Navigating the Digital Workplace

Legal and Ethical Considerations of Employee Surveillance and Emerging AI Technologies

June 6, 2024

ACC Association of Corporate Counsel NEW YORK CITY

JacksonLewis

Presenters

George Dunston

Chief Privacy Officer & Associate GC , Barnes & Noble

gdunston@bn.com

Joseph Lazzarotti

Principal, Jackson Lewis P.C.

Joseph.Lazzarotti@jacksonlewis.com

Teri Wood

Of Counsel, Jackson Lewis P.C.

Teri.Wood@jacksonlewis.com

Start of Day

- Employee clocks in by scanning a finger, hand, face or eye on a time clock
- Employee accesses facility by scanning a finger, hand, face or eye in connection with a security system

What Is Biometric Data?

- Biometric identifier
  A retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry
- Biometric information
  Any information — regardless of how it is captured, converted, stored or shared — based on an individual's biometric identifier used to identify an individual

Illinois Biometric Information Privacy Act

- Applies to private entities in possession of biometric identifiers or biometric information or which collect, capture, purchase, receive through trade or otherwise obtain biometric identifiers or biometric information
- Informed written release/consent prior to collection, disclosure
- Mandates safeguarding, retention and destruction policies "made available to the public"
- Permits a limited right to disclose with consent
- Prohibits sale, lease, trade or profit from biometric data
- Provides "aggrieved" individuals a private right of action for BIPA violations
  - A prevailing party *may* recover
    - $1,000 for each negligent violation or actual damages
    - $5,000 for each intentional or reckless violation, or actual damages

California

- Labor Code Section 1051
  - Prohibits employers from requiring, as a condition of employment, the collection of an employee's or applicant's photograph or fingerprint and furnishing same to a third party where same could be used to the detriment of the employee or applicant
- CCPA/CPRA
  i. Requires notice to consumers (including employees, applicants, contractors) at or before collection
  ii. Biometric information subject to reasonable security safeguard requirement
  iii. Biometric information considered "Sensitive Personal Information" and corresponding right to restrict use
  iv. Covered by private right of action provision for data breaches

New York

- Labor Law Section 201-a

· Prohibits employers from requiring employees to provide fingerprints unless required by law

· But: See NY DOL opinion letter issued April 22, 2010

  · States that "[w]hile Section 201-a does not prohibit voluntary fingerprinting of employees, employers may not take any adverse employment action against employees for not volunteering to be fingerprinted, or otherwise coerce employees to 'volunteer' to participate in the fingerprinting program"

· The SHIELD Act

  i. Requires businesses to maintain a comprehensive set of policies and procedures to safeguard personal information including biometric information

  ii. Adds biometric information to definition of private information subject to the state's breach notification rule

Starting Work

Employee logs on to work computer and work email

Employee Monitoring

Good Reasons

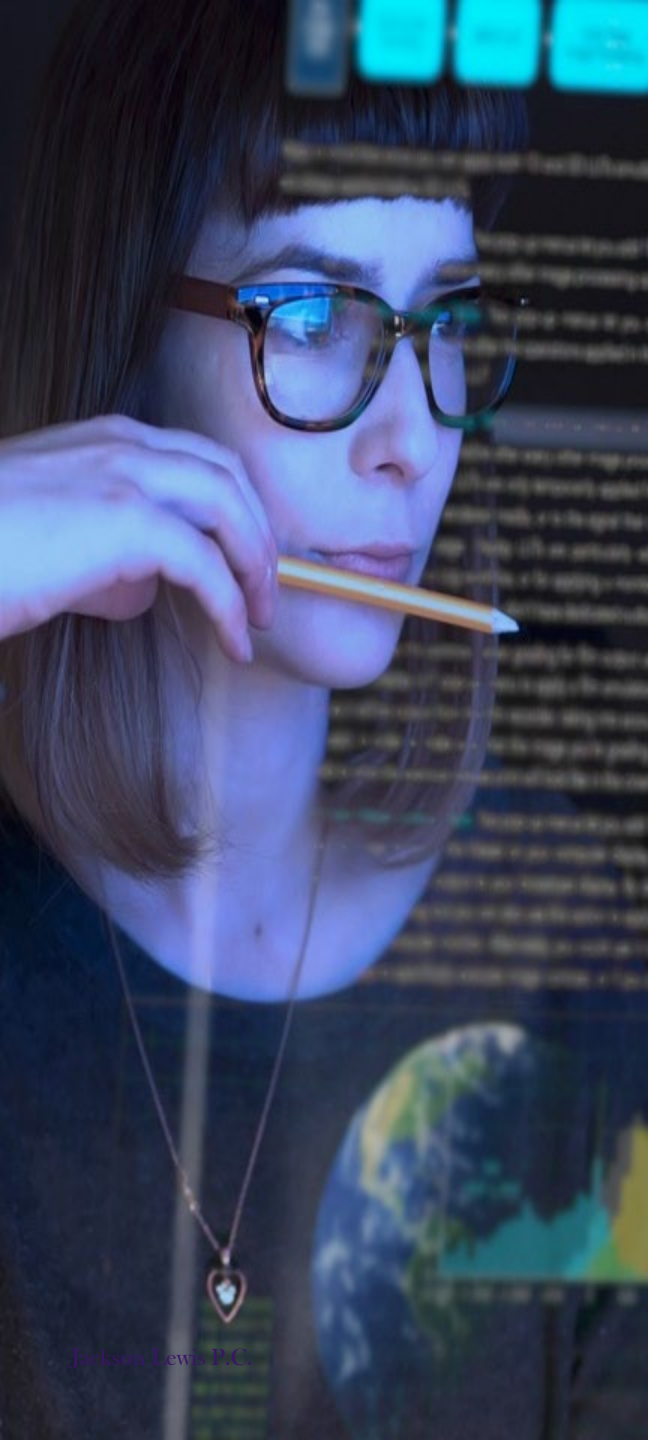
- Ensure productivity and engagement, good business practices, customer service
- Dissuade cyberslacking and social networking
- Protect trade secrets and confidential business information
- Prevent fraud, theft, embezzlement of money
- Avoid harassment claims
- Protect against wrongful termination claims
- Detect and dissuade improper behavior
- Avoid identity theft and data breaches
- Ensure employees are not snooping in medical records,
  driver's license records, etc.

Bad Reasons

- No reason at all
- Prurient curiosity
- Assess organizing activities; chill protected concerted activity
- Assess validity of health/disability claims
- Boredom

Restrictions on Monitoring

- Electronic Communications Privacy Act (ECPA)
- Stored Communications Act (SCA)
- Common law intrusion upon seclusion
- State wire tap acts
- Biometric privacy laws in CA, IL, NY, TX, NYC
- Notice requirements in CT, DE, NY, NJ (GPS), CA (CCPA)
- Restrictions on disclosure of social media passwords in 25+ states
- Record collection and retention requirements (e.g., CCPA, HIPAA, GINA, GIPA)



Practical Concerns

- Technology can promote isolation
- Are systems user friendly?
- Ability to individualize
- Costs of installation, operation, updates, etc.
- Reluctance to use/employee pushback because of fears about privacy and technology
- Storage, record retention and destruction
- Monitoring the monitors
- Ability to consistently obtain consent (when required), including from all users of the technology (e.g., contractors or temporary employees)
- Compliance with the company's own retention and destruction policies

Legal Concerns

- Expectation of privacy
- Notice requirements: CT, DE, NY (CA) for electronic monitoring
- Common law claim of intrusion upon seclusion
- Restrictions on requesting or requiring employees or applicants to disclose social media/online account usernames and passwords — does monitoring/spyware provide a back door?
- Access to information you do not need or want (e.g., disability information, financial information, etc.)
- Wage and hour issues
- Unintended evidence
- Labor considerations — bargaining, protected concerted activity

Time for Employee to Meet Client

- Employee “checks out” a fleet vehicle using an app on her phone
- Employee takes a fleet vehicle to visit a client worksite

Vehicle Tracking & Fleet Management

Vehicle tracking

- Geolocation
- Artificial intelligence
- Facial recognition
- More/other

Primary concerns

- Privacy
- Data collection

What Is the Internet of Things?

A vast network of physical devices, vehicles, appliances and other objects embedded with sensors, software and network connectivity

Concerns with IoT

Security vulnerabilities

- Device vulnerabilities: IoT devices can be susceptible to hacking, malware and unauthorized access due to weak security protocols
- Data breaches: Inadequate security measures may lead to data leaks, compromising sensitive employee information
- Lack of encryption: Unencrypted data transmission can expose confidential data during communication

Privacy risks

- Employee surveillance: IoT-enabled workplace monitoring can infringe on employee privacy rights
- Data collection: Gathering extensive data on employees' behavior, location, and activities raises privacy concerns
- Consent: Ensuring informed consent for data collection and usage is essential

Data overload

- Information flood: IoT generates massive amounts of data; managing and analyzing this flood can overwhelm organizations
- Relevance: Filtering relevant insights from the data noise becomes challenging

Ethical considerations

- Employee consent: Balancing data collection with employee consent and transparency
- Bias and discrimination: Algorithms used in IoT systems may perpetuate biases

Legal compliance

- Data protection laws: Organizations must comply with regulations to avoid penalties
- Data retention: Properly managing data retention and deletion policies

Developing Policies and Procedures to Protect Employee Data

Take Inventory of Data Being Collected

Identify data sources

- Analyze data held by various departments, including HR
- Consider both structured (databases) and unstructured (files, emails) data

Categorize data

- Classify data based on sensitivity (e.g., personal, financial, health)
- Assign risk levels to each category

Document data mapping

- Create a visual map showing data flow within your organization
- Highlight data storage locations, access points and data transfers.

Maintain accuracy

- Regularly update the inventory as data changes
- Ensure accuracy to support privacy laws and compliance

Ensure Data Is Safe

Access control and authentication

- User permissions: Limit access to employee data based on roles (e.g., HR, managers)
- Strong authentication: Implement multi-factor authentication (MFA) for secure logins

Data encryption

- In transit: Encrypt data during transmission using protocols like TLS/SSL
- At rest: Store data in encrypted formats (e.g., AES-256) to prevent unauthorized access

Regular audits and monitoring

- Access logs: Monitor who accesses employee data and when
- Suspicious activity: Detect anomalies and investigate promptly

Data minimization

- Collect only what's necessary: Avoid unnecessary data collection
- Purge obsolete data: Regularly delete outdated records

Ensure Data Is Safe (cont'd)

Employee training

- Security awareness: Educate employees about data protection best practices
- Phishing awareness: Train them to recognize phishing attempts

Vendor security

- Third-party vendors: Assess their security practices before sharing employee data
- Contracts: Include data protection clauses in vendor contracts

Secure physical storage

- Locked cabinets: Store physical records securely
- Access control: Limit entry to authorized personnel

Incident response plan

- Breach preparedness: Have a plan in place for data breaches
- Communication: Notify affected parties promptly

Policies

- Outline how the organization collects, uses and discloses employee data
- Ensure provision of requisite notices and consent (e.g., CCPA, monitoring, biometric)
- Explain reporting of data incidents, breaches and misuse
- Set forth cybersecurity policies that are buttressed with employee training
  - Administrative
  - Physical
  - Technical
  - Organizational

Questions?

JacksonLewis

Thank You!

JacksonLewis