# Employee Privacy in the Digital Workplace

Third Annual Labor & Employment Law Summit

January 23, 2020

# Introductions

- Ellen Blanchard
  - Managing Corporate Counsel, eDiscovery, T-Mobile
- Mike Burg
  - Senior Counsel, Privacy and Data Security, Zillow Group
- Angela Galloway
  - Corporate Counsel, Privacy, Nordstrom
- Joelle Hong
  - Corporate Counsel, Privacy & Data Security, Convoy

- Maureen O'Neill
  - SVP, Strategic Engagement, Consilio

# Meet the Human Resources Team at Washington.AI

Sam Ken Brandon Brian Diana David

Diana is the EVP of Human Resources at WAI. She's been doing a lot of reading lately on personal data privacy—it's a hot topic in the news these days.

She'd like to understand better how the concept of privacy applies in the workplace, and what privacy rights the employees at WAI have.

# Employee Workplace Privacy Rights

- Rights arising from the "Reasonable Expectation of Privacy"
- Rights and protections granted by other specific sources:
  - Statutes/regulations (biometrics, credit information, geolocation tracking, HIPAA)
  - Collective bargaining agreements
  - Contractual provisions
  - Public employees (4th Amendment)
  - Employees based in the EU and other non-US jurisdictions

David is a junior HR staff member. David is frequently late for work, which Diana knows because WAI tracks the time employees log on to their computer each day and provides reports on the time employees swipe their badges when they enter the building. Diana also knows that the first thing David does each day when he arrives at work is to log onto his personal Gmail account to check his messages.

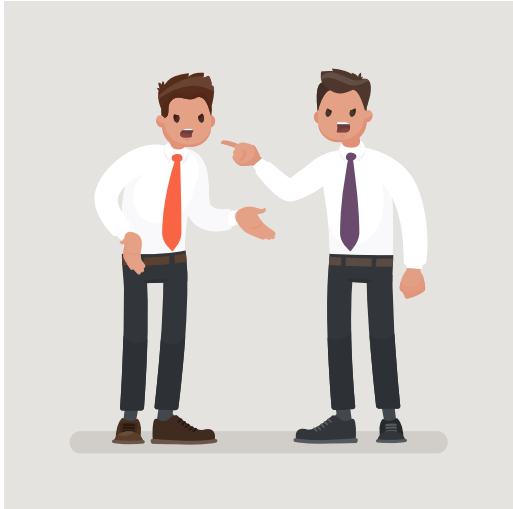
Ken is a senior member of Diana's HR team. He wakes up early every day for a workout. Whenever he works out, Ken wears a fitness tracker given to employees by WAI as a perk. He often participates in contests organized by WAI that reward employees for the number of steps logged by their trackers.

# Surveillance of Individual Employees

- Monitoring and tracking computer/network activity
  - *Context*—Tracking when activity is taking place, what devices are being used, where the activity takes place
  - *Content*—Monitoring the substance of communications and documents, and/or the nature of the activity (web sites visited, applications opened, etc.)
- Physical tracking
- Geolocation tracking
- Video/audio surveillance
- Fitness trackers/smart watches

When employees at WAI meet, they are asked to open an app that records the meeting. The recordings are then subjected to a tonal analysis, which can diagnose culture issues on a team, showing who dominates conversations, who demurs, and who resists efforts to engage in emotional discussions.

WAI also deploys software that analyzes emails to understand who employees interact with, how quickly colleagues reply, and who is most influential. The analysis also uncovers signs of conflict—which revealed that Sam and Brian have been arguing repeatedly about petty workplace issues.



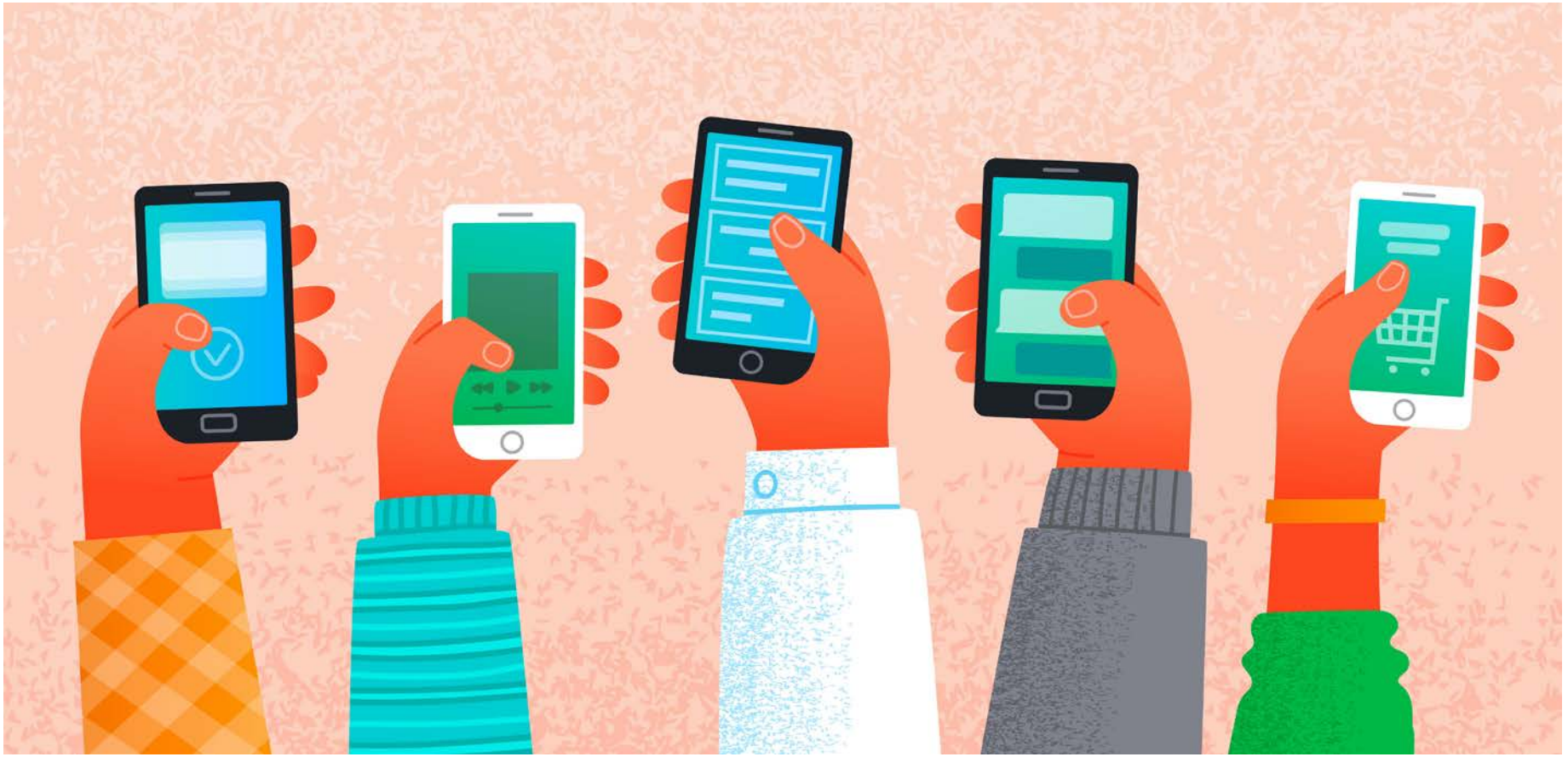
Sam and Brian manage the recruiting function at WAI. They recently started using a service that applies artificial intelligence to submitted resumes and job-seeker databases, and suggests which candidates will be the best fit for open positions. This service has saved them hours of time previously spent manually reviewing resumes. But Sam is a bit worried that the software seems to select a disproportionate number of men for job openings at WAI.

# Analysis of Aggregated Employee Data

- Analysis of email and other communications to determine relationship and networking patterns
- Tracking and measuring the frequency and duration of chats, emails, and meetings to assess productivity and time management
- Tonal analysis of emails, phone calls, conference room conversations, Slack channels, etc. to assess cooperation and conflict
- Use of AI to screen candidates, select employees for hire and promotion, and identify high potential employees

WAI has a voluntary BYOD program, which allows employees to use their own devices for work if they choose, and many WAI employees use their personal smartphones and laptops at work. But employees may opt for a company-owned device instead.

Diana chose the BYOD route, but she is becoming concerned about WAI's ability to access the personal information found on her devices. Susan has a phone issued by WAI, but recently she's been using it to send personal emails because her own phone is old and slow.



# Co-Mingling of Business and Personal Data

- Pervasive "co-mingling" of business and personal data:
  - BYOD devices: Phones, tablets, laptops, etc. that are owned by the employee and used for both work and personal matters. These devices typically contain substantial personal data.
  - Company-owned devices: Hardware owned by the employer and issued to employees for business purposes. Employees sometimes use these devices for personal matters as well.
- Software solutions exist that can help segregate data and applications into business vs. personal.

WAI encourages employees to be active on LinkedIn. The company asks employees to follow the company and share the latest WAI news on their personal feeds.

But WAI prohibits employees from posting about the business on their personal pages at Facebook, Instagram, and other social media platforms—the company monitors employees' personal social media feeds for content related to its business. Brandon recently was asked to take down a Facebook post about WAI's email analysis program.

# Monitoring and Restricting Social Media Usage

- Employees' use of social media while at work may be purely for business, purely personal, or a mix of both.
- Employees are often encouraged to use social media to promote the business—and employers have an interest in monitoring social media content related to the company.
- Using employees as "influencers" for social media marketing raises issues regarding advertising laws, including FTC guidelines on paid endorsements.
- When the company needs to collect information from a social media account, it's difficult to parse business content from personal.

WAI's General Counsel recently paid a visit to Diana. She explained that the company has been sued by a group of women claiming that the company discriminated against them on the basis of gender by failing to hire them as software engineers. The GC asked Diana to gather the personnel files of every employee in the engineering department and deliver them to the in-house legal team.

The GC also told Diana that WAI is looking to take on a new private equity partner. In connection with this round of funding, she needs Diana to prepare a spreadsheet with current and historical compensation information for every executive above the level of Vice President.

# Using Employee Data Outside the "Business-as-Usual" Context

- Employers collect various types of highly sensitive personal information from their employees, such as SSN, driver's license numbers, DOB, bank account info, health insurance information, etc.
- Employees should reasonably expect that such information will be used by the company for purposes consistent with the reasons for collecting it—to run the business, comply with regulatory requirements, offer and administer employee benefits plans, etc.
- But there will instances when the company must use this personal information in other contexts, such as in litigation and regulatory matters and corporate M&A transactions.

# Questions?