Employee Privacy and the 2023 Hybrid Workplace

Practicing Law Institute
24th Annual Institute on
Privacy and Cybersecurity Law
San Francisco, CA
May 8, 2023

Margaret Keane
MKeane Law
Margaret@mkeanelaw.com

Joanie Dillett
Axiom Legal

Agenda

- Introduction and Overview
- Emerging Employee Privacy Challenges in 2023
  - Surveillance and Employee Monitoring for Performance and Productivity
  - Evolving Privacy Standards for Communications and Data in Hybrid/Remote Work
  - Data Security Practices for “work from anywhere”
- Coming Attractions: AI meets the workforce

Surveillance and Employee Monitoring

Poll: 1. Is your company actively tracking in-office presence for employees?

Poll: 2. Are you using this data for any purpose other than payroll?

US: Surveillance and monitoring considerations

Some of the Tools:

- Audio and Video monitoring
- Surveillance – RFID, CCTV, GPS
- Biometrics – fingerprint log-in; retina scans
- GPS monitoring via smart phone or vehicle tracking
- Social media activity
- Software/apps showing away or on-line status; meeting tracking; calendar activity
- Keystroke logging
- Email monitoring
- Wellness tracking

US: Surveillance and Monitoring Considerations

Identify business rationale

- Improve Productivity. Address concerns about in or out-of-office productivity
- Protect Company Assets, including trade secrets
- Facilitate compliance and audits in regulated industries – e.g., FINRA, HIPAA
- Health and Safety Objectives
- Monitor employee engagement
- Measure attainment of SLA's and customer satisfaction

US: Surveillance and Monitoring Considerations

Increasing Regulatory Interest and Legislative Activity

- NJ: As of 4/18/2022, NJ requires notice of devices used to track movement of person, device or vehicle.
- NY: New law requiring prior written notice to monitor employee phone calls, email or internet access became effective 5/7/2022
- CA: AB 1651 (Workplace Technology Accountability Act) failed. Mandated notice and prohibited off-duty tracking, facial recognition technology and using algorithms in termination decisions
- NLRB GC Memo 23-02, calls for "vigorous" enforcement of existing surveillance policies governing organizing and includes proposed framework for broad standards beyond union organizing

U.S.: Surveillance and Monitoring Considerations

On-site Surveillance

- Cameras should be visible, not hidden or obscured, and clearly identified.
- Avoid use of CCTV cameras in places where employees have a reasonable expectation of privacy (e.g., restrooms, locker rooms).
- Avoid surveillance of employees engaged in organizing and NLRA protected activities
- Have a policy governing use of cameras with stated purpose(s) for using cameras, locations and times of operation. Video surveillance does not include audio recording.
- RFID can also be used to monitor on-premises activity. Notice is advised.

Voice Recording

- Most states only require one party to the telephone call to consent to the telephone recording
- Others --CA, CT, DE, FL, IL, MA, MI, NV,PA and WA either require all parties consent and/or some form of notice.
- Inform employees about the nature and extent of telephone recording and set out clearly in policies the circumstances in which employees may or may not use the employer's telephone systems (including mobile phones).

Internet Use Monitoring

- Permissible
- Notice required
- California: Disclose on CCPA notice

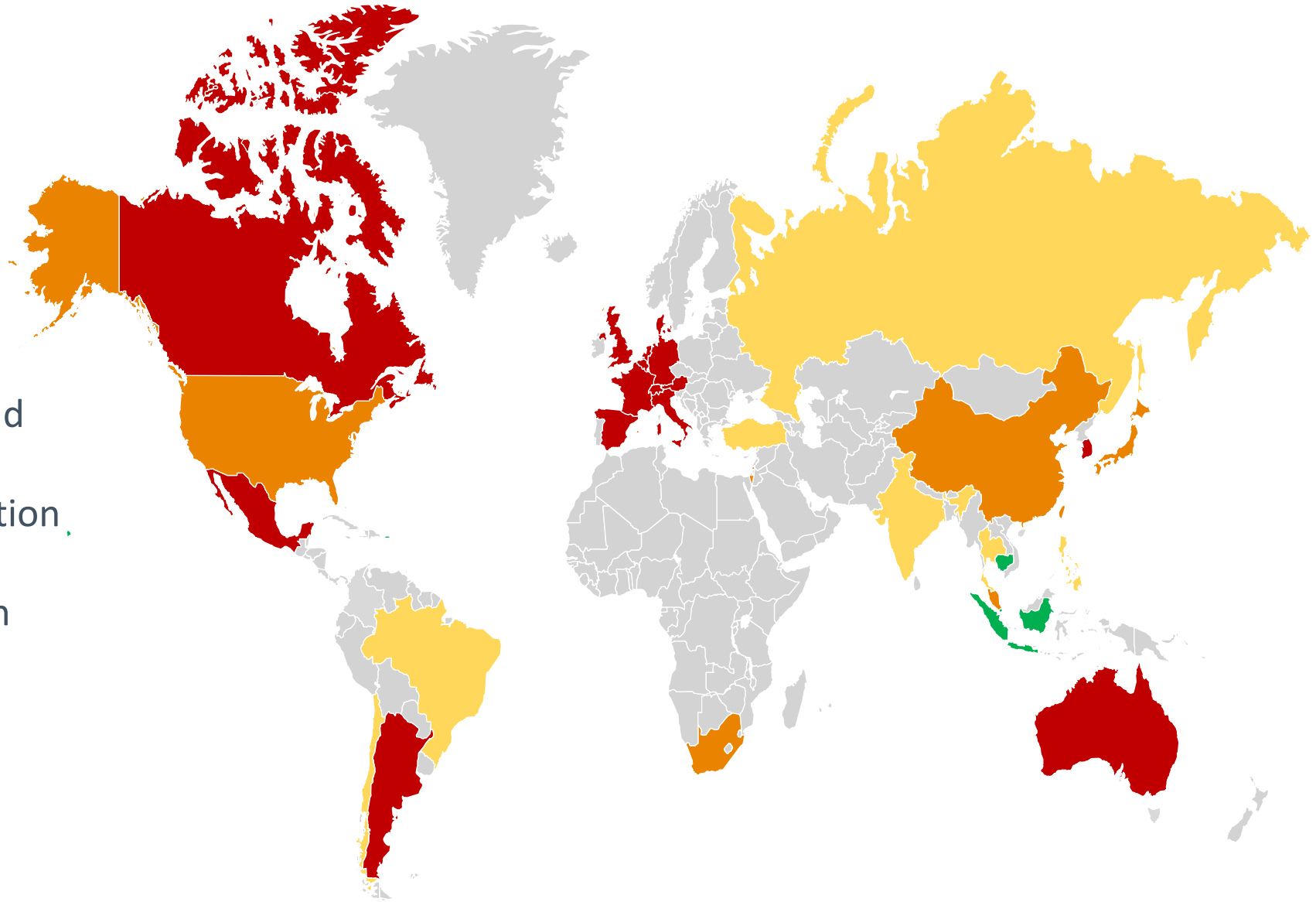
Keystroke Monitoring

- Not strictly prohibited if equipment provided by employer
- Notice / consent
- Wiretapping laws / case law
- May generate employee resistance

E-mail / Instant Message Monitoring

- Generally permissible on employer systems
- Exercise caution on BYOD devices
- Notice required
- State laws: Connecticut, Delaware, Colorado and Tennessee

International: Surveillance and employee monitoring



- Low regulation and enforcement
- Moderate regulation and enforcement
- Robust regulation and enforcement
- Heavy regulation and enforcement

- **Surveillance and employee monitoring**

Privacy

- E.g.,
- **EU**: GDPR
- **Singapore**: PDPA
- **Brazil**: LGPD

Surveillance / Communications

- E.g.,
- **Australia**: Workplace surveillance laws in NSW and ACT
- **Taiwan**: Communications Protection and Surveillance Act

Teleworking

- E.g.,
- **Portugal**: Law No. 83/2021 (effective Jan. 1, 2022)
- **Spain**: Law 10/2021 on remote working (effective July 9, 2021)

Employment

- E.g.,
- **Italy**: Article 4 of Law 300/1970
- **Switzerland**: Swiss Code of Obligations and Ordinance 3 to the Federal Labor Act

Evolving Privacy Standards for Video Collaboration and Communication Tools

Poll: 3. Do you record internal Video meetings? Ex. Zoom, Teams

Poll: 4. If yes, do you have a Retention Policy for managing these recordings?

Video Collaboration and Communications Tools:

meetings, chat, VoIP phone, social media platforms and more

FOR ALL USES:

- Update policies to reflect that anti-harassment, anti-discrimination, Code of Conduct and other policies apply to ALL employment communications, regardless of informal/formal nature, communication mode, or sender location
- Advise employees that they have no expectation of privacy when using these tools and should not share private information
- Consider adding/updating electronic resources policy
- Restrict access to current employees, ensure access ends upon termination
- Determine whether, when and how audio communications will be recorded
- Develop procedures to give notice and get consent for recordings where required and/or desired
- Update your retention policies

Video Collaboration and Communications Tools:

meetings, chat, VoIP phone, social media platforms and more

FOR MESSAGING APPS

- Develop processes for reporting and resolving complaints of inappropriate use – ex. Hate speech, personal insults using racist or sexist terms, offensive emojis
- Identify channels that the employer recognizes as official public communications channels – e.g., public Slack channels – and adopt appropriate policies for access and review, designate administrator, etc
- Develop separate protocols for private channels for internal use and those shared with third parties

Video Collaboration and Communications Tools:

meetings, chat, VoIP phone, social media platforms and more

FOR MEETING TOOLS – a few questions for discussion

Can my employer make me use the video feature on video calls?

Can my employer make me leave the video feature on all day to see what I do?

Can I have personal items in the background that others might find offensive?

Can my employer limit who's in the room with me?

Data Security for a Remote Workforce

Employers:

- Identify roles that require limiting company communications to secure company issued devices
- Update BYOD policies; obtain consents for remote wipes and accepting company software updates and consent to present device for inspection if requested
- Audit to ensure former employees are severed from access to all systems and databases
- Train employees when and how to encrypt specified communications and data
- Train employees to recognize scams and notify IT
- Update and modernize retention policies
- Provide ongoing training on privacy compliance

Data Security for a Remote Workforce

Employees:

- Always connect using Company's protocol, ex. private network – VPN
- Avoid public wi-fi networks, use cellphone hotspots or secure connections
- Be careful about shoulder surfing/screen displays working in public places
- Implement security software on personal devices used for work
- Develop travel policies for domestic and international travel
- Don't share computers or smart phones with family
- Complete security training regularly

Looking Ahead: AI at Work

Beyond our scope today, but look out for privacy issues with:

- AI systems in the workplace
- Automated decision-making tools
- Generative AI / ChatGPT
- NYC AI Bias law – NYC 144- enforcement deterred until July 5, 2023

Questions?