2024 EMPLOYMENT LAW Conference

Off to work we go!

An Update on California's Complex Privacy Laws and Employer Compliance Requirements

Fisher Phillips

FLOYD SKEREN MANUKIAN LANGEVIN

Presenters

Usama Kahf

Partner | Fisher Phillips LLP

949.798.2118 | ukahf@fisherphillips.com

David G. Graziani

Associate | Floyd Skeren Manukian Langevin LLP

818.715.0018 | David.Graziani@floydskerenlaw.com

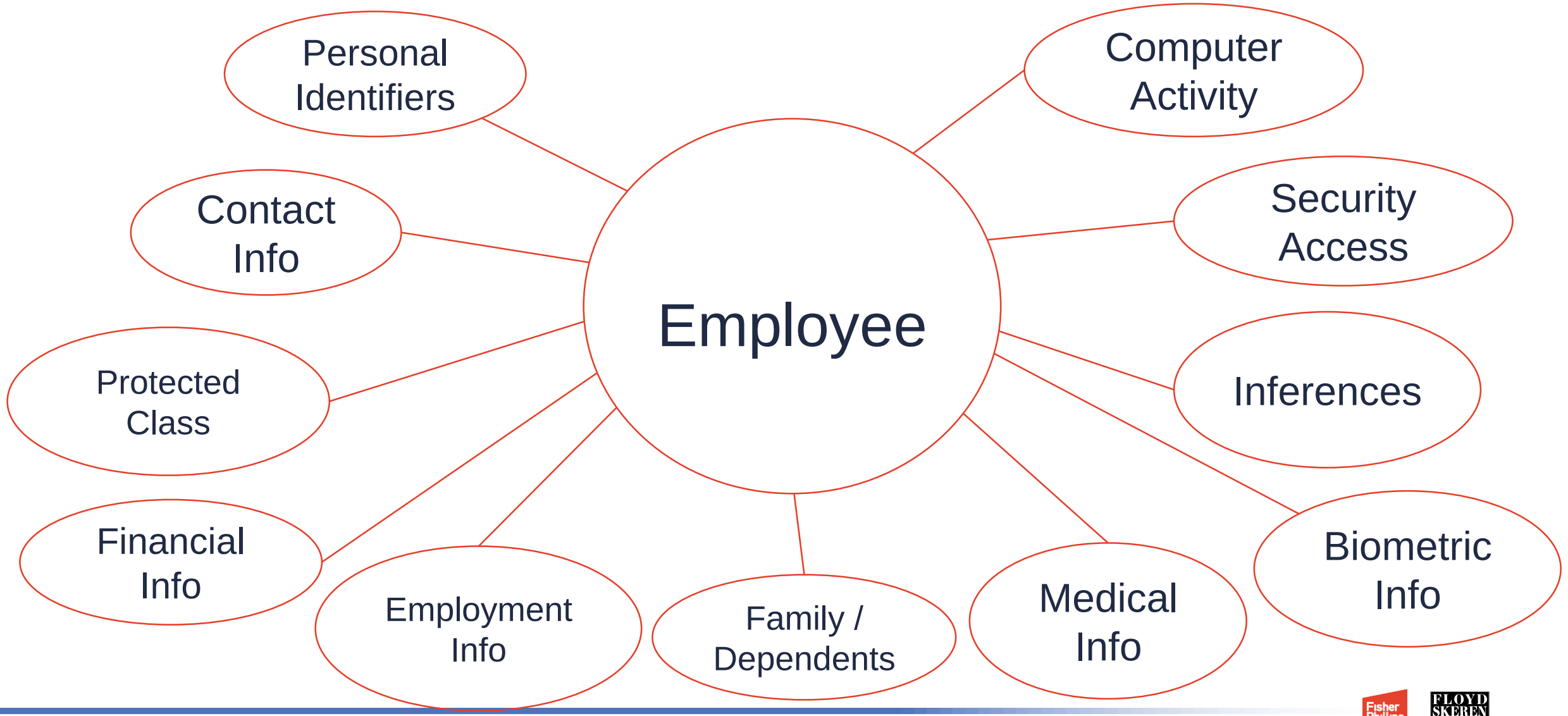
Agenda

- California Consumer Privacy Act (CCPA) requirements for employers
- Potential privacy litigation and abuse of process by employees
- Use of Artificial Intelligence by employers

California Consumer Privacy Act (CCPA)

- Covered "**Business**"
  - For-profit business AND does business in California AND collects the personal information of consumers who are CA residents AND
  - Meets one of several tests (most common: $25 mil annual gross revenue)
- "**Consumer**" is any natural person who is a CA resident, including:
  - Employees, job applicants, independent contractors
  - Family members, dependents & beneficiaries
  - Website visitors
  - Visitors to your physical locations in CA
  - I.e., anyone regardless of context of the interaction

What Is Personal Information?



Consumer Rights Under the CCPA

- Right to know what personal information is collected and right to access
- Right to know what personal information is sold/shared and to whom
- Right to correct inaccurate personal information
- Right to delete personal information
- Right to opt-out of the sale/sharing of personal information
- Right to limit use and disclosure of sensitive personal information
- Right to non-discrimination / right to no retaliation for exercising consumer rights

Basic CCPA Obligations for Employers

1) When collecting personal information:

   a) Distribute "**notice of collection**" to employees, job applicants, guests, website users, and other consumers

      - **Purpose limitation / accurate & complete**

   b) Provide either "**opt-in consent**" or a mechanism for consumers to opt-out of the sale of PI or sharing of PI for targeted ads

      - **Do employers "sell" or "share" their employee data?**

   c) Provide "**Limit Use of My Sensitive Personal Information**" option for SPI if you use/disclose SPI to infer characteristics about consumers

Basic CCPA Obligations for Employers

2) Annually update online and employee privacy policy
3) Implement at least two methods for all “consumers” to submit “consumer requests,” as well as a process for tracking and responding to requests
4) Implement reasonable security measures (both physical and electronic)
5) Conduct due diligence on service providers and update contracts with CCPA terms
6) Ensure all necessary employees attend CCPA training
7) Data minimization

Consequences of Non-Compliance

Law enforcement:

- California Attorney General
- California Privacy Protection Agency

Fines: $2,500 per violation, or $7,500 per intentional violation.

Enforcement actions – 5-year statute of limitations

Other Claims Stemming from CCPA

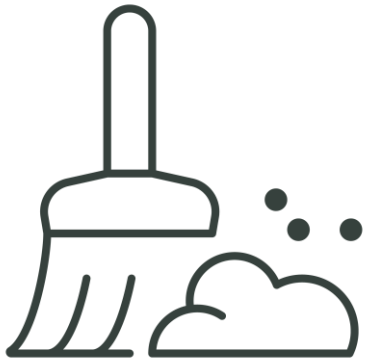
- Claims under the Unfair Competition Law

- Wrongful Termination or Retaliation Claims (Cal. Labor Code § 1102.5)
  - CCPA makes explicit that businesses cannot retaliate against an employee, applicant, or independent contractor for exercising their rights under the CCPA

Key CCPA Issues for Employers

- Employee or applicant exercise of a CCPA right is a protected activity under the CCPA
- Potential abuse of process by employees
  - Plaintiffs' use of CCPA to do prelawsuit evidence gathering
  - Request to correct
  - Request to delete
  - Request to access
- Are your vendors "selling" your employee data?

CCPA Enforcement Sweep – June 2023



- California Attorney General announced sweep of “large” employers
  - Auditing employer data collection, use, and disclosure practices in the employment context
  - Are you providing any CCPA notice to employees and applicants?
  - Do you have a privacy policy for employees?
  - Do you have a system in place to process consumer requests from employees and applicants?

CCPA Compliance Action Plan

- Data Inventory and Data Mapping
- Amend Notices and Privacy Policies
- Update Contracts with Vendors and Third Parties
- CCPA Request Management

Use of Artificial Intelligence by Employers

- Productivity Tracking: AI tools are deployed to analyze productivity metrics such as keystrokes, emails, and activity logs. Software like Hubstaff and Time Doctor track time spent on tasks, website usage, and application activity, providing detailed reports on employee productivity.

- Behavioral Analytics: AI algorithms can assess employee behavior patterns through monitoring communication tools (emails, chats) and interactions, flagging unusual activities that might indicate security threats or compliance issues.

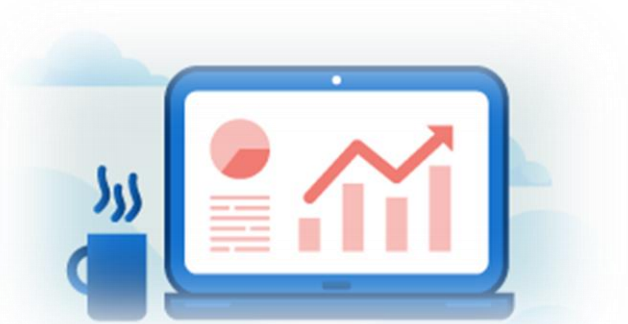
Use of Artificial Intelligence by Employers

- Performance Management: AI-driven platforms like Workday and SuccessFactors analyze performance data to identify high performers, provide feedback, and predict future performance trends. These systems can recommend personalized training and development programs.

- Wellness Monitoring: Some AI tools are designed to gauge employee wellness by monitoring signs of burnout or stress through physiological data (e.g., from wearable devices) or behavioral indicators like work hours and communication tone.

Benefits of AI in Employee Monitoring

- Enhanced Productivity: By providing real-time insights into employee activities, AI can help managers identify inefficiencies and improve overall productivity.
- Improved Security: AI systems can detect and prevent data breaches by monitoring for suspicious activities, reducing the risk of internal threats.
- Data-Driven Decisions: AI provides objective data that can enhance decision-making processes regarding promotions, layoffs, and resource allocation.
- Personalized Development: AI can identify skill gaps and suggest targeted training programs, fostering employee growth and satisfaction.



Ethical and Privacy Concerns

- Privacy Invasion: Continuous monitoring can be perceived as intrusive, potentially leading to a loss of trust between employees and employers.
- Data Security: Handling large volumes of sensitive employee data increases the risk of data breaches and misuse of information.
- Bias and Fairness: AI systems can perpetuate existing biases if not properly designed and audited, leading to unfair treatment of employees based on flawed data interpretations.
- Mental Health Impact: Constant surveillance can contribute to stress and anxiety, negatively impacting employee well-being and job satisfaction.

Best Practices for Ethical AI Use in Monitoring

- Transparency: Employers should be transparent about the extent and purpose of monitoring, ensuring that employees are fully informed about what data is collected and how it will be used.
- Consent: Gaining explicit consent from employees before implementing AI monitoring tools is crucial. Employees should have the option to opt-out without facing repercussions.
- Data Minimization: Collect only the data necessary for achieving specific, legitimate aims, and ensure it is stored securely.

Best Practices for Ethical AI Use in Monitoring

- Regular Audits: Conduct regular audits of AI systems to detect and mitigate biases, ensuring fair and equitable treatment of all employees.
- Balancing Monitoring with Privacy: Implement measures that balance the need for monitoring with respect for employee privacy. For example, anonymizing data where possible and limiting access to sensitive information.
- Employee Support: Provide support systems for employees who might feel overwhelmed by monitoring. This could include access to counseling services and clear communication channels for voicing concerns.

Bias

- Selection Bias
- Algorithmic Bias
- Confirmation Bias
- Measurement Bias
- Emergent Bias

Avoiding Bias

- Diverse and Representative Data
- Bias Detection and Mitigation
- Transparency and Explainability
- Diverse Teams and Stakeholder Engagement
- Regular Monitoring and Auditing

CCPA Proposed AI Regulations

- Broadly protect consumers (including employees and job applicants) from a business' use of automated decision-making technology (ADMT).

- ADMT is technology that processes personal information *and* uses computation to:
  - Execute a decision,
  - Replaces human decision-making, *or*
  - Substantially facilitates human decision-making

CCPA Proposed AI Regulations

- Would require businesses to:
  - Notify consumers about the technology
  - Allow opt-out of ADMT use
  - Allow access to information about the use of ADMT

When Would You Need to Comply with ADMT Requirements?

If you use ADMT in any of three ways:

1. For a significant decision
2. For extensive profiling (including “Work or Educational Profiling”)
3. For training ADMT

Pre-use Notice Requirements

1. Specific purposes for using ADMT
2. Description of the right to opt-out
3. Description of right to access information about the businesses use of ADMT
4. Right of no retaliation for exercising rights
5. Explanation of how ADMT works

Exceptions to Requests to Opt-Out of ADMT – No Opt-Out

- No Appeal
  - When ADMT used for Work or Educational Profiling, when necessary for security, fraud prevention, or safety purposes.
  - When ADMT used for certain significant decisions (hiring; allocation, or assignment of work; salaries, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits) **AND**
    - Necessary for purpose and used solely for the purpose; and
    - Conducted an evaluation of ADMT; and
    - Implemented accuracy and nondiscrimination safeguards.

Exceptions to Requests to Opt-Out of ADMT – No Opt-Out

- Human Appeal
  - Using ADMT to make significant decisions about employment opportunities or compensation.
  - *No exceptions to human appeal* for promotions, demotion, suspension, and termination.
  - *Exceptions to human appeal* for hiring; allocation, or assignment of work; salaries, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits if requirements in prior slide met.

Adverse Significant Decisions

What is a significant adverse decision? Use of ADMT that resulted in an employee or IC having their compensation decreased, or being suspended, demoted, or terminated.

Notice Requirements:

1. Use to ADMT
2. Right of non-retaliation
3. Right to access information used in ADMT
4. If business relying on human appeal exception, how to lodge an appeal.

Responses to Requests to Access Information About the Use of ADMT

1. Specific purpose for using ADMT.
2. Output of the ADMT for the individual.
3. How the business used the ADMT for the individual.
4. How the ADMT worked with respect to the individual.
5. Other CCPA rights and non-retaliation.

The Black Box Problem

- Can you explain *how* your ADMT made the decisions it did?

- Can you ensure:
  - Your ADMT was not trained on a biased or flawed data set?
  - Is your ADMT measuring what you want it to?

This

California Legislative Pipeline for AI

- Prohibiting Algorithmic Discrimination – AB 2930 (Bauer-Kahan)
- Addressing Employment Replaced by AI – AB 3058 (Low)
- Requiring Safety Standards for Large AI Models – SB 1047 (Wiener)
- Tackling “Digital Replicas” in the Entertainment industry – AB 2602 (Kalra)
- Regulating the Use of AI by State Agencies – SB 896 (Dodd)

ACLU Files Claims with FTC and EEOC

- ACLU requested FTC to investigate AI powered personality assessment test, a video interview tool, and a cognitive ability screen device.
  - Alleges developer's claim of "fair," "bias free," and "without adverse impact" tools amounts to a deceptive marketing tactic.

- ACLU also filed charge with the EEOC over the same AI tools.
  - Alleges these tools unfairly screen out applicants with disabilities and unfairly target those with certain racial backgrounds.

Conclusion

The use of AI to monitor employees offers significant benefits in terms of productivity and security but also raises important ethical and privacy issues. Organizations must navigate these challenges carefully by adopting transparent, fair, and respectful monitoring practices that safeguard employee rights while leveraging the advantages of AI technology.

QUESTIONS?

Presenters

Usama Kahf

Partner | Fisher Phillips LLP

949.798.2118 | ukahf@fisherphillips.com

David G. Graziani

Associate | Floyd Skeren Manukian Langevin LLP

818.715.0018 | David.Graziani@floydskerenlaw.com

2024 EMPLOYMENT LAW Conference

Off to work we go!

THANK YOU

Fisher Phillips

FLOYD SKEREN MANUKIAN LANGEVIN