SQUIRE PATTON BOGGS

2022 Developments and Trends Concerning Biometric Privacy and Artificial Intelligence

Data Privacy, Cybersecurity & Digital Assets

Presenters

Kyle Fath

Partner
Los Angeles

Kristin Bryan

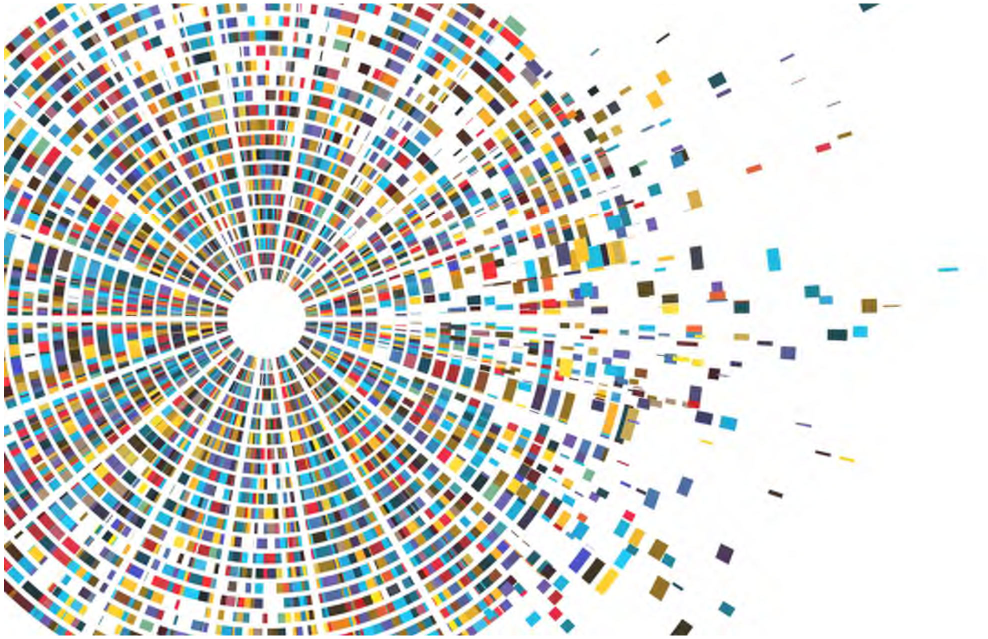
Partner
Cleveland

David Oberly

Sr. Associate
Cincinnati

Roadmap of Presentation

- Legal Requirements:
  - AI
  - Profiling
  - Other automated decision-making processes
- Litigation Landscape
- Specific State Approaches
  - Biometrics
  - Facial Recognition
- Federal Developments



SQUIRE
PATTON BOGGS

AI & Privacy Compliance

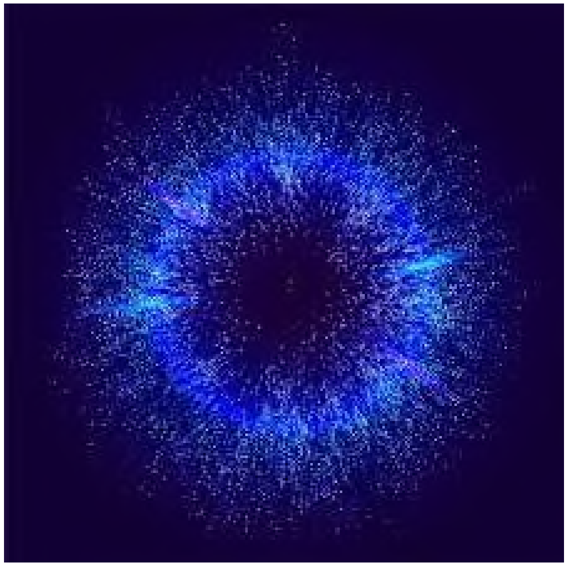
- General Data Protection Regulation (GDPR)
- California Privacy Rights Act (CPRA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)

Overview

- Use of AI in Business:
  - Quickly Process Information
  - Automate Operations and Delivery
  - 24/7 Customer Support

BUT - No Good Thing Comes Without Consequences

- Concerns:
  - Transparency
  - Explainabilty
  - Bias
  - Consumer Harm



Profiling and Automated Decision-Making

- **Profiling**
  - Automated processing
  - Of personal data/personal information
  - Evaluating/analyzing/predicting personal aspects
    - Performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
  - Does NOT necessarily involve taking action

- **Automated Decision-Making (ADM)**
  - Either solely automated, or
  - With human involvement

- **Distinction**
  - Profiling need not result in a decision
  - ADM does not necessarily include
  - Profiling

Examples: ADM and Profiling

- **Profiling:** Scoring a job applicant based on school attended

- **Solely ADM + profiling:** Auto-rejecting resumes of certain schools' graduates (or accepting resumes from only certain "target" schools)

- **Solely ADM (no profiling):** Auto-rejecting resumes of applicants less than 5 years out of college

- **ADM + Human Involvement:** Subjecting non-"target" school resumes with certain GPAs to human review before rejection or acceptance

Privacy Implications of Profiling and Automated Decision-Making

- GDPR already regulates profiling and automated decision-making

- Starting in 2023: the forthcoming privacy laws in California (Jan. 1), Virginia (Jan. 1), and Colorado (July 1) will regulate these activities

- Compliance Obligations
  - Notice/Transparency
  - Access Rights
  - DPIAs
  - Restrictions? Opt-out rights?
    - General profiling
    - Decision-making based on profiling
    - Solely ADM, including profiling

Notice/Transparency, Access Rights and DPIAs

SQUIRE PATTON BOGGS

	GDPR	CPRA*	VCDPA	CPA*
Access to meaningful logic	In privacy policy and in responses to access requests	In response to access requests (subj. to regulations)	No	No
Description of the likely outcome of the process with respect to the consumer	In privacy policy and in responses to access requests	In response to access requests (subj. to regulations)	No	No
DPIA Required?	Yes, for high risk processing generally	Yes, for high risk processing generally	Yes, for profiling that presents substantial injury to consumers	Yes, for profiling that presents substantial injury to consumers

Profiling & ADM:
Opt-Out Rights and Restrictions

	GDPR	CPRA*	VCDPA	CPA*
Profiling generally	Opt-out right	????	No opt-out right	No opt-out right
Decision-making based on profiling	Opt-out right	????	Opt-out right for profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer	Opt-out right for profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer
Solely ADM (profiling involved)	Prohibited if results in legal or similarly significant effects (subj. to exceptions)	????	Opt-out right for profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer	Opt-out right for profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer
Solely ADM (no profiling)	Prohibited if results in legal or similarly significant effects (subj. to exceptions)	????	No opt-out right if profiling not involved	No opt-out right if profiling not involved

Restrictions and Opt-Outs

GDPR	CPRA*	VCDPA	CPA*
Restriction (subj. to numerous exceptions): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Art 22(1). The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on [consent or LI] including profiling based on those provisions. Art 21(1).	“Opt-out rights with respect to businesses’ use of automated decision-making technology, including profiling” **[to be further defined in regulations].**	“To opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.” "Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.	“To opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.” "Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to essential goods or services.

CPPA’s Rulemaking

- Deadline for promulgating CPRA Regulations: July 1, 2022

- Delay announced at Feb 17 CPPA board meeting: may not have final regs until Q4 2022

- Preliminary Rulemaking Activities (completed)
    - Public comment – Sept. 22, 2021 through Nov. 8, 2021

Preliminary Rulemaking Activities on Automated Decision-Making

SQUIRE
PATTON BOGGS

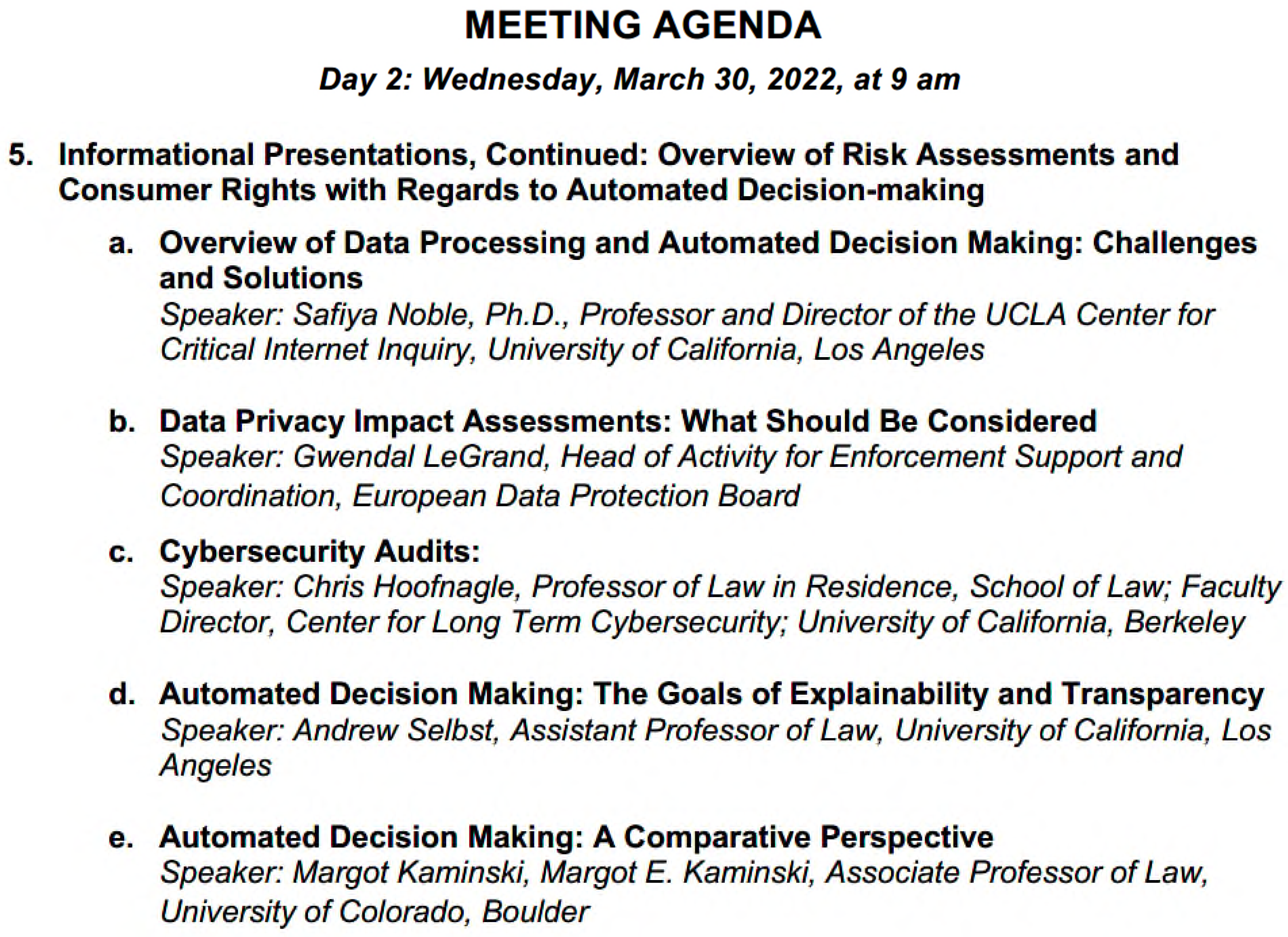
- What activities should be deemed to constitute “automated decision-making technology” and/or “profiling”?

- When consumers should be able to access information about businesses’ use of automated decision-making technology and what processes consumers and businesses should follow to facilitate access.

- What information businesses must provide to consumers in response to access requests, including what businesses must do in order to provide “meaningful information about the logic” involved in the automated decision-making process.

- The scope of consumers’ opt-out rights with regard to automated decision-making, and what processes consumers and businesses should follow to facilitate opt outs.

How will the CPPA approach ADM/profiling?



MEETING AGENDA

Day 2: Wednesday, March 30, 2022, at 9 am

5. **Informational Presentations, Continued: Overview of Risk Assessments and Consumer Rights with Regards to Automated Decision-making**

   a. **Overview of Data Processing and Automated Decision Making: Challenges and Solutions**
   Speaker: Safiya Noble, Ph.D., Professor and Director of the UCLA Center for Critical Internet Inquiry, University of California, Los Angeles

   b. **Data Privacy Impact Assessments: What Should Be Considered**
   Speaker: Gwendal LeGrand, Head of Activity for Enforcement Support and Coordination, European Data Protection Board

   c. **Cybersecurity Audits:**
   Speaker: Chris Hoofnagle, Professor of Law in Residence, School of Law; Faculty Director, Center for Long Term Cybersecurity; University of California, Berkeley

   d. **Automated Decision Making: The Goals of Explainability and Transparency**
   Speaker: Andrew Selbst, Assistant Professor of Law, University of California, Los Angeles

   e. **Automated Decision Making: A Comparative Perspective**
   Speaker: Margot Kaminski, Margot E. Kaminski, Associate Professor of Law, University of Colorado, Boulder

How will the CPPA approach ADM/profiling?

- Regulations must “further the purposes of this title”
- Regulate only final decisions?
- Separate opt-outs for automated decision-making and profiling?
- Require legal or similarly significant effects?
    - GDPR (broad – see EDPB guidance) vs. VCDPA/CPA (very narrow)
- Apply to interest-based advertising?

Takeaways

SQUIRE PATTON BOGGS

- Include profiling/ADM in employee, applicant, and other HR data mapping
  - Applicants: Even non-California-based “businesses” will have to address these issues with respect to applicants, assuming Californians can apply to job.

- Consider profiling and automated decision-making technology in other data inventory, as we wait for CPRA regs:
  - General profiling
  - Decision-making based on profiling
  - Solely ADM, including profiling
  - Solely ADM, without profiling

- Take a look at EDPB guidance on profiling and ADM

SQUIRE
PATTON BOGGS

AI & Biometrics Litigation

The current litigation landscape concerning biometric data and AI

The Illinois Biometric Information Privacy Act (“BIPA”)

- Illinois’ Biometric Information Privacy Act (“BIPA”)
- 2019 – Flood of class action litigation
  - Private right of action: $1,000 - $5,000 for **each** violation
  - *Rosenbach v. Six Flags Entertainment Corp.* (2019)
    - Illinois Supreme Court
    - Plaintiffs can collect any time an entity fails to comply
      - **Even if no actual harm or injury to plaintiff**
  - High damages + low bar => endless class action litigation
    - Seeking millions of dollars for procedural violations

Recent Trends in AI & Biometrics Litigation

SQUIRE PATTON BOGGS

- **BIPA Virtual Try-On (“VTO”) Class Action Litigation Wave**
  - VTOs allow shoppers to “try on” products from phones or computers
  - VTO tools do NOT utilize true facial recognition
  - Instead, use “facial detection” software
- **Voice Biometrics**
  - Voice-powered technology has become incredibly common
    - Assistants – Siri, Alexa, Google Home, etc.
  - Relies on a person’s unique voice pattern to identify the user
  - “Voiceprint”: Pattern of curved lines and whorls distinct to a speaker
    - No voiceprint, no problems
  - Previous suits targeted companies that recognizes a user’s voice
  - Recent litigation includes voice data used for time and attendance
- **Timekeeping Systems**
  - Voiceprints, facial recognition, finger/hand prints

Recent Trends (cont.)

- **Facial Recognition in Vehicle Monitoring**
  - Transportation companies increasingly use facial recognition tech
  - Suits allege cameras scan drivers' facial geometry
    - If true, brings this within BIPA
  - Definition of "facial recognition" is not clear
    - Unclear for now whether these devices are regulated

- **Case to Watch: Smart Coolers Litigation (*Roberts v. Cooler Screens Incorporated)***
  - "Smart Coolers" replace refrigerator cases in retail stores
  - Replace doors with digital screens that provide an "interactive experience"
  - Includes a "facial profiling system" that "detect[s] the age, gender, and emotional response of over 3 million verified daily viewers."

Anticipated Developments

- *Cothron v. White Castle System, Inc.*
  - December 2021: Court of Appeals certified question to Illinois Supreme Court
  - "Do section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?"
  - $1,000 to $5,000 for the first violation, or for each?
  - If a plaintiff scans their fingerprints every day for a year, is that 1 violation, or 365?

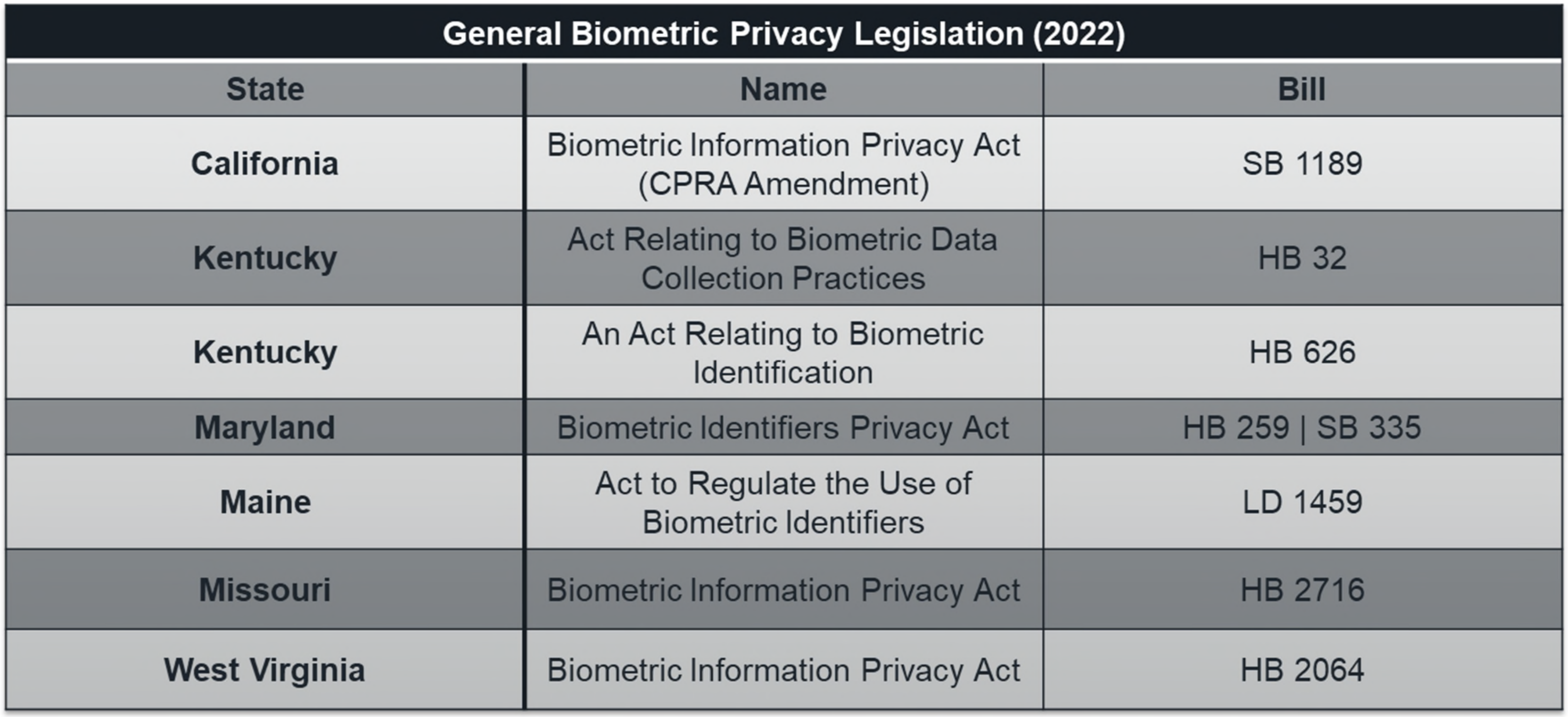
SQUIRE
PATTON BOGGS

State & Municipal Biometrics Legislative Priorities

Approaches States & Cities Are Taking to Regulate the Use to Biometric Technologies

General Biometric Privacy Bills

- **Current Biometric Privacy Statutes:** Illinois, Texas and Washington
- **New Legislation Proposed in 2022**



General Biometric Privacy Legislation (2022)

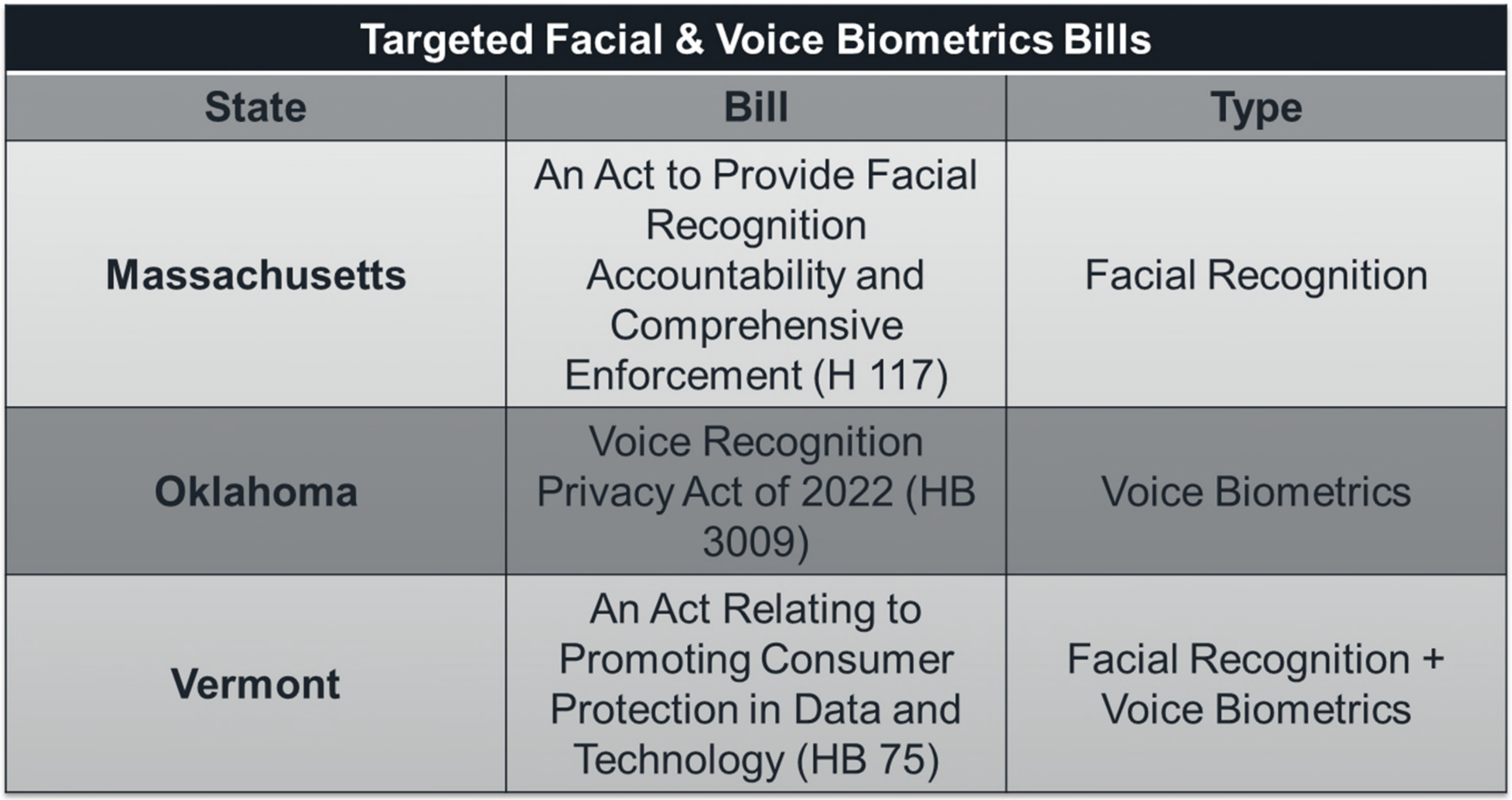
State	Name	Bill
California	Biometric Information Privacy Act (CPRA Amendment)	SB 1189
Kentucky	Act Relating to Biometric Data Collection Practices	HB 32
Kentucky	An Act Relating to Biometric Identification	HB 626
Maryland	Biometric Identifiers Privacy Act	HB 259 | SB 335
Maine	Act to Regulate the Use of Biometric Identifiers	LD 1459
Missouri	Biometric Information Privacy Act	HB 2716
West Virginia	Biometric Information Privacy Act	HB 2064

General Biometric Privacy Bills

- **BIPA Copycat Bills**
- **New Types of “Hybrid” Legislation**
  - Requirements & Limitations
- **High Exposure *and* High Compliance Burdens**
  - Same high liability exposure as BIPA copycat bills
  - Significant compliance burdens

Targeted Facial Recognition & Voice Biometrics Bills

- **More Focused Approach**
  - Some bills single out specific types of biometric technologies for greater regulation
- **Current Targeted Biometrics Regulation**



Targeted Facial & Voice Biometrics Bills

State	Bill	Type
Massachusetts	An Act to Provide Facial Recognition Accountability and Comprehensive Enforcement (H 117)	Facial Recognition
Oklahoma	Voice Recognition Privacy Act of 2022 (HB 3009)	Voice Biometrics
Vermont	An Act Relating to Promoting Consumer Protection in Data and Technology (HB 75)	Facial Recognition + Voice Biometrics

Inclusion of Biometric Data Within Scope of Consumer Privacy Laws

Consumer Privacy Laws’ Treatment of Biometric Data	
Statute	**Choice Obligations**
California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)	Consent not required
Virginia Consumer Data Protection Act (VCDPA)	Considered sensitive data, prior consent required for processing
Colorado Privacy Act (CPA)	Considered sensitive data, prior consent required for processing
Utah Consumer Privacy Act (UCPA)	Considered sensitive data, must present clear notice and opportunity to opt out

Inclusion of Biometric Data Within Scope of Consumer Privacy Statutes

2022 Legislation	
State/Bill	**Key Provisions**
New Hampshire (HB 597)	• Bill broadly defines "personal information" to include "facial photographs or images." • Includes private right of action with liquidated statutory damages.
New Jersey (AB 505)	• Brief but seemingly onerous GDPR-inspired general privacy bill that explicitly bans the processing of biometric data for identification purposes.
New York (AB 680 B)	• Bill requires private entities to obtain permission before collecting certain private information, including facial biometric information, and requires that data can be handled in a manner that keeps it safeguarded. • Can be enforced by either the New York AG or by private right of action.
New York Digital Fairness Act (AB 6082)	• Severely restricts the collection, use, and dispersion of biometric information. • Creates a private right of action with the possibility of punitive damages and authorizes the AG to bring enforcement actions. • Also imposes a fiduciary duty to the covered entity with respect to the individual whose data has been gathered.

Inclusion of Biometric Data Within Scope of Consumer Privacy Statutes

- **Impact of Differing Approaches to Regulating Biometric Data**
  - **Complete Data Inventories**
  - **Understand Compliance Requirements, including:**
    - Notices at Collection
    - Permitting choice (opt-out, consent)
    - Data Protection Assessments

Biometric Privacy Legislation: Takeaways

- **Increased Biometric Privacy-Focused Legislative Activity**
  - Expect Trend of Increased Legislation to Continue Beyond 2022
  - Added Pressure on Lawmakers From Lack of Progress by Federal Lawmakers
  - End Result = Greater Regulation, Increased Liability Exposure
- **Continued Focus on Regulation Targeting Facial Biometrics**
  - Current Focused Regulation
    - Portland Facial Recognition Ban
    - Baltimore Facial Recognition Ban
    - New York City “Commercial Establishments” Biometric Identifiers Information Ordinance
  - Lawmakers Showed Continued Desire to Single Out Facial Recognition With Targeted Legislation
  - End Result = Lawmakers Continuing to Take Aim at Facial Recognition, Greater Regulation in Immediate Future

Biometric Privacy Legislation: Takeaways

- **More Complex and Costly Compliance Burdens Stemming From New Hybrid Biometric Privacy Laws**
  - End Result = Compliance Fairly Straightforward Task Today, But That May Soon Change
- **Increased Reliance on Private Rights of Action as Primary Enforcement Mechanism**
  - All Four Biometric Privacy Laws Enacted in 2021 Contained Private Rights of Action
  - Trend Continued in 2022, With Majority of Biometrics-Focused Bills Allowing for Class Litigation
  - End Result = Risk of Class Litigation Avalanche Spreading to Other Parts of the Country

SQUIRE PATTON BOGGS

Anticipated Federal Developments

Proposed federal legislation concerning biometrics and AI and other anticipated developments in 2022

FTC Regulatory Developments

- Artificial Intelligence
  - The FTC possesses enforcement capabilities to regulate the development and use of AI, depending on context:
    - Section 5 of the FTC Act — “unfair or deceptive acts or practices”
    - Fair Credit Reporting Act — decisions to provide credit
    - Equal Opportunity Credit Act — algorithms that discriminate based on race, color, sex, age when making credit determinations
  - The FTC aims to clarify how algorithms are used and how the data contributes to output
- Biometrics
  - Bias and discrimination arising from use of biometrics is also now a focus of the FTC
  - Recent research has shown algorithms and biometric systems are biased against faces of color
    - iPhone’s FaceID feature
    - 2020 remotely-administered bar exam — threatened to fail applicants of color because their webcams could not detect their faces.

FTC Regulatory Developments (cont.)

- **FTC April 2021 Press Release**
  - Press release signaled the Commission’s focus on advances in AI going forward
  - Concerns about how advances in AI can be utilized without “inadvertently introducing bias or other unfair outcomes”

- **FTC Resolutions Focused on Algorithmic and Biometric Bias — Sept. 2021**
  - FTC voted to approve a series of resolutions directed at key enforcement areas
  - Allow FTC staff to investigate allegations of bias in algorithms and biometrics
  - “These resolutions enable the FTC to take swift action against a whole host of illegal conduct in important areas of concern to the Commission.”
  - “Companies engaging in conduct implicated by these resolutions should be forewarned: the FTC looks forward to aggressively using these resolutions and will not hesitate to take action against illegal conduct to the fullest extent possible under the law.”

FTC Enforcement Activity

- FTC finalized its settlement with Weight Watchers over alleged violations of the Children's Online Privacy Protection Act
  - Weight Watchers marks the first time that the FTC has utilized disgorgement in a COPPA case
- Part of a larger shift by the FTC to prioritize "meaningful disgorgement" as a remedy in privacy and security and enforcement actions
- First used in FTC's action targeting improper facial recognition with Everalbum, Inc.
- Algorithmic Disgorgement as New Normal in Near Future

Enforcement (cont.)

- Algorithmic Disgorgement as New Normal in Near Future
  - Weight Watchers settlement indicates that algorithmic disgorgement may soon become a standard component in future FTC settlements
  - Particularly outsized impact on developers of artificial intelligence and related technologies which rely heavily on the development of advanced algorithms
  - Another example of the FTC's focus on the impact AI can have in relation to consumer privacy and related issues
  - December 2021 Notice:
    - "considering initiating a rulemaking under Section 18 of the FTC Act to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination."
  - A broad range of privacy, cybersecurity and AI issues that the FTC may seek to regulate as previewed by its Notice
  - The FTC has increasingly cautioned that AI may "inadvertently introduc[e] bias or other unfair outcomes" to medicine, finance, business operations, and media
  - Declared algorithmic and biometric bias as a focus of enforcement in resolutions passed in Fall 2021

Federal Legislative Developments

- Algorithmic Accountability Act of 2022 (S 3572)
  - Proposes to direct the FTC to promulgate regulations that require any “covered entity” to:
    - Perform impact assessments
    - Meet other requirements regarding automated decision-making
  - Requires promulgation of regulations on automated decision-making processes that implicate an “augmented critical decision process” on a consumer
- HB 4521 (Omnibus Bill)
  - Research on best standards in the fields of digital identity management and biometrics

SQUIRE PATTON BOGGS

Concluding Remarks

CLE

For those of you who require CLE credits please note the following states have been approved for CLE in
AZ, CA, NJ, NY, OH and TX.

Please write down the following affirmation code [TCB45]

A couple business days after today's session you will receive an email with ***uniform certificate of attendance*** and ***program evaluation*** to complete and SUBMIT to my colleague, Robin Hallagan at robin.hallagan@squirepb.com.

Contacts

Kristin Bryan

Partner

216.479.8070

kristin.bryan@squirepb.com

Kyle Fath

Partner

213.689.6582

kyle.fath@squirepb.com

David Oberly

Senior Associate

513.361.1252

david.oberly@squirepb.com

www.consumerprivacyworld.com

Consumer Privacy World

Keeping you informed on the evolving law on data privacy, security and innovation.

It’s a vast privacy world out there.

Don’t worry, we’ll help you explore it. Lots to see.

Meet the Incredible Attorneys Powering Consumer Privacy World

Our privacy attorneys are truly best in class and the undisputed leaders of the Consumer Privacy World. We have assembled one of the most experienced and dedicated consumer privacy teams on the

Global Coverage

SQUIRE PATTON BOGGS

Abu Dhabi
Atlanta
Beijing
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Cincinnati
Cleveland
Columbus
Dallas
Darwin
Denver
Dubai
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid

Manchester
Miami
Milan
Moscow
New Jersey
New York
Palo Alto
Paris
Perth
Phoenix
Prague
Riyadh
San Francisco
Santo Domingo
Seoul
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC

Africa
Brazil
Caribbean/Central America
India
Israel
Mexico

🟩 Office locations

⬛ Regional desks and strategic alliances