INTERNATIONAL ASSOCIATION OF FIRE FIGHTERS

TECHNOLOGY, DATA PRIVACY, AND AI IN FIRE OPERATIONS FOR YOUR UNION

March 31, 2026

OBJECTIVES

Technology and Legal Risks

- Learn to identify legal and privacy risks from technologies like body cameras and biometric tracking in disciplinary contexts

Negotiating Technology Policies

- Explore negotiating safeguards such as access controls, retention limits, and member consent for biometric data use

Emerging Legal Frameworks

- Review new laws restricting AI and facial recognition use in public sectors

Responsible Social Media Use

- Best practices on protecting reputations, securing communications, and complying with laws on speech

BODY CAMERAS AND EMS PROVIDERS

USE OF BODY CAMERAS – LAW ENFORCEMENT

47%

Of law enforcement agencies have acquired body worn cameras

95%

Of police departments with 500+ officers have adopted use of body worn cameras

50%

States have mandated body worn cameras statewide

CONCERNS REGARDING USE OF BODY CAMERAS

Traditional privacy of medical examinations and treatment could be impacted

- EMT and paramedic interaction with police at crime scene, scene of accident, back of an ambulance, hospital emergency room
- Private Health Information (PHI) recorded during emergency medical treatment
- Impediment to free, open physician-patient dialogue/patient forthrightness and trust impacts ability of emergency medical employees to properly diagnose and treat

FEDERAL HIPAA CONCERNS

FEDERAL LEGISLATION: HIPAA

Health Insurance Portability and Accountability Act (HIPAA)

- Enacted “to protect the confidentiality, integrity, and availability of electronic protected information.”
- Prohibits disclosure of “individually identifiable health information,” defined as:
  - Any information collected from an individual;
  - that is created or received by a covered entity;
  - relates to the condition of said individual or the provision of health care to said individual; and
  - identifies the individual or can be used to identify the individual.
- Could bridge the privacy gap among states, but only applies to “covered entities”

FEDERAL LEGISLATION: HIPAA

- HIPAA requires EMS agencies to safeguard protected health information (PHI), but it does not expressly prohibit the recording of patient encounters.
- Body camera recordings may be used for treatment, healthcare operations, and other purposes permitted by HIPAA's Privacy Rule.
- EMS agencies, as employers, can use body camera footage for healthcare operations activities allowed by HIPAA, such as quality assurance, employee evaluation, and developing clinical protocols.
- Safeguarding body camera footage containing PHI is crucial to prevent a “breach”, which requires reporting by the EMS agency. Lack of clear guidelines and policies, as well as inadequate training, may lead to disciplinary issues for IAFF members. To address these concerns, EMS agencies should establish comprehensive procedures for the use and storage of body cameras and ensure proper training for employees.

REGULATION OF USE

- As it stands now, EMS body camera footage containing PHI is largely unregulated.
- The lack of regulation, and the lack of clarity in regulations that do exist, creates a series of potential problems for IAFF members.
- Locals should ensure that the wearing, usage, and storage of body cameras is set forth in clear and comprehensive procedures and that employees are afforded ample training on those procedures.

HIPAA AND MEDICAL PRIVACY – "WHAT COUNTS AS PHI?"

An EMS crew's camera accidently records a patient's face, conversation, and medications that are visible on their counter. A supervisor later uses the footage in a performance evaluation, but the agency has no formal HIPAA-compliant storage procedures.

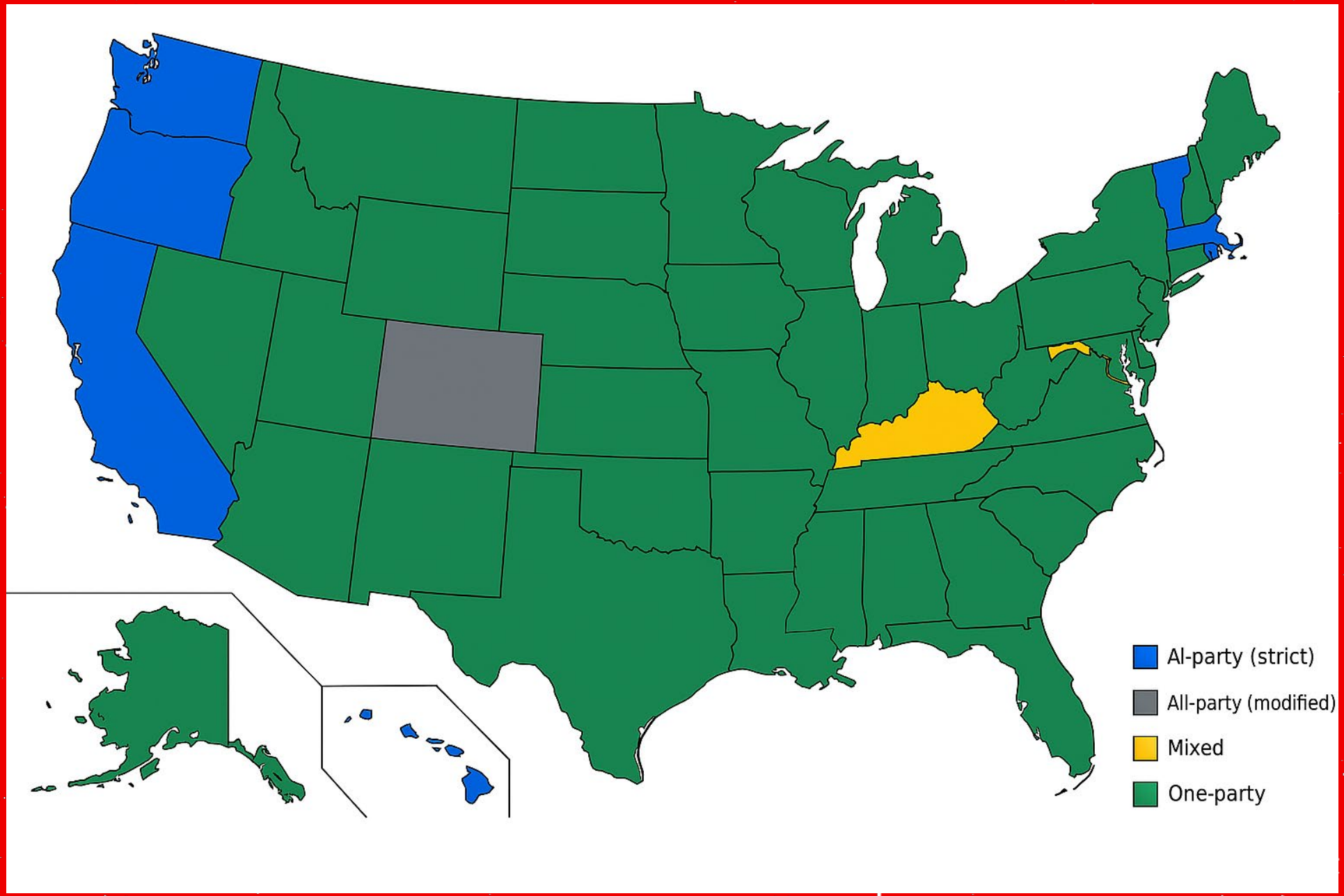
QUESTIONS

1. What in the video is considered PHI under HIPAA?
2. What new disciplinary risks does this create for members?
3. What policy language should locals insist on around storage, access, security, training, prohibiting unauthorized uses?
4. What parts should not be used for discipline?

STATE CONSENT LAWS

ONE PARTY VS. TWO PARTY CONSENT

- States have varying wiretap/eavesdropping laws requiring a person recording a conversation to provide notice and obtain consent before recording
- Some states require consent of all parties being recorded before recording
- Most only require the consent of one party to a recording
- Important for IAFF members to know the consent requirements of their states


Al-party (strict)
All-party (modified)
Mixed
One-party

STATE PRIVACY AND CONSENT LAWS – "TO RECORD OR NOT TO RECORD"

Your state is a two-party state for audio recording.

You arrive at a chaotic scene in a private home with a distressed patient, family arguing, and police present.

Pressured for time, the medic forgets to inform the patient that the camera is running.

A family member complains

QUESTIONS

1. What are the legal risks for the member?
2. What contract/policy protections does the union need?
3. Should cameras be required to be turned on at all times, or under specific circumstances?
4. How do “intrusion upon seclusion” laws affect EMS entering a home?

OTHER STATE LAW CONSIDERATIONS

STATE LEGISLATION: PRIVACY LAWS

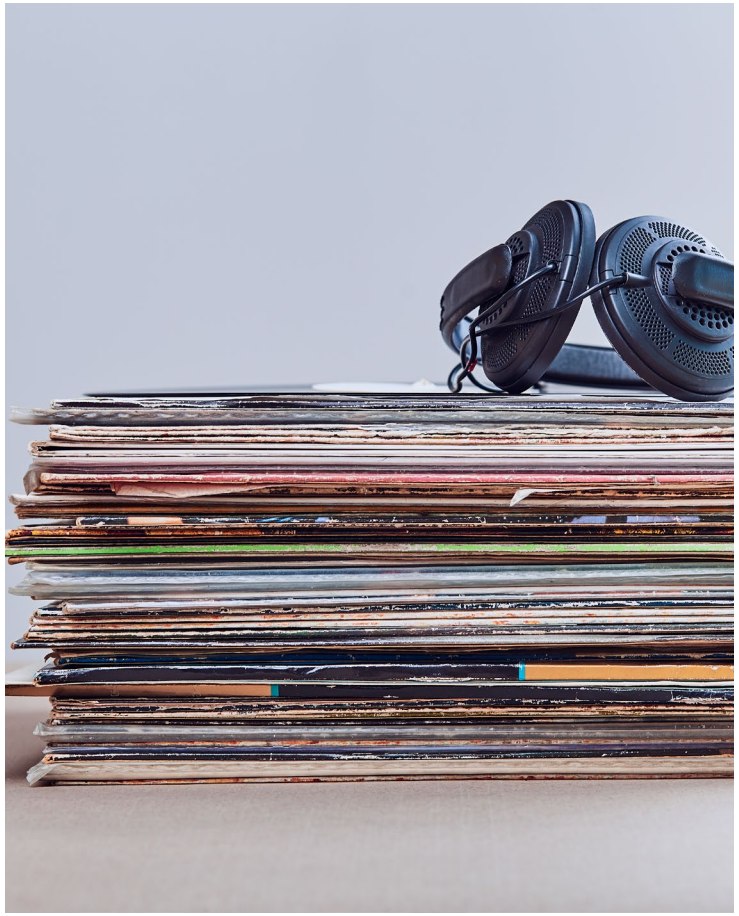
- Prohibits use of body cameras during medical evaluation or treatment (Connecticut)
- Exempts from public records law
  - All police body camera footage (Illinois)
  - Court approval required for access to body camera footage (North Carolina)
  - Footage taken in medical facilities (Florida, Washington State)
  - Footage taken in a “private place” (North Dakota)
  - Footage taken of a minor (Washington State, Connecticut, Oklahoma)

STATE LEGISLATION: PUBLIC RECORDS LAWS

- Body camera footage often available to public
- While such laws may exempt records relating the medical treatment, often ambiguous and largely untested
- Weighing public's interest in disclosure against agency's (individual's) interest in maintaining confidentiality

PUBLIC RECORDS AND RELEASE LAWS– “WHO GETS THE FOOTAGE”

A local TV station files a public records requires for footage of a well-known community member treated on scene after a crash. State law has ambiguous medical exemptions.



QUESTIONS

1. What are the privacy implications for the patient?
2. What are the job-protection implications for the medic?
3. What safeguards must exist in state law or agency policy?
4. What should the union demand in writing about release rules, redaction, and timelines?

THE RIGHT TO NEGOTIATE OVER WEARING BODY CAMERAS

PUBLIC SECTOR

- In most states where IAFF members enjoy public sector bargaining rights, public sector employers with unionized work forces are required by law to collectively bargain with union representatives over “mandatory subjects of bargaining.”
- Mandatory subjects = wages, hours, and terms and conditions of the bargaining unit’s employment.
- Body-worn cameras are likely to be deemed a mandatory subject of bargaining, meaning that a department or municipality must bargain with the union over the decision to wear body cameras, as well as the effects such new policies, procedures, protections and discipline, prior to implementation.

PUBLIC SECTOR

- Departments or municipalities may have the right to unilaterally require employees to wear body cameras, depending on the phrasing of the management rights clause or relevant statues in their jurisdiction
- Unions can argue that body cameras were not anticipated when the management rights clause was established, making it inapplicable
- Additionally, a strong zipper clause in the collective bargaining agreement may prevent mid-term modifications without bargaining
- Unions demanding bargaining over body camera implementation have faced mixed outcomes. Some jurisdictions consider it a management prerogative and not subject to bargaining, while others require impact bargaining to address issues like disciplinary measures, privacy concerns, and safety implications

PUBLIC SECTOR

Denver Police Protective Assoc. v. City and County of Denver, Colo., #15CV33862, (Dec. 19, 2016)

- Court interpreted "personal safety or health equipment" in the Denver City Charter to encompass body cameras, as a matter of law
- Found the Denver Police Department's Body-Worn Camera Policy was a mandatory subject of bargaining

Floyd v. City of New York (S.D.N.Y. 2014)

- Union argued matter of officer safety, privacy, and discipline
- Court found management right

PUBLIC SECTOR

Jacksonville Consolidated Lodge 5-30, FOP v. City of Jacksonville, 44 FPER ¶129 (Oct. 18, 2017)

- The Florida Public Employees Relations Commission (PERC) determined that, under Florida law, the decision to implement body cameras sets a standard of public service and is thus a management right.
- PERC also acknowledged that the impact of that decision on terms and conditions of employment (e.g., monitoring police officers) is negotiable upon proper request.

In the Matter of Arbitration between Oklahoma City, OK and The Fraternal Order of Police, Lodge 123 (June 14, 2016)

- Arbitrator found unilateral implementation of body camera program violated collective bargaining agreement where agreement was silent on the issue

PUBLIC SECTOR

Management Prerogative

- Pennsylvania Labor Relations Board, Fraternal Order of Police, Delaware County Lodge 27 v. Yeadon Borough, Decision No. PF-C-18-100-E, 2019 BL 346958
- Michigan Employment Relations Commission, Berrien County and Berrien County Sheriff -and- Police Officers Labor Council, Decision No. C17 L-122, 2018 BL 529662.

Negotiate Over the Impact

- Illinois Labor Relations Board, Decision, Fraternal Order of Police, Lodge #7 and City of Chicago (Department of Police), Case Nos. L-CA-17-037, L-CA-20-024

PRIVATE SECTOR

- The National Labor Relations Board (NLRB) has not issued any specific decisions regarding private sector employees wearing body cameras, but the issue could arise for private sector EMS operators in the IAFF
- The NLRB may consider the issue of body-worn cameras as analogous to workplace surveillance cameras or other uniform-related matters
- Employers must provide notice to unions and engage in bargaining over the installation of surveillance equipment, including body cameras, to avoid unfair labor practices

PRIVATE SECTOR

- Salem Hospital Corporation a/k/a The Memorial Hospital of Salem County, 360 NLRB 768 (2014)
  - Employers have a duty to negotiate in good faith with union representatives regarding mandatory subjects of bargaining, which includes uniform requirements and workplace attire
- Carey Salt Co., 360 NLRB No. 38, slip op. at 12 (2014); Peerless Food Products, 236 NLRB 161, 161 (1978)
  - Unilateral changes to employees' terms and conditions of employment related to body-worn cameras could be deemed unlawful if they are material, substantial, and significant departures from existing conditions
- The presence and content of management rights clauses and zipper clauses in collective bargaining agreements will impact whether an employer is obligated to negotiate over the decision and effects of implementing a body camera policy

BARGAINING RIGHTS – MANDATORY OR MANAGEMENT?

Your city announces, via email on Friday at 4:55 PM, that all EMS personnel will begin wearing body cameras next month

No bargaining. No discussion

QUESTIONS

1. Is that a mandatory subject of bargaining? Why or why not?
2. What parts must you demand bargaining on (policy, discipline, tech issues, training)?
3. Does your current contract have a management rights clause or a zipper clause – and how would it impact your leverage?
4. What is your *first* communication to management?
5. What is your *first* communication to your members?

WEARABLE TECHNOLOGIES AND DATA CONCERNS

TYPES OF WEARABLE TECHNOLOGIES

- Fitness trackers
- Smartwatches
- Rings
- Sensors embedded in protective gear for fire fighters.

BIOMETRIC AND PERSONAL DATA COLLECTED

- These devices gather biometric data like heart rate, respiration, hazardous exposure, and location to monitor wellness and safety.
- Continuous data collection raises concerns about data storage, usage, consent, and potential misuse in employment settings.
- Legal frameworks and policies are essential to protect firefighters' data rights and ensure transparency and fair use of information.

LEGAL FRAMEWORKS GOVERNING WEARABLE TECHNOLOGY

FEDERAL EMPLOYMENT LAWS

Americans with Disabilities Act (ADA)

- Prohibits disability inquiries or mandated exams via wearables unless job-related and necessary.
- Requires employers to ensure that data collected is not used to infer disability status, unless the information is obtained through lawful medical exams or voluntary wellness
- Requires that any health-related data collected be stored separately from personnel files and treated as confidential medical information
- If wearable technology identifies potential health concerns, employers cannot use this to take adverse action unless condition poses a **direct threat** and all ADA standards are met
- Requiring wearables that monitor physiological indicators (e.g. exertion, stress) may constitute a medical examination under ADA if used to assess an employee's physical or mental impairment
- Employers must provide reasonable accommodations if employee cannot use devise because of disability
- If data is used in performance evaluation or discipline, unions may argue that such use constitutes a disability-related inquiry, triggering ADA protections and potential bargaining obligations

FEDERAL EMPLOYMENT LAWS

Genetic Information Nondiscrimination Act (GINA)

- GINA restricts collection and use of genetic data through workplace wellness programs and wearables
- Employers must ensure wearable devices do not indirectly collect genetic information, such as family medical history or inherited traits
- Any wellness program offering incentives must avoid creating pressure that could be viewed as coercing employees to disclose genetic information
- Unions can demand contract language requiring employers to certify that wearable data platforms are configured to block genetic-related data collection
- GINA prohibits employers from using any genetic-related insights (even algorithmic predictions) to make decisions about fitness for duty

FEDERAL EMPLOYMENT LAWS

EEOC Wellness Program Guidelines

- Participation in wellness programs must be voluntary with clear data use and anti-retaliation policies
- Wellness programs must clearly disclose what data is collected, how it will be used, and who will have access to it
- Employers must ensure that no adverse action (discipline, reassignment, denial of promotion) is taken against employees who choose not to participate
- Data must be stored as confidential medical information
- Employer must provide reasonable accommodations
- Employees must receive annual notice of privacy protections and right to opt out without penalty

FEDERAL EMPLOYMENT LAWS

Data Privacy and Non-Discrimination

- Laws ensure wearable data is used without discrimination based on race, sex, disability, or genetics
- Cannot be used to make assumptions about protected characteristics
- Data collected must be limited to what is strictly necessary for legitimate operational needs, reducing risks of discriminatory misuse
- Employees should receive clear notice and the opportunity to correct inaccurate data
- Employers should implement anti-bias audits

STATE LEGISLATION: PUBLIC RECORDS LAWS

- Wearable technology data often available to public
  - Open Records
  - Sunshine
  - FOIA
- While such laws may exempt records relating to medical treatment, they are often ambiguous and largely untested
- Weighing public's interest in disclosure against agency's (individual's) interest in maintaining confidentiality

STATE PUBLIC RECORDS VS PRIVACY LAWS

- Broad/generalized public records laws could theoretically apply to wearable technology data
  - Idaho Code Ann. § 18-6701(2)
  - Missouri Rev. Stat. § 542.400(8)
  - Colorado Rev. Stat §24-72-202(7)
- Michigan Freedom of Information Act:
  - exempts from disclosure “information of a personal nature if public disclosure…would constitute a clearly unwarranted invasion of an individual’s privacy.”

STATE PUBLIC RECORDS VS PRIVACY LAWS

- New Mexico's Public Records Act provides that "[e]very person has a right to inspect public records of this state except…records pertaining to physical or mental examinations and medical treatment of persons confined to an institution."
- West Virginia's public records law exempts from disclosure "[i]nformation of a personal nature such as that kept in a…medical…file."

IS THIS DATA PROTECTED BIOMETRIC DATA... OR NOT?

- Heart rate
- Steps per day
- GPS location tracking
- Fingerprints
- Family medical history
- Exposure levels (toxins/smoke)
- Iris or facial scan

ANSWERS

Heart rate – Personal health data (NOT biometric)	•Typically, not considered “biometric identifiers” •Still protected under ADA if used for disability-related inferences and under wellness program rules (data must be voluntary and confidential)
Steps per day – Personal data (NOT biometric)	• Considered general wellness or fitness data • May still be protected under EEOC wellness guidance
GPS location tracking – Personal data (NOT biometric)	• Triggers duty to bargain when used for discipline or monitoring • Considered workplace surveillance governed by labor law
Fingerprints – Biometric identifier (protected)	• Explicitly defined as biometric data • Use often requires advanced notice, informed consent, and retention/destruction policy
Family medical history	• Covered under GINA • One of the most strictly regulated categories
Exposure levels (toxins/smoke)- Personal health data (NOT biometric)	• Still sensitive and may be protected by CBA language
Iris or facial scan- Biometric identifier (protected)	• Requires advanced notice, informed consent, and retention/destruction policy • Using for timekeeping can violate state laws if done without consent

MONITORING, SURVEILLANCE, AND DUTY TO BARGAIN

MONITORING, SURVEILLANCE, AND DUTY TO BARGAIN

- Wearable devices monitor worker productivity, safety, and location across industries like healthcare, mining, and construction.
- These technologies raise significant privacy concerns when used without proper negotiation or safeguards in place.
- Employers must negotiate with unions before implementing monitoring tech affecting discipline or performance evaluation.
- Collective bargaining defines data collection limits and protects workers' rights amid increasing workplace surveillance.

SCENARIO A

A fire department installs GPS-enabled gear to track crew movement for *safety* – but later uses the data to issue discipline

- Must the employer bargain?
- Is there a privacy or discrimination issue?
- What potential CBA language could protect the members?

SCENARIO B

A department requires smartwatches for wellness monitoring; participation is labeled “optional,” but employees who decline lose incentive pay.

- Must the employer bargain?
- Is there a privacy or discrimination issue?
- What potential CBA language could protect the members?

SCENARIO C

A research institution gathers biometric exposure data through turnout gear sensors without disclosing retention policies.

- Must the employer bargain?
- Is there a privacy or discrimination issue?
- What potential CBA language could protect the members?

MODEL CONTRACT AND POLICY LANGUAGE

MODEL LANGUAGE

Duty to Bargain: The employer shall have an affirmative obligation to notify and bargain with the union prior to the implementation, expansion, or modification of any technology, policy, or practice that involves the collection, monitoring, storage, or analysis of personal or biometric data from bargaining unit members. This includes, but is not limited to, wearable devices, GPS devices, or facial recognition tools. The employer shall not implement such technologies without first providing the union with reasonable advance notice of at least __ days, full disclosure of the technology and its purpose, and an opportunity to bargain over its impact and use.

MODEL LANGUAGE

Data Governance and Destruction Clause: All personal and biometric data collected by the employer shall be securely stored. The employer shall not sell, trade, or disclose such data to third parties without employee consent and must maintain a data retention schedule and delete data within __ days of its collection unless otherwise required by law. Employees shall be notified immediately of any data breach or unauthorized access.

MODEL LANGUAGE

Prohibit Surveillance: The employer will not use employee electronic devices, such as devices associated with fitness trackers or **wearable biometric sensors,** to monitor or surveil employees. Any personal or biometric information collected through an employer-issued or third-party device, including data shared with research institutions, shall not be used as the basis for, nor admitted as evidence in, any disciplinary action.

MODEL LANGUAGE

Right-to-Know Clause: The employer must fully disclose any technologies used by the employer or third-party vendors that collect, store, or analyze personal or biometric data. This includes prior written notices to identify the type of data collected, the purpose of collection, the entity responsible for data management, the duration of data retention, and any third parties with whom the data may be shared. The employer shall also provide employees with access to their own data upon request, without excessive delay, and allow employees to opt out of non-essential data collection without adverse employment consequences. The employer must notify all employees and union representatives __ days before the introduction or expansion of any type of employee monitoring regarding personal and biometric data

MODEL LANGUAGE

Technology Committee: A joint Labor-Management Technology Committee ("The Committee") will be established to review and discuss the implementation, use, and impact of technologies that collect, monitor, or analyze personal or biometric data. The committee should include equal representation from the union and management and serve as a forum for transparency, education, and input on data-related workplace practices. The committee will meet regularly or as needed to recommend safeguards, assess privacy concerns, and ensure that any technology introduced respects members' rights.

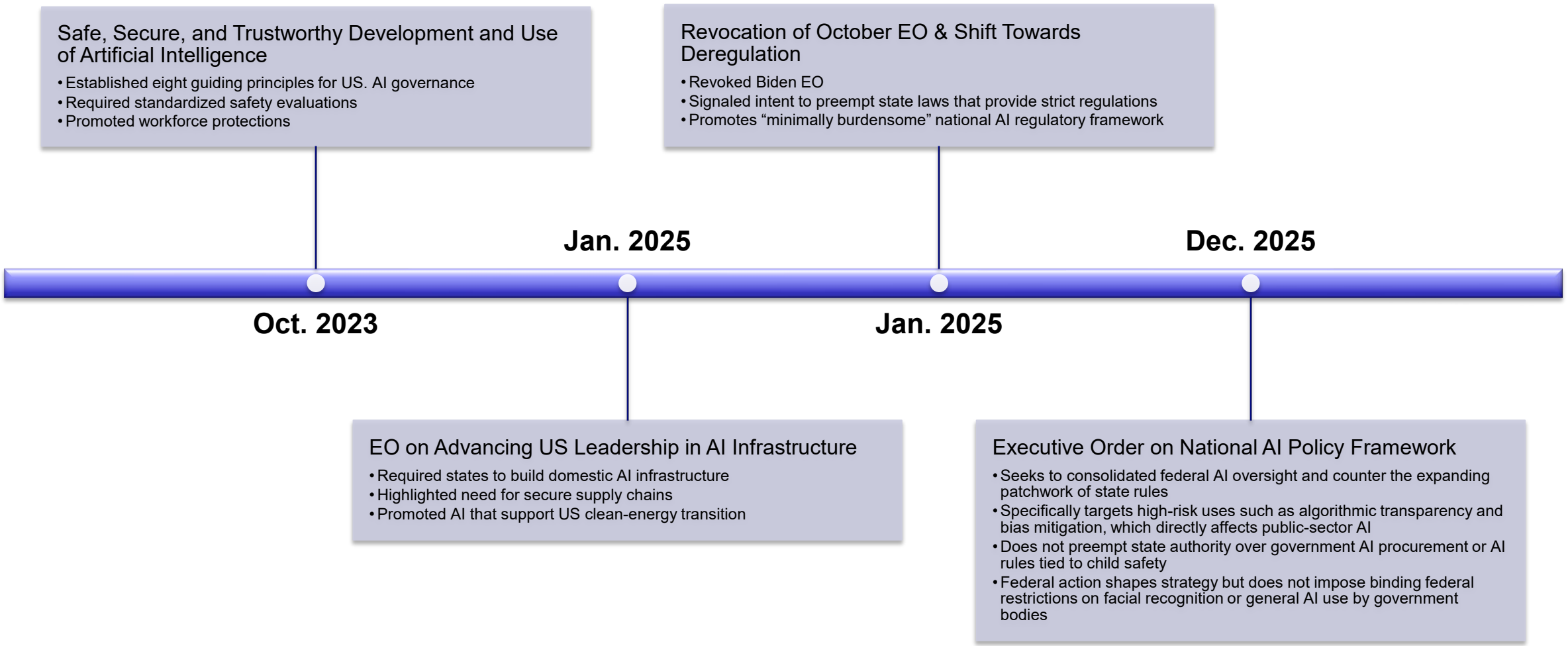
LAWS GOVERNING AI AND FACIAL RECOGNITION IN THE PUBLIC SECTOR

LEGAL LANDSCAPE

US has no federal law specifically restricting facial recognition in the public sector

Oversight is fragmented across states and municipalities

FEDERAL LANDSCAPE – EXECUTIVE ORDERS



STATE-LEVEL RESTRICTIONS

- New York (2025)
  - State agencies must publish detailed inventories of all automated decision-making tools used by the government
  - This includes systems for hiring, benefit eligibility, public safety, and other administrative decisions
  - Contains worker protections that specifically state AI systems by state government cannot diminish rights under collective bargaining agreements and cannot be used to displace civil service roles or cause job loss
- Maryland (2024)
  - Enacted policies regulating how AI can be used by state agencies, providing a governing framework for automated decision systems
  - Not a ban, but imposes operational constraints and oversight
- Colorado (2024-2025)
  - First broad statewide AI law regulating developers and deployers of high-risk AI
  - Must adopt bias-prevention measures and exercise reasonable care
  - Would include any public sector biometric or identification system

SOCIAL MEDIA USE AND THE FIRST AMENDMENT

“

[the government] shall make no law … abridging the freedom of speech … or the right of the people peaceably to assemble, and to petition the government for a redress of grievances. ”

First Amendment

FIRST AMENDMENT RIGHTS

- Freedom of **speech**
- Freedom of **assembly**
- Freedom of **association**
- Freedom to **petition**

FIRST AMENDMENT RIGHTS

- Public employees **do not relinquish** their First Amendment rights by accepting government employment
- But their rights are **more limited** than those of normal citizens

PROTECTED SPEECH

If a public employee speaks in his or her capacity **as a citizen**, and the speech relates to **a matter of public concern**, then he or she cannot be disciplined in retaliation for the speech, unless the employer has an **adequate justification** for treating the employee different from any other citizen.

PROTECTED SPEECH – GARCETTI V. CEBALLOS, 547 U.S. 410 (2006)

- If the speech at issue is expressed as part of the employee's official **job duties**, it is made as an "employee" and not as a "citizen," therefore it is **unprotected.**
- This decision has been roundly criticized by legal scholars and the plaintiff's bar.
- Led to a new verb - being "Garcettized."

“CITIZEN” V. “EMPLOYEE SPEECH”

- Was speech within the scope of **“official duties”**?
  - Yes → Employee
  - No → Citizen
- Look at **job description** and **actual duties**
- “Citizen” speech may include information **related to, or learned through,** public employment

“CITIZEN” V. “EMPLOYEE SPEECH”

- Every situation requires a **case-by-case analysis**
- Speech made in one’s capacity as a **union member or official** is likely “citizen” speech

MATTERS OF PUBLIC CONCERN

- Relates to any matter of political, social, or other concern to the community
  - Staffing
  - Response times, government inefficiency and waste, inadequacy of funding for emergency services
  - Failure to follow health and safety rules (unsafe working conditions, environmental violations)
  - Equipment malfunctions
  - Discriminatory policies
  - The right to organize
- Determined by looking at the content, form, and context of the speech

MATTERS OF PUBLIC CONCERN

- Mere personnel grievances are typically NOT matters of public concern
- *E.g.*, complaints about internal personnel rules or policies, statements about disputes with employer regarding compensation/benefits
- However collective personnel grievances raised by unions may be matters of public concern, although courts differ on this issue. Ex: *Ellins v. City of Sierra Madre*, 710 F.3d 1049 (9th Cir. 2013) (collective personnel grievance raised by union official was matter of public concern); *Van Compernolle v. City of Zeeland*, 241 F. App'x 244, 250 (6th Cir. 2007) ("A group effort to gain more overtime is no less an internal personnel dispute than if it were the effort of one officer.")

EMPLOYER JUSTIFICATION

- **Speech on matters of public concern can still be unprotected**
- If employer’s right to efficient operations outweighs employee’s right to freedom of speech, court's will find that employer did not violate employee's First Amendment rights by disciplining employee for speech.

EMPLOYER JUSTIFICATION

- Employer usually needs actual evidence that the speech:
  - interfered with regular operation of the department;
  - impaired discipline by superiors (i.e., constituted insubordination, disloyalty, eroded morale among co-workers);
  - eroded public confidence in department; or
  - otherwise impaired efficiency of department

PROTECTED SPEECH

- A fire chief acted as a government agent when emailing firefighters about a job- related issue from his official account using his official title. *See Holbrook v. Dumas*, 658 F. App'x 280, 288–89 (6th Cir. 2016).

- But a fire captain acted as a private citizen when he called city council members from his home as a concerned taxpayer. *See Stinebaugh v. City of Wapakoneta*, 630 F. App'x 522, 527–28 (6th Cir. 2015); *see also Westmoreland v. Sutherland*, 662 F.3d 714, 719 (6th Cir. 2011).

- *DeCrane v. Eckart*, No. 1:16-cv-02647, 2021 WL 3909802, at *5 (Sept. 1, 2021) (alleged leak to media about fire chief's deficient training protected First Amendment speech)

- *Foley v. Town of Randolph*, 598 F.3d 1, 9 (1st Cir. 2010) (holding that the chief "was speaking in his official capacity and not as a citizen" when he made the statements, and the statements were therefore not protected by the First Amendment, at press conference after fatal fire that killed two children, ages 17 and 10)

WHAT IS "SOCIAL MEDIA?"

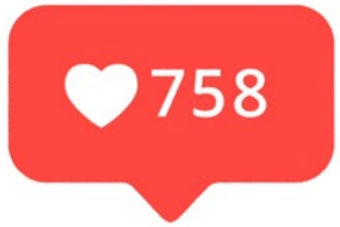
- Umbrella term for internet-based services that permit users to create, share, re-purpose and publish informational content. Social media websites require users to affirmatively join, and typically require users to create a uniquely identifiable profile. Ex: Facebook, Twitter (X), LinkedIn, blogs, Wikis, and Google+

  - **Blog**: short for "weblog;" type of website, usually maintained by a single individual/entity with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse chronological order, and usually with a particular topic or area of concentration.

  - **Wiki**: website that allows the easy creation and editing of any number of interlinked web pages via a web browser. Wikis are typically powered by wiki software and are often used to create collaborative websites, to power community websites, for personal note taking, in corporate intranets, and in knowledge management systems. Ex: Wikipedia

THE FIRST AMENDMENT AND SOCIAL MEDIA

- How does social media fit in to what we've just discussed?
- Posts on social media are "speech" for purposes of the First Amendment
- Even "liking" a post on social media can be considered speech



THE FIRST AMENDMENT AND SOCIAL MEDIA

- Because of the widespread dissemination of speech on social media, courts are more willing to find this speech to be “disruptive” to the workplace and thus not protected
- In other words, more likely that employer will be able to show adequate justification for an adverse employment action based on speech addressing a matter of public concern

THE FIRST AMENDMENT AND SOCIAL MEDIA

Examples from real cases:

- In *Moreau v. St. Landry Parish Fire Protection District No. 3*, No. 19-30767 (5th Circuit, April 7, 2020), a fire fighter who was upset that police forcibly removed a teacher from a school board meeting posted on Facebook “all of this going on with this poor teacher being treated so unfairly makes one thing perfectly clear … These ‘boards’ everywhere, ruled by good old boy politics, need to be dissolved ASAP … We have the same exact problem at our fire department … A board of clueless idiots making the decisions that affect many including the very employees who actually do the job.”
- The fire fighter was terminated for his comments and brought a First Amendment lawsuit against the employer.
- The Fifth Circuit concluded that the fire fighter’s comments were personal criticisms that did not arise to the level of being a matter of public concern. As such, his termination was upheld, notwithstanding the fact that the speech involved public criticism of elected officials.

THE FIRST AMENDMENT AND SOCIAL MEDIA

Examples from real cases:

- In *Marquardt v. Carlton; City of Cleveland*, 971 F.3d 546 (6th Circuit, 2020), an EMS captain was fired for commenting on social media on the shooting death of a 12-year-old African-American, Tamir Rice, by police. The captain posted: “Tamir Rice should have been shot and I am glad he is dead ... I am upset I did not get the chance to kill the criminal [expletive].”
- The fire fighters in each case sued, claiming that they were terminated for engaging in protected speech.
- The trial judges ruled in favor of the fire departments, concluding the First Amendment did not apply, because the postings did not involve a matter of public concern. Both fire fighters appealed.

THE FIRST AMENDMENT AND SOCIAL MEDIA

Examples from real cases:

- In *Marquardt*, the Sixth Circuit concluded that as offensive as the captain's post may have been, it nonetheless involved a matter of public concern, namely race relations.
- In sending the case back to the trial court for further proceedings, the Sixth Circuit cautioned that its ruling should not be considered supportive of the comments that the captain posted. In fact, the court reminded the parties that the *Pickering* test has three components, and under the balancing test, an employer "may regulate employee speech to a greater extent than it can that of private citizens, including to discipline employees for speech the employer reasonably predicts will be disruptive."

THE FIRST AMENDMENT AND SOCIAL MEDIA

Examples from real cases:

- *Fenico v. City of Philadelphia*, No. 20CV3336, 2024 BL 386043 (E.D. Pa. Oct. 28, 2024)
- A dozen police officers who were disciplined after their private Facebook posts came to light sued the City of Philadelphia for First Amendment retaliation
- Plaintiffs made a variety of Facebook posts on their personal accounts about hot-button topics such as race, religion, immigration, sexual orientation, gender, and crime

THE FIRST AMENDMENT AND SOCIAL MEDIA

- The Court denied all the officers' claims and held that the Department's interest in preventing disruption in the police force outweighed any interest that the public might have in a series of police officer Facebook posts
- In denying the retaliation claims of all the officers who were disciplined, the Court repeatedly held: "The City has demonstrated that the posts were likely to cause significant interference with the PPD's operations. Because the City's interest in preventing this disruption outweighs his and the public's interest in his posts, his posts are not protected."

STAYING OUT OF TROUBLE

STAYING OUT OF TROUBLE

Connect	Choose	Control
Connect everything you say to a matter of public concern	Choose the right forum • Statements to the public vs. Statements to supervisor	Control the context • Personal/political disputes vs. Operational/policy disputes

STAYING OUT OF TROUBLE

Have	Have friendly witnesses around, but still document your statements
Use	Use reasonable and constructive language
Make	Make sure the speech is not disruptive
Be	Be careful on social media—assume everyone can see your posts

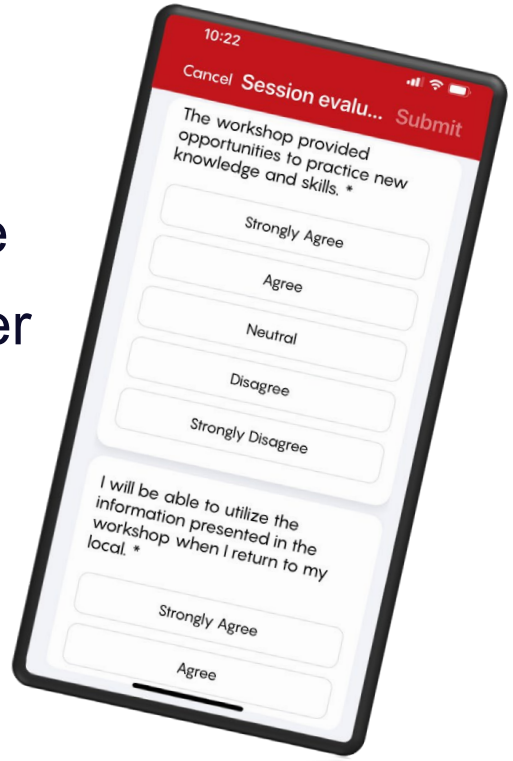
THANK YOU!
ANY QUESTIONS?

Mark Linscott
IAFF Legal Counsel |
mlinscott@iaff.org

Lauren McDermott
IAFF Legal Counsel |
lmcdermott@iaff.org

EVALUATION AND WIN AN IPAD!

- **Submit your workshop and overall evaluations to be automatically entered in two drawings for a new iPad!**
- **Complete your evaluations using the IAFF app:**
  1. Download the IAFF app and sign in with your iaff.org username
  2. Tap the 2026 Strive for Excellence Summit event image to enter the event's dashboard
  3. Tap "Sessions" and tap on the workshops you attended
  4. Tap "Evaluation" and complete the evaluation
  5. Tap "Submit"



For the event's overall evaluation, follow steps 1 and 2, then tap "Event Evaluation" located in the event's Dashboard.