Protecting Worker Privacy:

Electronic Surveillance Contract Language

Overview

The IAM has always fought for a say in Management's use of new technology in the workplace. Employers are consistently trying to use technology to monitor and track workers, often with disciplinary implications. Within this memo, we will provide model contract language to combat these issues and protect employee privacy on the job.

Background

Throughout history, the implementation of technology has had a direct impact on workers' job content and employment. Its introduction can also raise privacy and disciplinary issues beyond the literal performance of job duties.

Specifically, new surveillance and monitoring technology can pose a unique threat to employee rights in the workplace. It can:

- Force workers to self-censor their discussions about working conditions, for fear of the boss listening.
- Stifle workplace activism, discourage member engagement, and reduce campaign participation by making workers afraid their bosses will be able to identify them as pro-union.
- Allow Management to use video or audio evidence to discipline or fire workers.
- Track worker productivity, potentially leading to forced speed-ups, unsafe working conditions, and increased workplace injuries.
- Violate workers' personal privacy, especially for workers who regularly use computers.
- Track employees' locations on and off the job through vehicle or cellular monitors or other geolocation-tracking applications.
- Subject employees to discipline for social media presence.

These systems affect workers in all types of workplaces. According to the *Nation*, "nurses in Florida wear geolocation tags to track the time they spend with patients and how efficiently they move through the hospital."[1] Some workplaces that are computer-centric or rely on remote teleworking use software called WorkSmart, which takes screenshots of workers' screens and then combines them with measures of app usage to measure productivity. The WorkSmart website brags that when the system is on, "it will use keyboard activity, application usage, screenshots, and webcam photos to generate a timecard every 10 minutes."[2]

[1] https://www.thenation.com/article/worker-surveillance-big-data/
[2] https://www.crossover.com/worksmart-productivity-tool

Warehouse workers are also at the forefront of workplace surveillance. Amazon recently patented a watch that would emit ultrasonic sound pulses and radio transmissions to track where an employee's hands were in relation to inventory bins, and provide "haptic feedback" to steer the worker toward the correct bin[3] and to track "time consuming" tasks like taking a break or using the restroom. [4] Other Big Tech companies are working on implantable—and trackable—RFID microchips that would go under the skin and could be monitored in a similar fashion.[5]

Prohibiting Surveillance

Prohibiting workplace surveillance should be a goal for every contract. Language below represents an ideal prohibition. (If you are unable to secure this language, fight to include the right-to-know and defining purpose and scope clauses below.)

> *"The employer will not monitor, surveil, or spy on employees through any means. The employer will not track via GPS or other tracking device the movements or location of employees. The employer will not install cameras or recording devices without the informed consent and mutual agreement of the union.*
>
> *The Company will not view, examine, or monitor employee's social media. Social media postings will not be the basis of, or admitted as evidence to any disciplinary action. Such postings will also not be examined during an employee evaluation, or review."*

If the employer insists on surveilling employees, and you are unable to secure the prohibitive language above, the CBA can include other clauses seen below.

Right-to-Know Clauses

This type of clause focuses on notifying employees and unions before companies install surveillance equipment, and requiring employers share what the data is used for.

> *"The Company must notify all employees and union representatives X days before the introduction or expansion of any type of employee monitoring/electronic surveillance devices, including, but not limited to cameras, audio recorders, GPS devices, RFID chips, biometric data, keystroke logging, computer screen monitoring.*
>
> *The Company agrees that employees have a right to access any and all data collected on them, and that employees must be able to obtain without excessive delay copies of personal data relating to him or her. The employee also has the right to have personal data rectified, blocked, or erased and should be furnished the results of such data collection (if there are any).*
>
> *Information shall be furnished to the employee's union representative only to the extent that such data is necessary to dutifully represent the employee."*

[3] https://www.theverge.com/2018/2/1/16958918/amazon-patents-trackable-wristband-warehouse-employees
[4] https://www.thenation.com/article/worker-surveillance-big-data/
[5] https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html

Definition of Purpose and Scope

This language defines the intent of surveillance equipment, and limits its usage to certain areas and purposes.

> *"Any and all data collected by the Company through electronic surveillance devices shall be used for safety and security purposes only. Electronic surveillance equipment is not intended to invade the privacy of employees. Data will not be used for any other reason, such as but not limited to:*
>
> - *Employee discipline*
> - *Productivity monitoring*
> - *Employee review or evaluation*
> - *Random or individual employee audits*
> - *Aiding a criminal investigation (unless a proper warrant has been furnished)*
>
> *Surveillance equipment will not be installed in non-work areas, including restrooms, break rooms, kitchens, lunchrooms, etc. The Employer must meet and confer with the Union in deciding the location, number of, and orientation of all surveillance devices.*

Monitoring of Social Media

Employers often inspect their employees' social media before and after being hired. The NLRB has generally found that employee social media posts are protected activity that they cannot be disciplined for if the posting is related to group action rather than individual gripes. Union collective bargaining agreements can strengthen these protections.

> *"The Company will not view, examine, or monitor employees' social media. Social media postings will not be the basis of, or admitted as evidence to, any disciplinary action. Such postings will also not be examined during an employee evaluation or review."*

Several states have enacted legislation that protects employees' social media accounts from employer snooping. For the states where no such legislation exists, the following language may be useful:

> *"The Company shall not request, require, or otherwise coerce an employee to:*
>
> *1) disclose login information for the employee's personal social networking account;*
> *2) access his or her personal social networking account in the employer's presence in a manner that enables the employer to observe the contents of the account;*
> *3) compel or coerce an employee to add a person, including the employer, to the list of contacts associated with the employee's personal social networking account; or*
> *4) cause an employee to alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account.*
>
> *Furthermore, the employer shall not take adverse action against an employee because the employee refuses to disclose his or her login information, access his or her personal social networking account in the employer's presence, add a person to the list of contacts associated*

with his or her personal social networking account, or alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account."

Right to Use Email and Internet at Work

Many IAM members use computers for work. Occasional personal use is almost always permitted, despite many employers' stated "zero tolerance policies" to the contrary. Contract language can help ensure that these policies are not unfairly enforced to discipline particular workers.

"Keystroke or screen monitoring technologies will not be installed or used on computers used by employees. Employees should use their workplace technology and equipment primarily for work related purposes, but employees may from time to time need to use workplace technology and equipment for important personal matters. Such uses will not be considered violations of any work rule."[6]

[6] Some language in this document comes from District 140 Local 2323 Machinist contracts and from UNI Global Union's report on *Top 10 Principles for Workers' Data Privacy and Protection*