10 Topics to Make You a Data All-Star

Daniel Goldberg – *Partner, Data Strategy, Privacy & Security Group*
Rick Borden – *Partner, Data Strategy, Privacy & Security Group*

Frankfurt Kurnit Klein + Selz PC

Frankfurt Kurnit Klein + Selz PC

1. Legal landscape & enforcement priorities: Q2 2024
2. How to think about compliance across states
3. What to expect in a regulatory investigation
4. Essential terms for contracts involving data
5. What is health data?
6. Minors: children, teens & students
7. The in(put)s and out(put)s of biometric data
8. SEC cybersecurity disclosures
9. iOS privacy manifests
10. Don’t forget to register as a data broker in Texas & Oregon

1

Legal landscape & enforcement priorities: Q2 2024

Laws, Rules & Regulations	
Federal	No comprehensive data protection law FTC Act Sectoral (*e.g., COPPA, CAN-SPAM, TCPA, HIPAA, HBNR, GLBA, FCRA, VPPA, FERPA*)
State	17 comprehensive privacy laws Consumer protection laws Sectoral (*e.g., AADC, BIPA, CIPA, MHMD, SOPIPA*) Data breach and cybersecurity laws
International	*e.g., GDPR, UK Data Protection Act*
Industry	*e.g., NAI, IAB, PCI, NIST*
Platform	*e.g., iOS, Android, Chrome*
Contract	*e.g., data processing addendums*

Enforcement	
FTC	GoodRx (Feb 23); BetterHelp (Mar 23); Premom (May 23); Monument (April 24); Cerebral (April 24) X-Mode Social (Jan 24); InMarket (Jan 24); Avast (Feb 24); Kochava litigation Edmodo (May 23); Alexa (May 23); Xbox (June 23) RiteAid (Dec 23) – Biometrics, AI
California	Sephora (Aug 22) DoorDash (Feb 24) Letters Enforcement advisory – data minimization
Colorado Connecticut	Letters
Litigation	Wiretapping

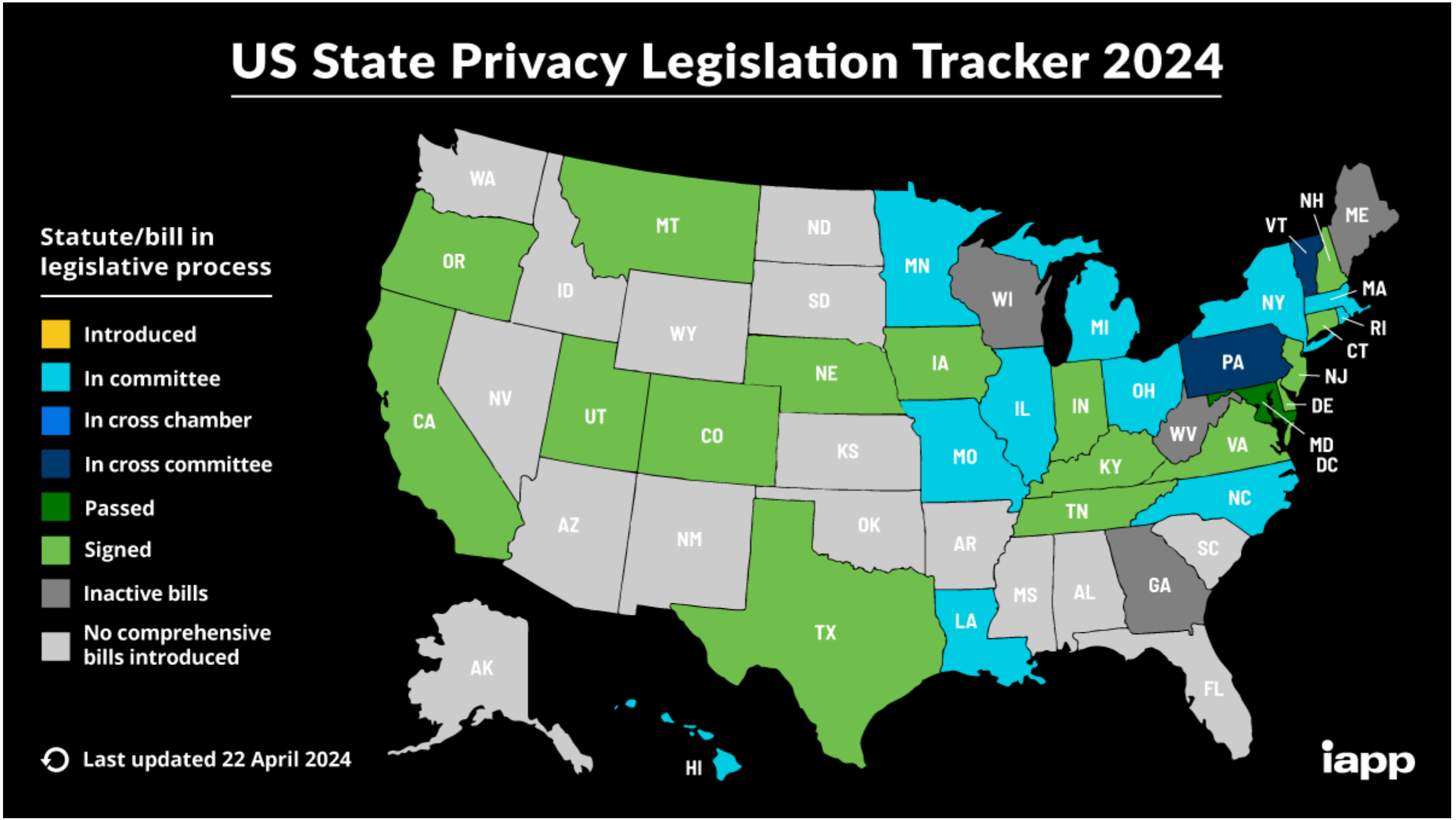
Common Topics

1. Pixels, trackers & targeted advertising
2. Health data
3. Algorithms, AI & biometrics
4. Minors – children, teens & students
5. Data brokers

2

How to think about compliance across states

US State Privacy Legislation Tracker 2024



Key Issues	
Applicability	Effective date, thresholds, exemptions, right to cure, rulemaking
Rights	Know/access/data portability, correct, delete, obtain a list of third parties, not be discriminated against, sales, shares/targeted advertising, profiling/automated decisionmaking, recognize signals, revoke consent
Contracts	Terms required
Privacy Policy	Disclosures required
Processing	Purpose limitation, data minimization, duty
Sensitive Data	Definitions, rights, secondary use restrictions
High Risk Activities	Targeted advertising, children, inferences, profiling/automated decisionmaking, financial/lending/insurance/housing, education, criminal justice, health care, essential services
Risk assessments	Requirements
Financial incentives	Loyalty programs
Security	Reasonable security, retention

3

What to expect in a regulatory investigation

How do companies get on the radar?

- Sweeps
  - Website or mobile app sweeps
  - Sector-focused (e.g., retailers)
  - Practice-focused sweeps (e.g., loyalty programs)
- Consumer complaints
- Consumer social media posts
- Data breaches
- Public reporting/investigations
- Lawsuits
- News articles

Investigatory process

- Contacted by regulator (letter, email, phone)
- Presentation of allegations
  - Initial contact
  - Formal presentation
- Opportunity to respond
  - 30, 45, 60 days
  - Consider requesting a meeting
  - Often ends here
- Investigation and remediation
  - Forensics
- Settlement
- Post Settlement

What to do if you receive a request?

- Have documentation ready – best defense is a good offense
- Immediately contact legal counsel
- Legal hold
- Develop a strategy
- Timely respond
- Don’t be antagonistic

4

Essential terms for contracts involving data

Data Processing Terms

- Controller to Processor:
  - Instructions for processing
  - Nature and purpose of processing
  - Type of personal data and duration of processing
  - Rights and obligations of both parties
  - Ensuring duty of confidentiality
  - Return or deletion obligations
  - Record keeping obligations
  - Assessment rights
  - Subprocessor obligations
  - CPRA language
  - Standard contractual clauses (where applicable)
- Controller to Controller / Third Party
  - CPRA third party language
  - Standard contractual clauses (where applicable)
  - Probably want mutual obligations
- AI/Automated Decision-making
- What is not required by law:
  - "Non-negotiable"
  - Cross-references
  - Disclaimers of liability
  - Indemnification
  - Insurance
  - Reps and warranties
- What is often negotiated:
  - Definitions
  - Audit rights
  - Authorization for subprocessors
  - Timeframes for return and deletion
  - Costs of assistance
  - Party responsible for notice and consent
  - Security obligations

Data Licenses, Use in Machine Learning

- Hedge Funds Require Detailed Due Diligence
  - Data Provenance
  - Privacy
- Data Rights
- Data De-identification

Training Data Terms

- Ownership/Licensing of “Trained” Models
- Right To Use Model Weights
- Data “Ownership”
- Personal Information
- Model Deletion

5

What is health data?

Which are protected health information (PHI)?

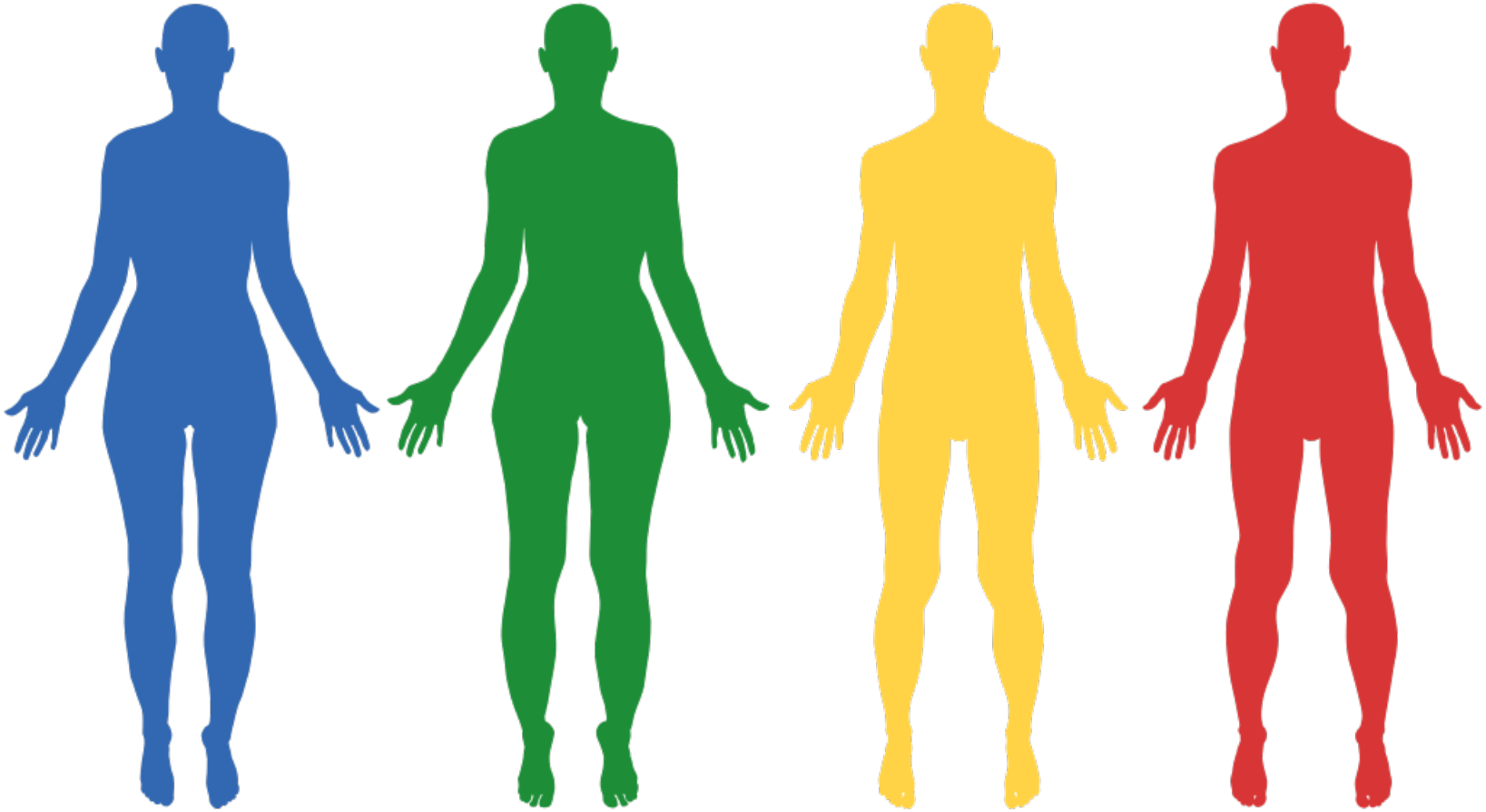
Heartrate

Sleep

Mental Health

Blood Pressure

Disability



Genetics

Medical History

Diet

Diagnosis

Disease Risk

Medications

Fertility

Clinical treatment

Sexual health

Trick question!

- Historically none unless from a covered entity under HIPAA
- But that is changing
  - Washington My Health My Data
  - Nevada Consumer Health Data Privacy Law
  - California and other comprehensive state privacy laws
  - FTC Act Section 5
  - Health Breach Notification Rule – finalized rule April 26, 2024

Definition of Consumer Health Data

- Linked or reasonably linkable to a consumer
- Identifies the consumer's past, present, or future physical or mental health status (e.g., health conditions, diagnoses, precise location, biometric data, bodily functions, such data derived from non-health data)

5: Does the definition of consumer health data include the purchase of toiletry products (such as deodorant, mouthwash, and toilet paper) as these products relate to "bodily functions"?

Information that does not identify a consumer's past, present, or future physical or mental health status does not fall within the Act's definition of consumer health data. Ordinarily, information limited to the purchase of toiletry products would not be considered consumer health data. For example, while information about the purchase of toilet paper or deodorant is not consumer health data, an app that tracks someone's digestion or perspiration is collecting consumer health data.

6: If a regulated entity or small business draws inferences about a consumer's health status from purchases of products, could that information be considered consumer health data?

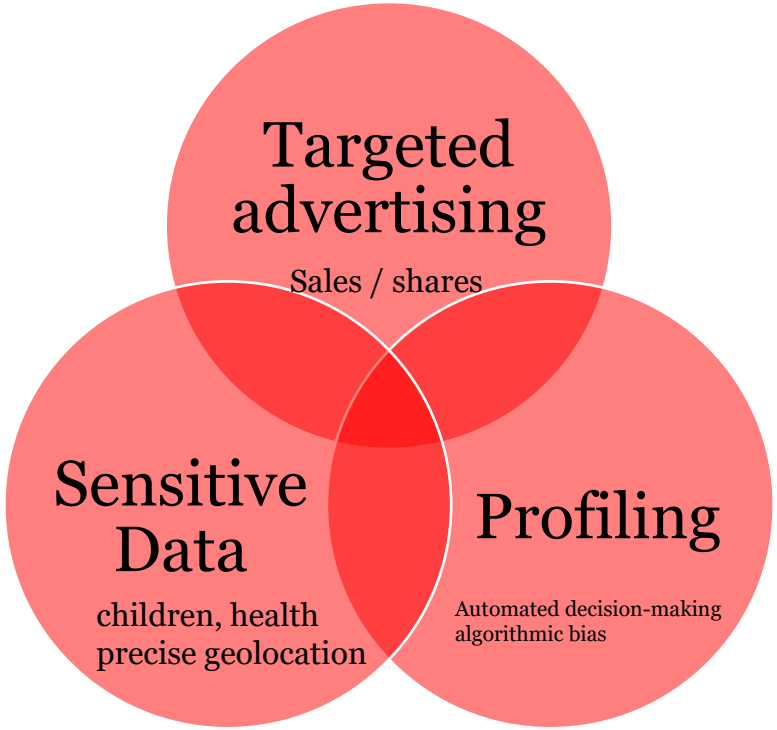
Yes. The definition of consumer health data includes information that is derived or extrapolated from nonhealth data when that information is used by a regulated entity or their respective processor to associate or identify a consumer with consumer health data. This would include potential inferences drawn from purchases of toiletries. For example, in 2012 the media reported that a retailer was assigning shoppers a "pregnancy prediction score" based on the purchase of certain products; this information is protected consumer health data even though it was inferred from nonhealth data. Likewise, any inferences drawn from purchases could be consumer health data. In contrast, nonhealth data that a regulated entity collects but does not process to identify or associate a consumer with a physical or mental health status is not consumer health data.

Why is everyone concerned?

- Washington My Health My Data
  - AG enforcement and private right of action
  - Detailed consumer health data privacy policy
  - Prohibits collection or sharing of consumer health data without opt in consent
  - Prohibits selling / targeted advertising of consumer health data without a separate authorization that satisfies the following: written and signed, specific data intended to be sold, name and contact info of purchaser, description of purpose for sale, including how gathered and used, right to revoke, expires after 1 year
- Comprehensive State Privacy Laws
  - Require opt-in consent, California requires opt-out (but could be opt-in)
- Federal
  - 5 actions within the last year relating to pixels and targeted advertising using “health data”
- Pixel litigation
  - 50+ lawsuits in the past year relating to pixels and collection of “health data”

Takeaways

- Health data is broad and includes device identifiers, inferences and hashed audiences
- Opt-in consent required – cannot be bundled as that is a dark pattern
- Recipient cannot rely on general consent
- “Anonymous” and “de-identified” standards need to be reevaluated
- Data brokers, clean rooms, etc. likely to be impacted
- May need to geo-restrict or “wait and see”



6

Minors: children, teens & students

Children

- COPPA
  - Still main law that governs collection of personal information from children under 13
  - Must obtain verifiable parental consent prior to collection unless an exception applies
  - Also requires privacy policy, parental control, security, retention limitations, not conditioning participation on more information than reasonably necessary
- NPRM (Dec. 23)
  - Declined to change “actual knowledge” standard
  - More specificity around “support for the internal operations”
  - Move to prohibit targeted advertising or profiling
- But states are also actively applying COPPA
  - Many states require compliance with COPPA
  - No safe harbor
  - Mixed audience – tracking technologies
  - Push for “constructive knowledge” standard

Teens

- Opt-in to Sales
  - Some states require opt-in to sales 13-15
  - Tricky for enforcement
- Advertising
  - Some states have restrictions around ad content shown to minors
  - SDKs
- Social Media Laws
- Age Appropriate Design Codes
- International (GDPR)
  - Defines children as under 16

Students

- Specific concerns around student data
  - FERPA (K-12) and state-specific laws
  - Edmodo FTC action
  - Vendors must
    - Only use data for purpose of providing services
    - Not engage in advertising using data

7

The in(puts) and out(puts) of biometric data

Highly Regulated

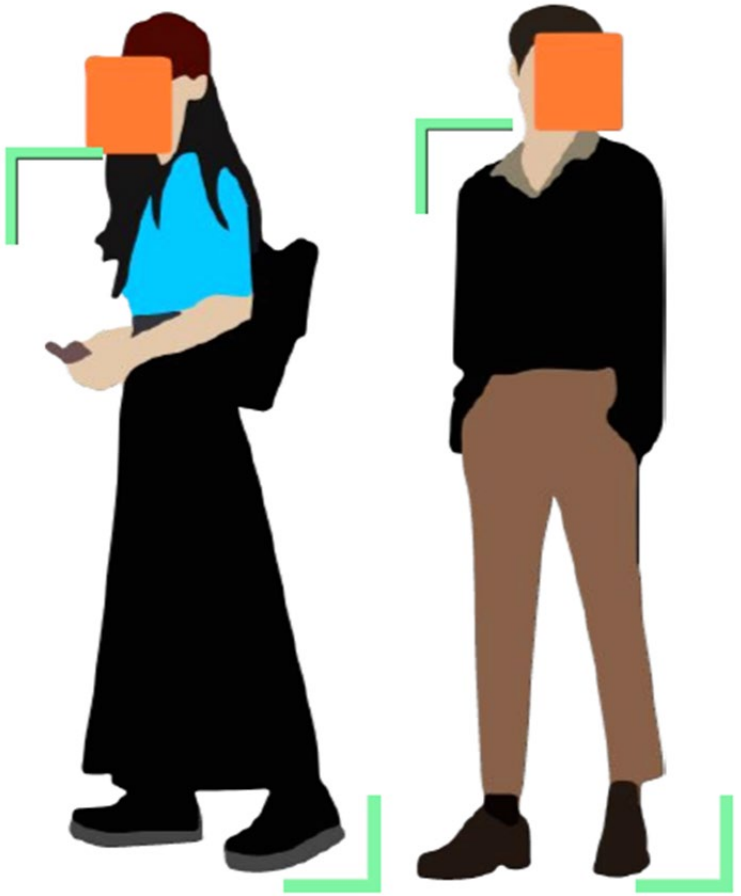
- Biometric information includes retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, gait patterns
- Often an identification component
  - "used to identify", "intent to identify", none
- Federal – FTC Section 5
- State/city laws (not comprehensive)
  - Illinois – Very high risk. Disclosures and opt-in. Private right of action – strict liability.
  - Washington – High risk. Disclosures and opt-in. Private right of action.
  - Comprehensive State Privacy Laws – High/mid risk. Disclosures and opt-in.
  - California – Mid risk. Disclosures and opt-out.
  - New York City – Mid risk. Disclosures and no sharing.

Biometrics + AI - Rite Aid (December 2023)

- 5-year prohibition on deploying facial recognition technology
- Must destroy all photos and videos of consumers collected in connection with technology, and any data, models, or algorithms derived therefrom
- Must require third parties to destroy photos, videos, and derivatives
- Must establish comprehensive information security program
- Prohibited from using any automated biometric security or surveillance system unless:
  - Establish comprehensive program to prevent substantial physical, financial, or reputational injury, discrimination based on race, ethnicity, gender, sex, age, or disability, stigma, or severe emotional distress to consumers
  - Establish procedures to provide consumers with notice and means of submitting complaints
  - Establishes a written retention schedule

Takeaways

- More AI, less facial scanning
  - Know the terms: Body movement vs facial detection vs facial recognition
  - But is it privacy safe if you don't know how the AI works?
- Must conduct due diligence to understand technology
- Expect focus on algorithmic bias



8

SEC Cybersecurity Disclosures

SEC Public Company Rules

- Reg S-K Item 1.06
  - Regulation S-K Item 106(b)
    - Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
  - Regulation S-K Item 106(c)
    - Registrants must:
      - Describe the board's oversight of risks from cybersecurity threats.
      - Describe management's role in assessing and managing material risks from cybersecurity threats.
- Item 1.05 of Form 8-K – Incidents
- 2018 Cybersecurity Guidance
- Enforcement Actions
  - Blackbaud
  - Pearson
  - First American
  - SolarWinds

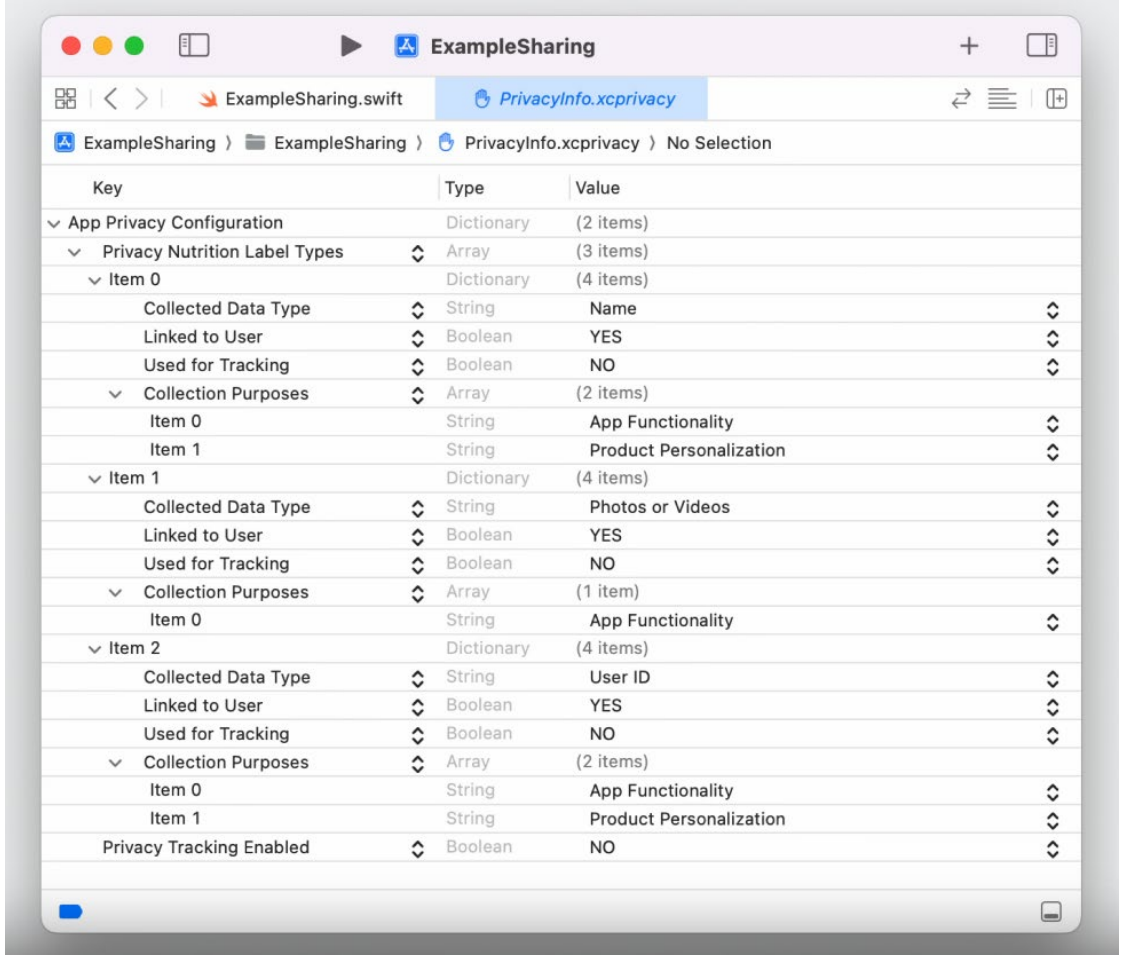
9

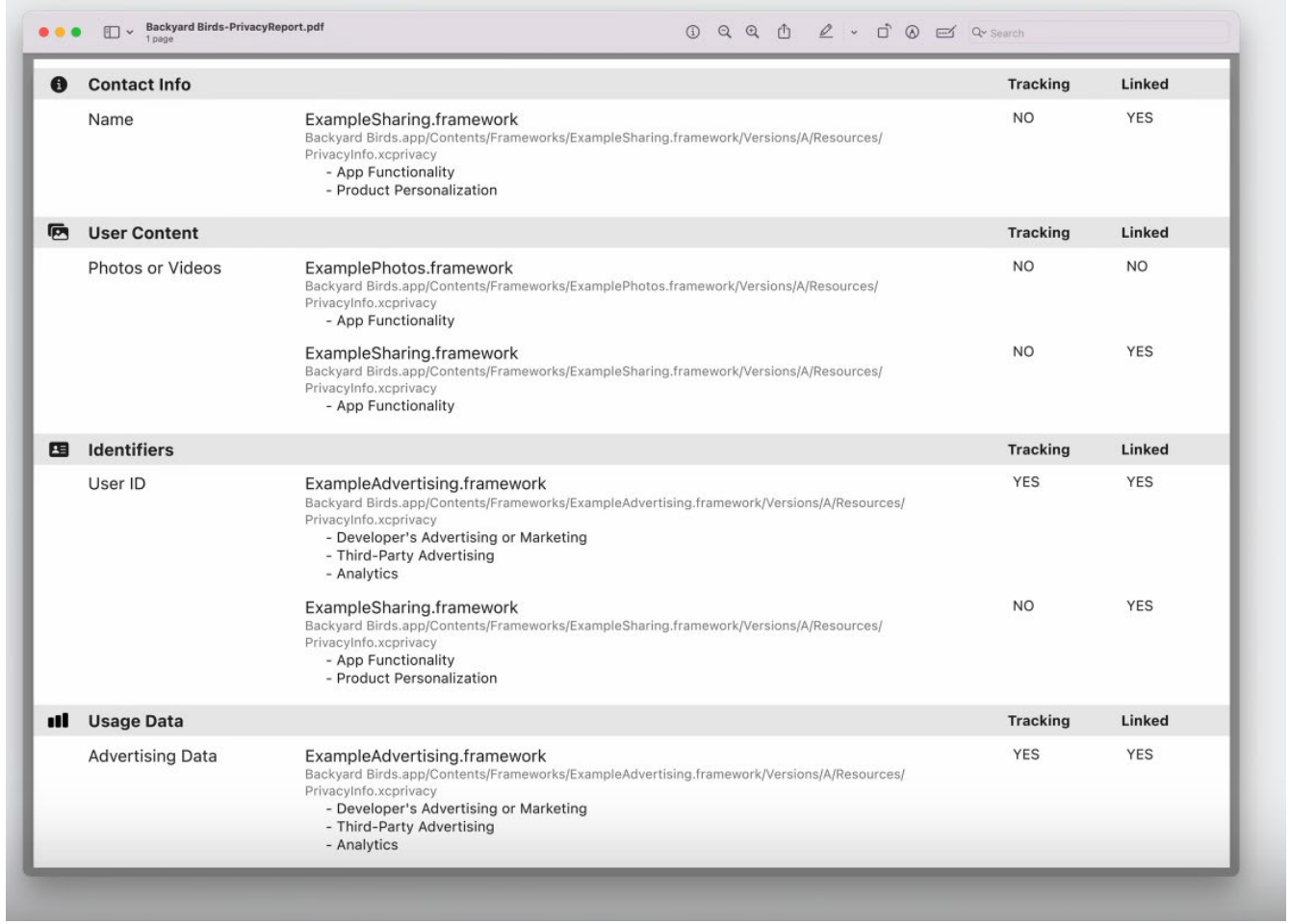
iOS Privacy Manifests

Starting in iOS 17, app developers and SDK developers can each fill out questionnaires to create **privacy manifest** files that outline their data practices. They can also include a **signature** file to verify the version.

Xcode will aggregate all privacy manifests for an app and summarize in a **report** that the app developer can review to ensure compliance and build its privacy nutrition label

iOS will automatically block / show tracking domains not specified in the privacy manifest





- Certain SDKs identified by Apple (“Privacy Impacting SDKs”) must include a privacy manifest and signature
- Certain APIs identified by Apple (“Required Reason APIs) will require the app developer to select an approved reason for using the API
- Fall 2023 - Apple said it would start checking manifests and signatures, sending informational emails
- Spring 2024 – manifests and signatures will become part of App Store review

10

Don’t forget to register as a data broker in Texas & Oregon

Texas Secretary of State
Jane Nelson

Frequently Asked Questions for Data Brokers

What is a data broker?

A business entity whose principal source of revenue is derived from the collecting, processing, or transferring of personal data that the entity did not collect directly from the individual linked or linkable to the data.

Tex. Bus. & Com. Code § 509.001.

1. Are data brokers required to register with the Secretary of State?

Yes. Section 509.005 of the Business and Commerce Code provides that a data broker must register with the Secretary of State in order to conduct business in Texas. See Form 4001 (PDF). A data broker registers by filing a registration statement with Secretary of State, which must be accompanied by the $300 registration fee. The Secretary of State will issue a registration certificate upon filing a completed registration statement.

A registration certificate is effective for one year and may be renewed by filing a renewal application with and paying the $300 renewal fee to the Secretary of State.