

## **Does the Employer Hold All the Cards: How and When Can Employees Fight Back?**

Matt Shechter  
General Counsel,  
United Food & Commercial Workers, Local 7

- The General Rule: No Reasonable Expectation of Privacy in the Private-Sector Workplace
  - Brief note on historical development
- The Many, Many Exceptions – Context Always Matters
  - Numerous state and federal laws place substantive restrictions on the right of the employer to monitor its staff.
    - Electronic Communications Privacy Act
      - Under Federal Law, employers can monitor/collect telephonic (and sometimes other electronic) communications made in the workplace in most cases with employee consent. Even without consent, can be done for legitimate business reasons.
        - But what about when you are listening to the message you collected?
      - But be wary of state restrictions – some (California, Connecticut, others) specifically require an employer to advise as to the scope of monitoring in advance or prohibit any monitoring unless all parties consent (Maryland, Penn.)
    - Stored Communications Act (Another piece of ECPA)
      - Access Without Authorization
      - Exceeding Authorized Use
    - NLRA
      - Section 7 Rights
      - 8(a)(5) implications in unionized workplaces
    - Many other statutes can come into play depending on the context
  - Arbitrators left to fill in the gray areas have taken a variety of approaches.
- Monitoring of an employee's social media ("SM")
  - My boss has no right to access my Facebook page (even if I did put it out there for the whole wide world to see), does she?
    - State laws (~20 states) that prohibit employers from asking for personal (employee) SM passwords
    - Example: what if I left my work cell phone logged in to my personal Facebook?
  - Even if there's a right of access on the part of the employer, employees may still be in a "safe" space.
    - Protected, concerted activity
      - NLRB GC Memo 23-02
    - Smoker's rights statutes / off-duty conduct laws
    - Title VII / anti-discrimination law considerations
    - Just Cause
    - Example: XYZ Company employee Facebook page

- Video/Audio Surveillance
  - Now where did you put that camera?
    - Cameras/Audio Recording in Breakrooms/Cafeterias
      - Because of the limited nature of the employer's interests in these areas combined with the high likelihood they might capture personal and/or NLRA Section 7 activity, cameras in these areas are almost certainly going to be unlawful.
        - Wiretap Act / Statutory / Criminal Penalties
    - Off-the clock monitoring
  - Did you bargain for the right to have that camera (unionized workplaces)?
    - Cameras in the workplace are a mandatory subject of bargaining
    - Management rights clause / *MV Transportation*
  - Surveillance during organizing campaigns / in response to Section 7 activity
- Monitoring communications made on employer-owned devices
  - Broadly speaking employers have the right to monitor what is done on devices/systems owned by the employer.
    - Internet Use Monitoring
  - When on an employee owned system, employees are most likely to have protected rights when communications are at issue.
    - Does the employer permit employees to chat about non-work subjects in the company Slack?
    - Monitoring of which co-workers an employee is calling on his company-owned cell phone.
    - SCA – employee's access of personal Gmail on company owned system.
    - GPS/location tracking
- Artificial intelligence – the next battleground