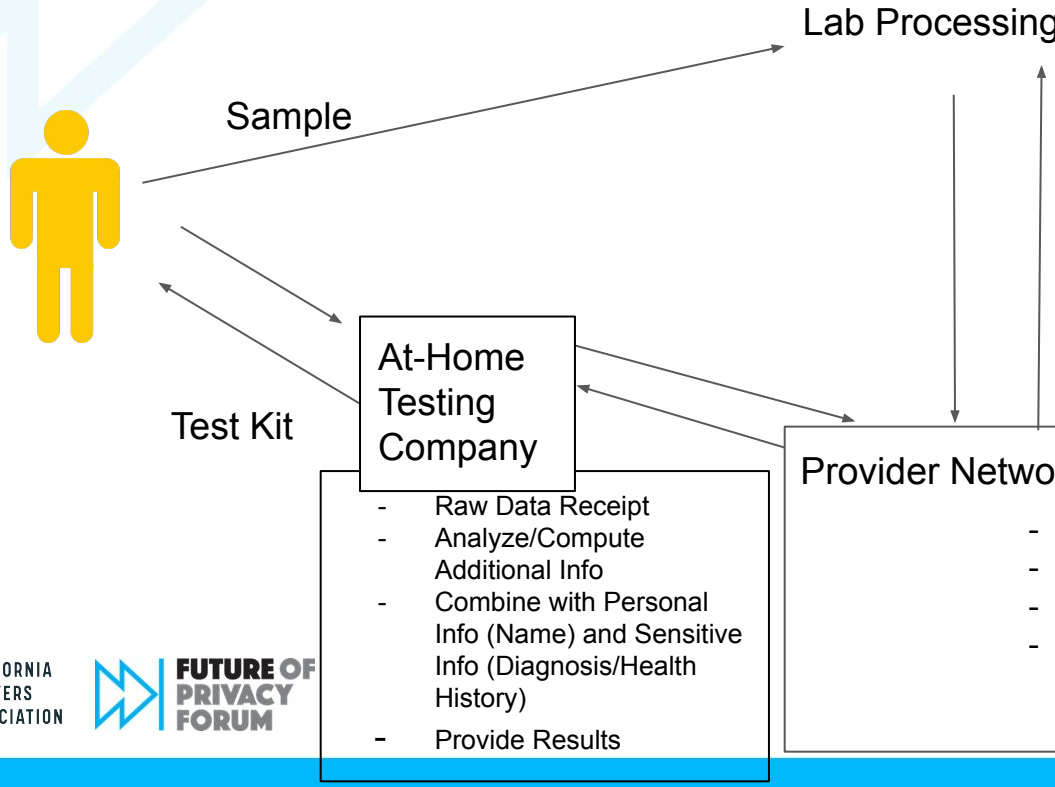


Some tests have regulatory approval/ability for direct-to-consumer ordering.

These tests are provided directly to the lab, which may or may not be subject to HIPAA.

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM

At-Home Lab Testing: With Provider



Some tests can't be ordered without a provider.

Companies often contract with a provider network to manage these tests.

Provider Network may or may not be subject to HIPAA

Case Study 2: Mobile Apps

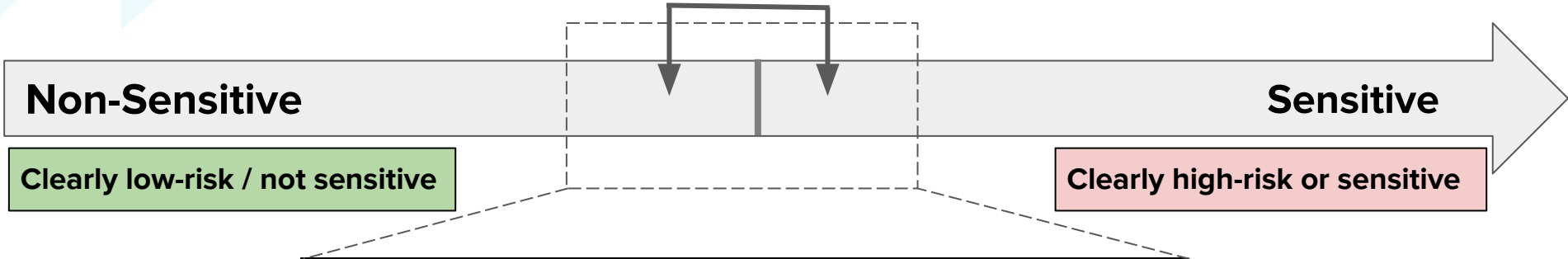
- Feature that allows users to follow or identify topics/issues of interest
- Service directed toward, but not exclusive to, a particular group of users
- Big data analytics and AI

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM

Discussion: Sensitive Data

Data that may fall into either category based on the particular **statute** (or its **interpretation)**:

- Steps, workout logs, heart-rate - when is it “concerning health”?
- “Sex life” data - what does that include?
- “Philosophical beliefs” - what is included?



Data that may fall into either category based on **context/use (and thus, may differ between covered entities)**:

- “Sensitive” → but when used for routine or non-sensitive purposes - e.g. a website URL in routine traffic; names of apps
- Non-Sensitive → but when used to make sensitive inferences - e.g. shopping purchases, device usage

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUT PRI FORUM

Discussion: Sensitive Data cnt'd

"Personal Information" includes:

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
(L) Sensitive Information

"Sensitive personal information" means: (1) personal information ***that reveals*** (A) a consumer's social security, driver's license, state identification card, or passport number; (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) a consumer's precise geolocation; (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; (F) a consumer's genetic data; and (2)(A) the processing of ***biometric information for the purpose of uniquely identifying a consumer***; (B) personal information collected and analyzed concerning a consumer's health; or (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation. Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) of Section 1798.140 shall not be considered sensitive personal information or personal information.

"Biometric information" means an individual's physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), ***that is used or intended to be used***, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

Q&A

PRIVACY LAW
CALIFORNIA LAWYERS ASSOCIATION
FUTURE OF PRIVACY FORUM