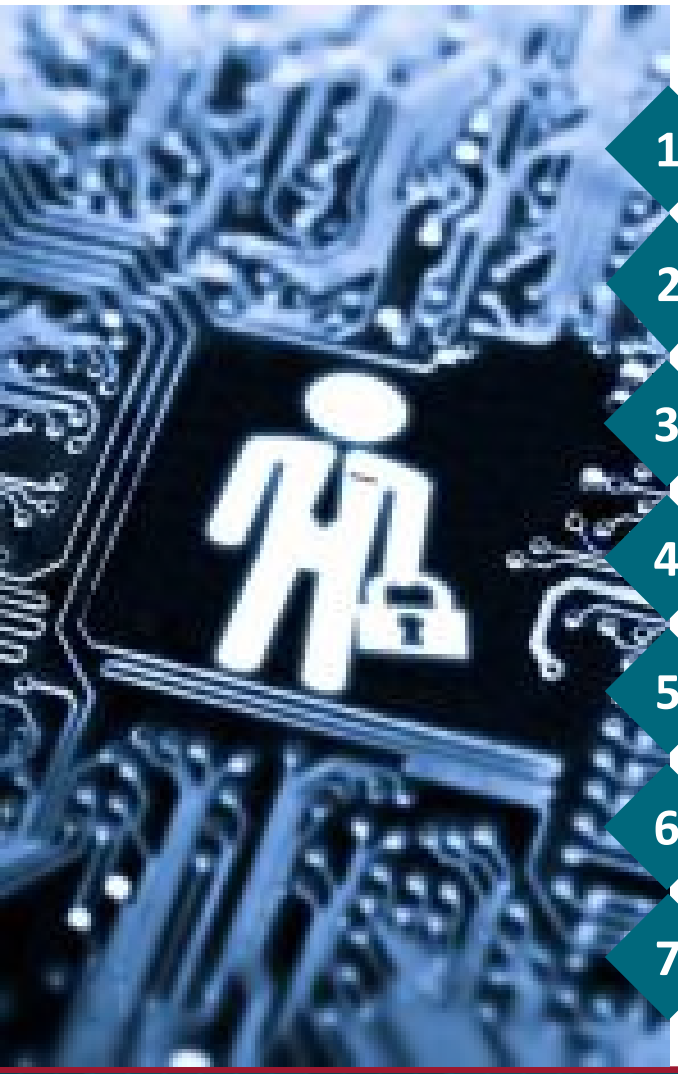
CONSTANGY
BROOKS, SMITH & PROPHETE LLP

Navigating the Digital Frontier:

Employee Privacy Rights and Legal Obligations in the Modern Workplace

Constangy | April 2024



Agenda

1. Introductions
2. Overview of U.S. Employment & Data Privacy Laws
3. Biometric and Genetic Data
4. Employee Disclosures and Third-Party Requests
5. Artificial Intelligence
6. Employee Surveillance
7. Key Take-Aways

1

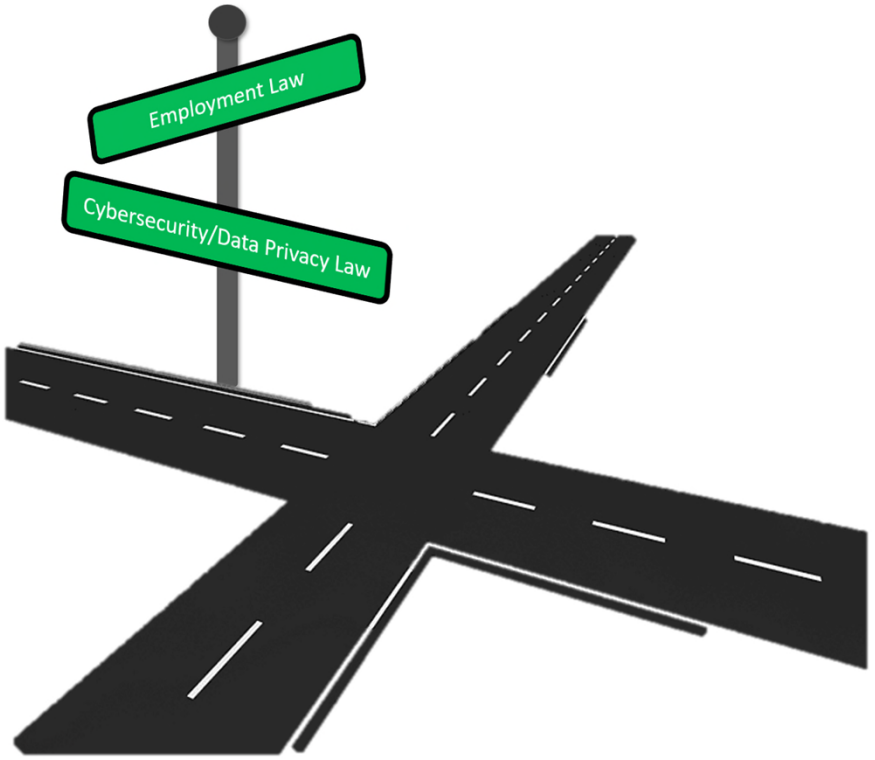
Introductions

Presenters

Sarah Rugnetta
Partner, Vice Chair
Cybersecurity & Data
Privacy Team

Ashley Orler
Partner, Co-Chair
Cannabis & Employee Substance Abuse
Practice Group

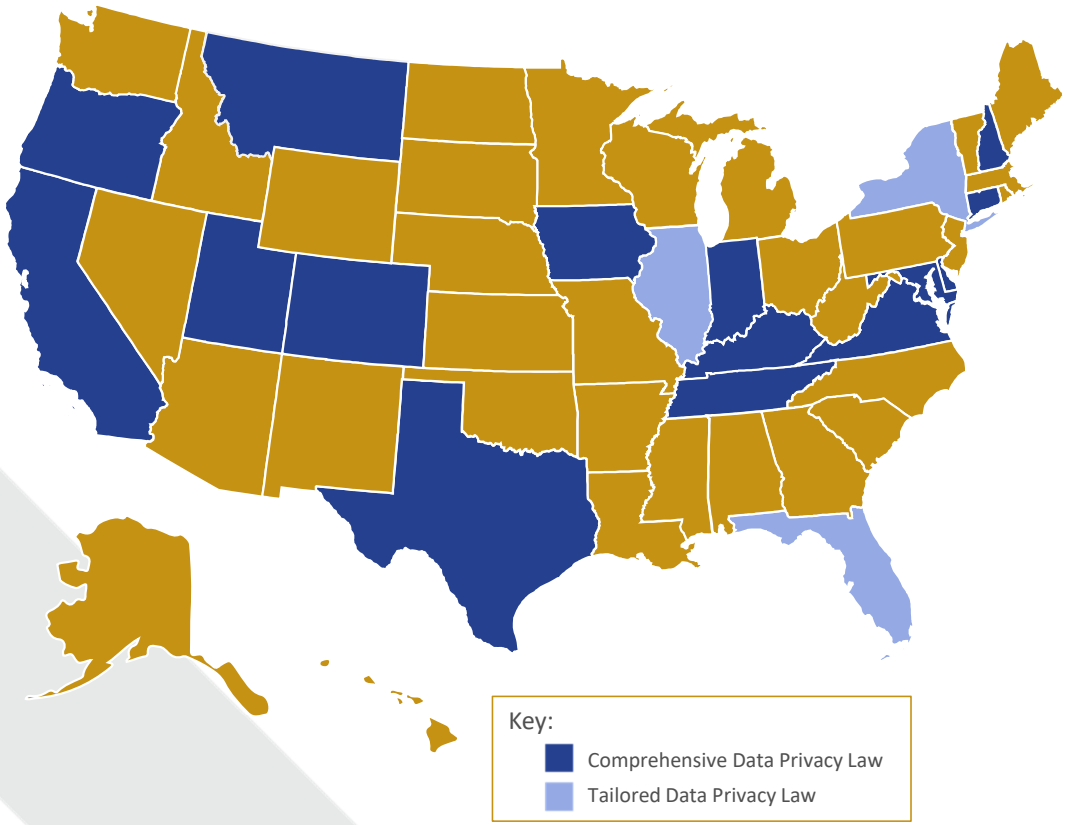
Intersection of Employment Law and Cybersecurity/Data Privacy Law



2

Overview of U.S. Employment & Data Privacy Laws

Data Privacy: United States Snapshot



- HIPAA/HITECH
- SEC
- FERPA
- TCPA
- FTC Act
- VPPA
- GLBA
- CAN-SPAM
- FCRA/FACTA
- COPPA

Overview of the California Consumer Privacy Act

Applies to the collection of personal information related to a consumer

"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." (Cal. Civ. Code § 1798.140(o)(1))

Unlike many of the other state privacy laws, the CCPA applies to employee and business-to-business data.

Overview of the California Consumer Privacy Act

Determining Whether You are a "Business"

- A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity
- Organized or operated for the profit or financial benefit of its shareholders or other owners

Do you do business in the State of California and meet one or more of the following thresholds:

- ✓ Annual Gross revenues in excess of $25,000,000; **OR**
- ✓ Annually buys, receives, sells, or shares for commercial purposes, the personal information of 100,000 or more consumers, households, or devices; **OR**
- ✓ Derives 50% or more of its annual revenues from selling consumers' personal information

Data Privacy Requirements

Employee Privacy Protections

3

Biometric and Genetic Data

Biometric Information – Definitions

- Definitions vary, but generally data generated by electronic measurements of unique physical characteristics that can be used to identify an individual; generally includes:
  - Retina or Iris Scan
  - Fingerprint
  - Voiceprint
  - Scan of hand or face geometry
- Not included:
  - Photographs
  - Physical descriptions
  - Information that can't be used to identify an individual

Regulation of Biometric Information

Illinois Biometric Information Privacy Act

- Informed Consent
- Biometric Information Policy
- Both must describe purpose of collection, disclosures, and retention period.

State Data Privacy Laws

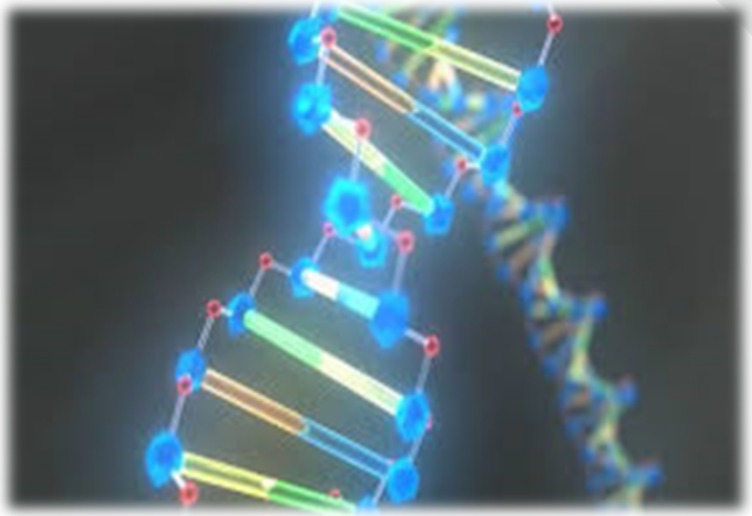
- Higher requirements because considered sensitive private information (SPI)
- Laws in CA, CO, UT, CT, and VA impose additional obligations for the collection, use, and sharing of biometric information.
- Colorado Data Privacy Act requires ***opt-in*** for certain uses/disclosures of SPI

State Breach Notification Laws

- Many require notification if biometric information is impacted.
- Definitions of PI vary by state breach notification law.

Genetic Information Protections

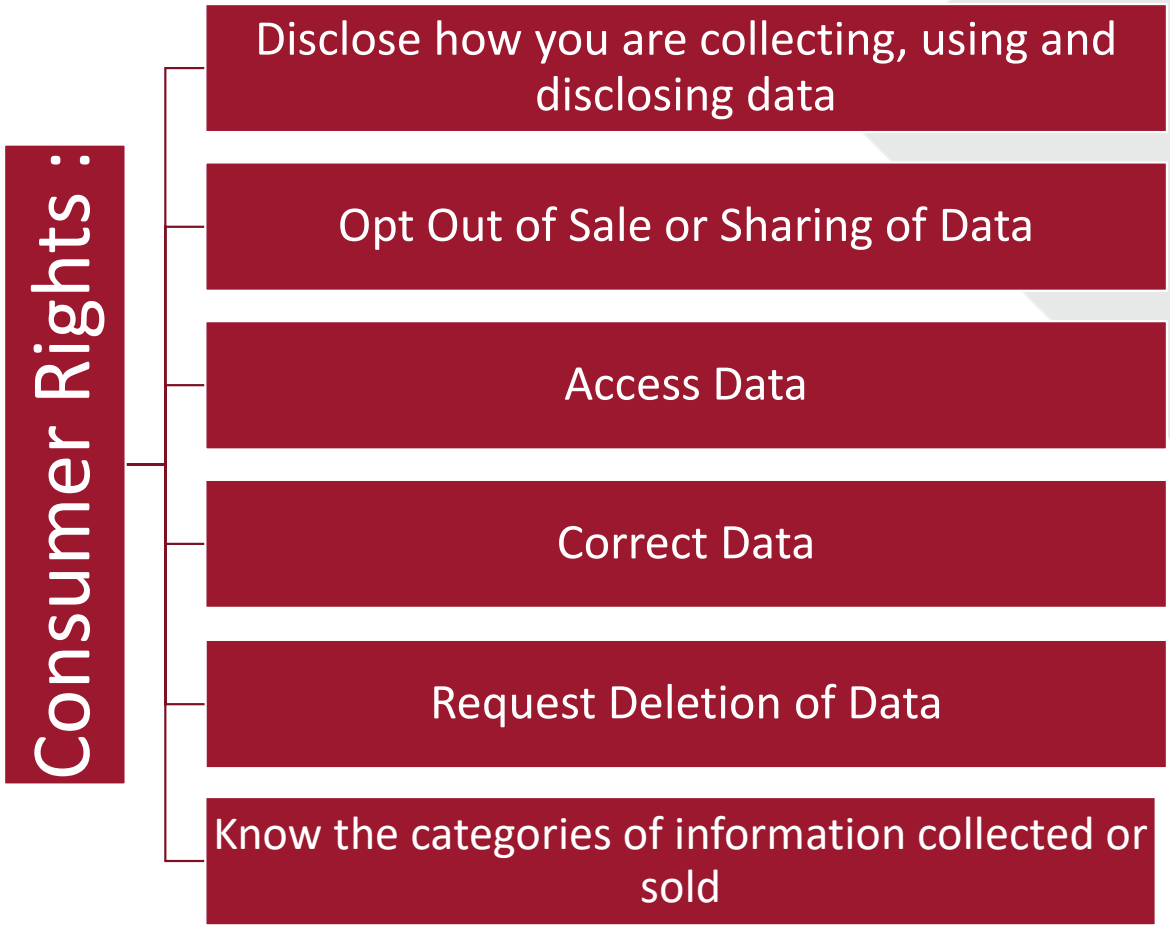
- Illinois Genetic Information Privacy Act, *410 ILCS 513/1, et seq.*
- Genetic testing and information derived from genetic testing is confidential and may be released only to the individual tested and to persons specifically authorized in writing
- Specifically prohibits employers from certain actions related to genetic testing or genetic information
- Other states have similar laws
- Litigation is on the rise against employers



4

Employee Disclosures & Third-Party Requests

California Data Subject Rights & Responses



Disclosures and Consent May be Required to Obtain or Provide Data

- Disclosures may be required before providing employment records to third parties

  Illinois Personnel Record Review Act, *820 ILCS 40/1 et seq.*, requires employer to provide written notice to the employee before divulging a disciplinary report, letter of reprimand, or other disciplinary action to a third party.

- Don’t forget HIPAA may apply to certain employers

- Fair Credit Reporting Act requires consent and disclosures for background checks and drug/alcohol testing

5 Artificial Intelligence

Legal Requirements

- **Federal Laws: FTC & EEOC**
  - FTC: Unfair and Deceptive Practices (Section 5 of FTC Act): Focus largely on the AI developers – claims about AI, its effectiveness, whether it can be misused for fraud and whether you've mitigated risks.
  - EEOC has started to bring enforcement actions under nondiscrimination laws when AI tools—either deliberately or inadvertently—reject candidates based on protected characteristics.
    - First lawsuit against an English-language tutoring services company "iTutorGroup" for allegedly programming its online recruitment software to automatically reject older applicants.

- **Local Laws**
  - NYC Local Law 144: Prohibits employers and employment agencies from using an automated employment decision tool unless the tool has been subject to a bias audit within one year of the use of the tool, the information about the bias audit is made publicly available, and the correct notices have been provided to employees and/or job candidates.

Bias & Discrimination

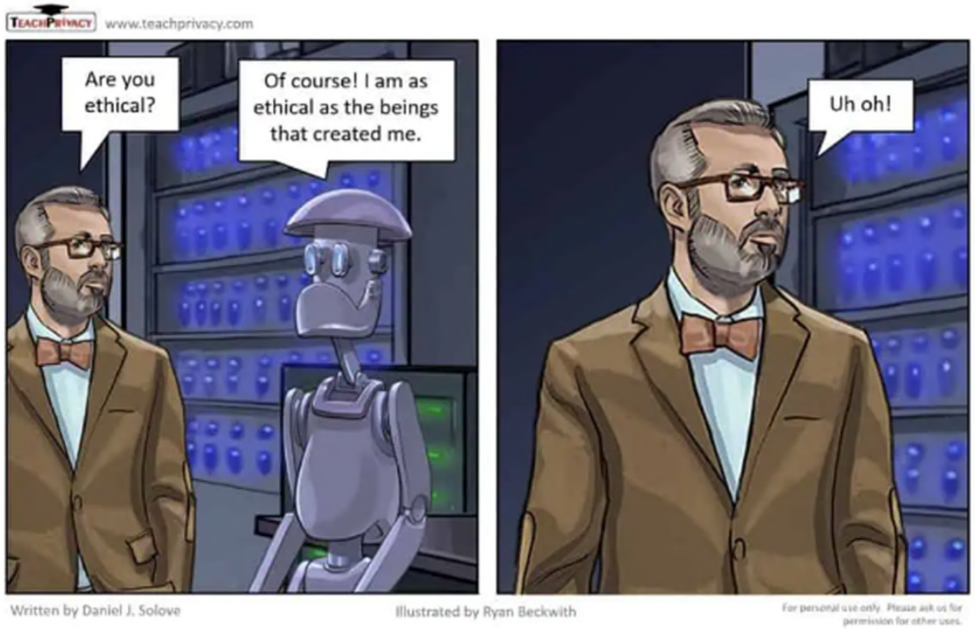
- **Bias and discrimination in AI**
  - Recruitment & Hiring: Use AI to screen resumes for experiences appropriate to role.
    - *Derek L. Moblry v. Workday Inc. (U.S.D.C / N.D.C.A.)*, Feb. 2023- Screening tool allegedly disproportionately disqualified African American individuals over 40 w/ disabilities.

  - EEOC Technical Assistance provides guidance:
    - Is the tool job-related and consistent with business necessity?
    - Is the Interface accessible and are reasonable accommodations available?
    - Are materials presented to job applicants / employees in alternative formats?
    - Did the vendor attempt to determine whether its algorithm disadvantages certain individuals?

Ethical Implications of AI

Cartoon: AI Ethics

Posted on June 21, 2023 (June 21, 2023) by Daniel Solove



Source: [Artificial Intelligence (AI) Blog by Daniel J. Solove | TeachPrivacy]

6

Employee Surveillance

Employee Monitoring

- **Delaware Code Title 19**
  - Requires employers to notify employees of electronic monitoring beforehand
  - One time notice acknowledged by employee in writing or electronically OR daily notice each day employee accesses electronic services
  - Includes telephone conversations, email, internet access

- **Connecticut Law**
  - Prohibits employers from surveillance in areas designated for health or personal comfort
  - Requires employers to provide prior written notice for electronic monitoring
  - Includes use of computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems

Social Media Privacy

- **States Protect Employee's Social Media Accounts**
  - Prohibits employers from requesting usernames, passwords, and other credentials for accessing personal social media accounts
  - Most states have some form of this prohibition

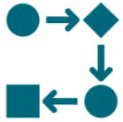
7

Key Take-Aways

Building a Data Security & Privacy Program

- All organizations should build a sustainable and scalable data security and privacy program that is tailored to the size of the organization and the sensitivity of its data and systems.
- DS&P programs should address:

 **People**

 **Policies & Procedures**

 **Technology**

- All three areas are necessary for an effective program
- Security should not be left solely to IT staff and tech consultants

Review of Employment Practices

- All organizations should review annually their employment policies and practices

- This review should include a review of employee data and technology tools used by employees

8

Q & A

CONSTANGY
BROOKS, SMITH &
PROPHETE LLP

Thank You!

For further questions or comments visit our website or contact one of our attorneys.