



Lunch and Learn:

**Electronic Monitoring
and Surveillance in
the Workplace**

What is data?

- Data is facts, statistics, and other pieces of information used to analyze something or to make decisions about something.

What types of data are employers collecting about us?

Examples of Data Collected and Used in the Workplace

<u>Workplace activities, interactions data</u>		<u>Job activity data</u>	
• Body movements • Co-worker interactions (<i>in person, by phone, text, email, collaboration tools</i>) • Location (<i>workstation, building, in the world</i>) • Peer reviews	• Performance reviews • Restroom access and use • Safety habits • Smart phone use, Wi-Fi access, instant messaging • Time clock • Video and audio recordings of work performed	• Calendar (<i>how much of your day is spent in meetings, who you are meeting with, how long</i>) • Computer (<i>system log ins, keystrokes, screenshots, application use, time spent working on a task</i>) • Customer service interactions (<i>calls, claims, customer ratings and reviews</i>) • Driving (<i>vehicle location - GPS, braking patterns, route, speed, accidents, behaviors while driving and in the vehicle, conversations, cell phone use</i>) • Internet (<i>email content and who was emailed, file downloads, web searches</i>) • Machine interactions (<i>handheld devices, industrial machines, robots, wearables, photocopiers</i>)	
<u>Health and wellness data</u>		<u>Biometric data</u>	
• Exercise activity • Heart rate and respiration • Menstruation and pregnancy tracking • Overall movement and activity levels • Sleep patterns		• Body language, walking gait • Eye movements • Facial geometry, facial expressions • Fingerprint, palmpoint, ear print	• Hand geometry • Iris or retina scan • Tone of voice
<u>Cognitive and behavioral data</u>		<u>Historical data</u>	<u>Digital footprint</u>
• Cognitive function assessment results • Personality test results • Questionnaire and survey responses • Skills test performance • Virtual, augmented reality device use		• Credit report • Consumer activity • Driving record • Education • Employment, salary history	• Health screening, alcohol, drug test results • Professional licenses, certifications • Residences • Volunteer activities
			• Internet presence, blogs • Online forum activities • Social media activity



Source: Lisa Kresge, [Data and Algorithms in the Workplace: A Primer on New Technologies](#), UC Berkeley Labor Center, November 2020.

Why do employers monitor workers?



Employers monitor workers because

Data is POWER!



How is worker data used by Artificial Intelligence (AI)?

- **Artificial Intelligence models** are trained on large amounts of data and recognize patterns in that data.
- **Predictive AI:** AI models that make “predictions” about future outcomes.
- **Generative AI:** AI models that “generate” content, such as writing, images and videos.
- **Agentic AI:** AI models that operate autonomously to accomplish specific tasks or goals.

Harms from employee surveillance and monitoring without guardrails

- Loss of privacy
- Harm to worker morale
- Harm to worker safety and health
- And harms from the use of this data...



Harms from the use of data collected through employee surveillance and monitoring without guardrails

- Automation / replacement of work by technology
- Work-flows intensified or sped up to unsafe levels
- Loss of worker autonomy
- Reduced public service quality and safety
- Use by AI systems to make employment decisions
- Biased data can lead AI systems to make biased recommendations or decisions
- Attacks on union activities and worker solidarity – “Algorithmic Union Busting”



“Algorithmic Union Busting”

What kind of surveillance could help employers engage in anti-union actions?

- Audio or video recordings
- Email monitoring, employer equipment monitoring
- Location data
- Who people interact with, how long they interact
- Social media
- Private employee group chats and email groups
- *What else?*



Bargaining – Establishing Guardrails Against Harms from Surveillance and Monitoring

- About a third of union members reported having at least one provision related to automated management or surveillance in their CBAs.
 - Half were in place before 2022

How has Surveillance Changed?

- Analyzing worker behavior
- Combining data across systems
- Commodification of data
- Biometrics

SURVEILLANCE PROVISIONS

"Use of surveillance cameras/monitors is primarily for security reasons. However, surveillance footage may be reviewed to determine misconduct and to determine appropriate disciplinary measures. Management may review surveillance footage to investigate specific complaints or concerns about employee misconduct. If evidence of misconduct is found within the surveillance footage, then the footage may be used to process disciplinary actions. If discipline is brought against the employee due to surveillance footage, the employee in question may also request to review the footage..."

BROAD ELECTRONIC MONITORING DEFINITION

“Use of surveillance cameras/monitors electronic monitoring is primarily for security reasons. “Electronic monitoring” means the collection, recording, observation, tracking, or analysis of employee activity, communications, location, movement, physical or behavioral characteristics, biometric information or work performance through electronic devices or systems, including cameras, GPS, audio systems, software, and artificial intelligence or algorithmic tools.

DATA SECURITY AND WORKER PRIVACY

Electronic monitoring data will be encrypted and stored securely and will only be stored for as long as necessary for its stated purpose. The Employer will not share or sell data collected on employees to any third party. In the event of a data breach, the Employer will immediately notify affected employees and take corrective steps in a timely manner. Access to electronic monitoring data will be limited to personnel with legitimate operational need.



HUMAN REVIEW

Any automated inference must be independently verified and not used as the sole basis for discipline.

DUTY TO BARGAIN

Electronic monitoring will not be implemented, expanded, or modified without prior notice and bargaining with the Union.

Other guardrails...

- Employee notice and/or consent
- Limiting data collection to only when is necessary for operations
- Specifying retention periods

BARGAINING RESOURCES

- [AFSCME Contracts Database](#)
- Limited sample language
- Model language
- New technology information request template
- Sample language from other unions upon request
- [Berkeley tech language database](#)
- Bargaining over AI workshops
- Additional research support upon request!

Legislation – Establishing Guardrails Against Harms from Surveillance and Monitoring

- **Certain types of electronic monitoring should be prohibited**
- **There should be limits on other types of electronic monitoring**, with requirements around
 - Providing notice to workers about what type of monitoring is occurring and the monitoring's purpose
 - Allowing employees to have access to their data, and the opportunity to correct mistaken data
 - Data minimization - employers should only be allowed to collect the minimum amount of data to accomplish the purpose of data collection
- **Strong protections for data security – how that data can be used, stored and accessed**
- **Certain uses of worker data should be prohibited**



Questions, Discussion

- Reach out to work with us on legislative or bargaining language, if we can provide other kinds of support or to ask questions!
 - Jenny Ho – jho@afscme.org
 - Christine Silvia-DeGennaro – csilvia@afscme.org
 - Research@afscme.org

