RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: LAW-F03

RETHINKING EMPLOYEE SURVEILLANCE IN A NEW DIGITAL ERA

Natalie Pierce

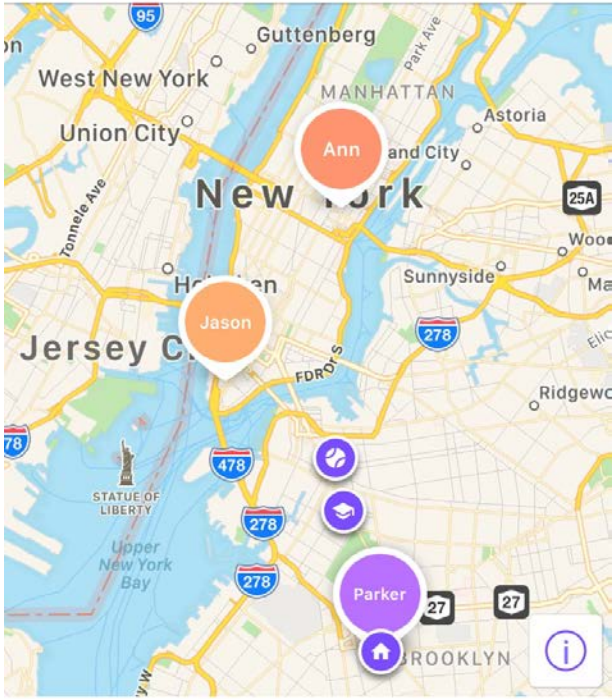
Shareholder | Co-Chair, Robotics, AI and Automation Industry Group
Littler, San Francisco
npierce@littler.com

Jason Straight

Sr. VP, Cyber Risk Solutions | Chief Privacy Officer
UnitedLex Corp.
New York, NY
jason.straight@unitedlex.com

Verizon LTE 6:55 PM 41%

Straight Family Check In



Ann · 45%
Near 664 3rd Ave

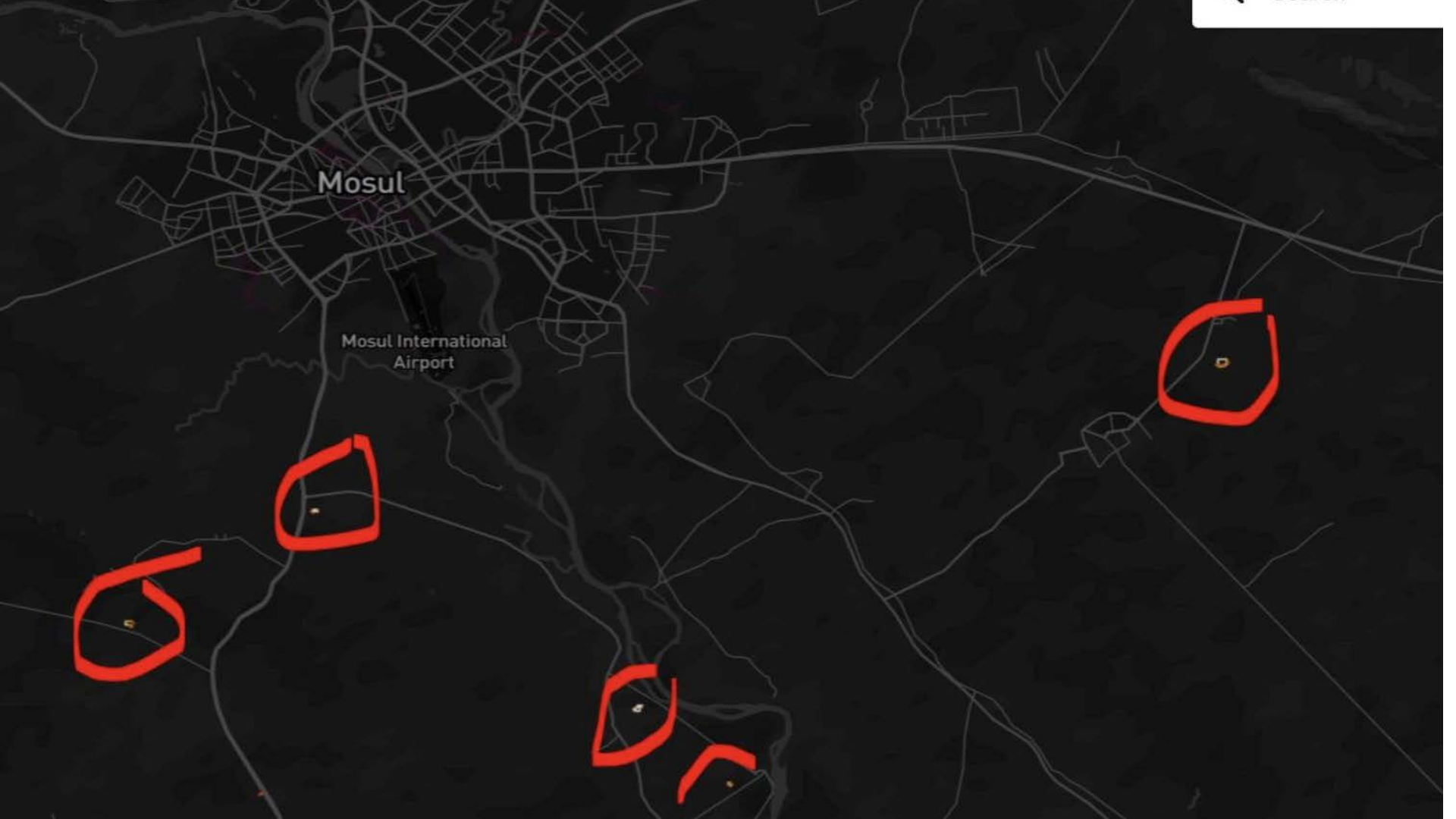
Parker · 100%
At Home

Jason · 41%


12:35


GPX
Terrain Map
Le Don
Paton
St. John
St. Mary
St. Ouen
Les Monts
Trinity
St. Martin
St. Peter
A12
A9
A8
La Route de la Pulente
St. Brelade
A13
St. Helier
Grouville
A4
A3
Longueville Rd


West Hove Golf Club
A27
Benfield Valley Golf Course
HANGLETON
PORTSLADE
Hangleton Rd
Nevill Ave
Weald Allotments
Hove Park
Hove Recreation Ground
Old Shoreham Rd
Hallyburton Rd
Portland Rd
Montgomery St
Sackville Rd
New Church Rd
Wellington Rd
Hove Museum and Art Gallery
Kingsway
A259
A270
A2023
Goldstone Crescent
Dyke Rd Ave
Withdean Park
CLIVEDEN CLOSE
Preston Drove
PRESTON
Preston Park
Surrenden Rd
Ditchling Rd
Dyke Rd
Cromwell Rd
Addison Rd
Davigdor Rd
Western Rd
North Laine
Churchill Square Shopping Centre
BRIGHTON
Brighton Pier
Hollingbury Golf Co
Brighto
KEMPTOW


Mosul
Mosul International Airport

WHAT IS PERMISSIBLE AND WHAT IS NOT?

Reasons for Employee Monitoring and Surveillance

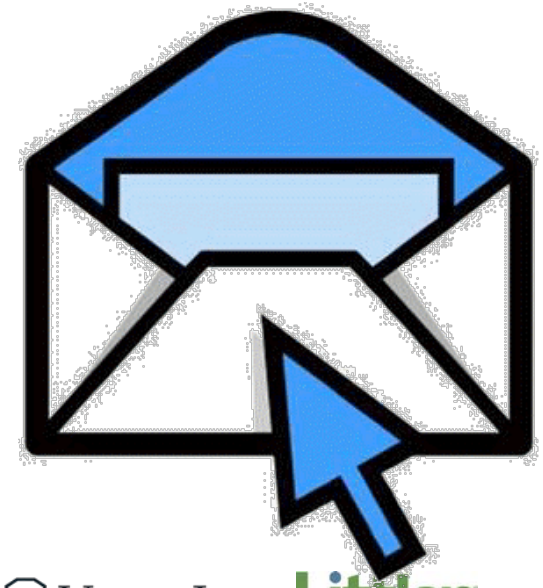
Employers have compelling reasons to monitor employees

Protect confidential information	Investigate employee misconduct	Manage employee performance	Health and Wellness Programs
Personal information Trade secrets Customer information	*EEOC v. Management Hospitality of Racine, Inc.*, 666 F.3d 422, 436 (7th Cir. 2012)	Efficiency and diligence Use of personal social media during work hours	Insurance discounts Reduce absenteeism Improve loyalty

Risks of Employee Monitoring and Surveillance

- Monitoring and surveillance can run afoul of a broad array of privacy laws, including:
  - State privacy laws
  - Federal Stored Communications Act
  - State social media protection laws
  - Lawful off-duty conduct laws
  - State and federal wiretap laws
- Not to mention that unconstrained monitoring may damage employee morale

Hypothetical # 1



When Jane is away from her desk, you happen to see a Gmail message open on Jane's company-issued computer that appears to be from Tom. The content of the message suggests that the two are in a romantic relationship in violation of company policy.

Can you click on other emails to further investigate?

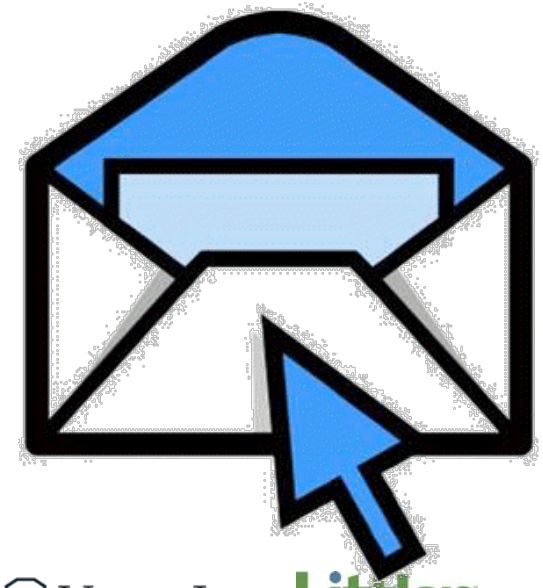
Should you confront Jane with the first email?

Monitoring of Employee Documents and Communications on Company Computer Systems

Invasion of privacy and related claims can turn on workplace policies. Key questions include:

- Are employees adequately informed that they have no expectation of privacy when using computer systems at the workplace?
- Does the policy make clear that electronic resources such as email, internet, and all messages transmitted through or stored on the company's system are the property of the employer and the employee's use of those resources is not private?
- Does the policy may clear that the employer may, in its discretion, review communications transmitted through or stored on the employer's system?

Hypothetical # 1



- Gmail not on employer's own computer system
- Gmails not "readily accessible to the general public"
- Emails already opened?
- Consent?
  - Mere notice inadequate
  - Best practice is signed consent

UnitedLex Littler

Hypothetical # 2

An employer wants to install GPS tracking on company-issued mobile devices provided to its sales team to track their whereabouts.

Is this permissible?

Statutory Restrictions

- 12 states prohibit unauthorized installation of an electronic tracking device on a vehicle
  - CA, CT, DE, HI, IL, LA, MI, MN, TN, TX, VA, WI
  - All these laws permit tracking with the owner's consent
- LA, NC, and WI are the only states that prohibit tracking of individuals without consent.
  - (LA allows tracking of a vehicle with the owner's consent, but otherwise prohibits tracking of an individuals without consent.)
- **NLRA:** Is tracking a mandatory subject of collective bargaining?

Hypothetical # 2

Generally, if your state has a GPS tracking law, you must first obtain consent from the members of the sales team.

- Employer wants to

Wearable Technology

Examples Of Wearables

- Health Trackers
- Fitness Trackers
- History Recorders
- Performance Enhancers
- Performance Managers

Employee Wellness Programs

- 4 out of 5 employers offering some sort of employee wellness program
  - 13 million activity trackers currently involved in corporate wellness plans
- Programs track any or all of the following:
  - Activity levels (e.g. “steps”)
  - Sleep patterns
  - Nutrition and diet
  - Heart rate
  - Weight and BMI

Hypothetical # 3

John enrolls in employee health and wellness program and accepts a "free" GPS-equipped fitbit to help track his fitness goals. John calls in sick on the day the NCAA basketball tournament is being played in town. John is a huge fan and his boss thinks he is lying about being sick to attend the game. John's employer wants to access his GPS tracker information to see where John is.

Is this permissible?

Hypothetical # 3

Probably an overreach by the employer as John did not consent to this sort of tracking?

Recommendations

1. Limit location tracking to working hours
2. Define the business purpose for the tracking
3. Control access to the location information
4. Limit disclosure of the location information
5. Provide robust notice to employees
6. Don’t rely exclusively on location information to impose discipline

SOCIAL MEDIA AND OFF DUTY CONDUCT

Taylor [redacted]

I HATE MY BOSS

Like · Comment · 5 hours ago near Lucia ·

[redacted] like this.

Lizzy [redacted] Dido

5 hours ago via mobile · Like · 1

Taylor

I HATE MY BOSS

Like · Comment · 5 hours ago near Lucia ·

like this.

Lizzy Dido

5 hours ago via mobile · Like · 1

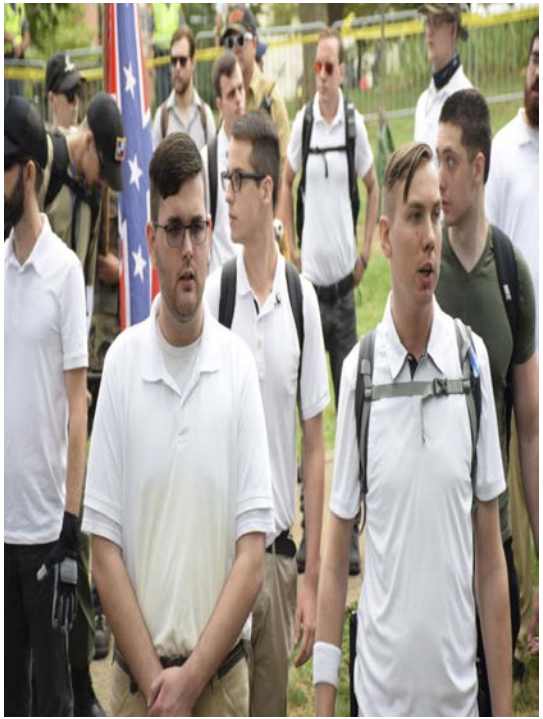
Jeremy You do realize we're friends on fbook right?

What I did was legal and on my own time, you just didn't like it.

More than 30 states protect employees against adverse action based on some form of lawful off-duty conduct:

- Lawful Off-Duty Conduct – *e.g.,* CA, CO, NY
- Political Activity – e.g., CA, CO, LA, NY, UT
- Consumption Of Lawful Products – *e.g.,* IL, MN, MT, NV, NY, NC, TN, WI
- Smoking/Tobacco Use – about 1/3 of states
- Social Media Privacy Laws – e.g., CA, CO, IL, MI, WI
- Firearms – *e.g.,* IN, ND

Political and Social Commentary Have Become a Daily Issue in the Workplace



Pleading the First!

- Employees frequently say this about their off-duty speech but, unless the employee works for the government, it is ***NOT TRUE***.
- The U.S. Constitution prohibits Congress and the states (not private employers) from imposing certain limits on employee speech.
- While private sector employees may not have the First Amendment protections they think they do, employees can often seek protection under state laws

Hypothetical #4

The local news circulates a photo of a woman flipping off President Trump's motorcade. After the photo goes viral on social media and late night talk shows, a member of management notifies HR that one of his subordinates, Susan, has disclosed that she is the woman in the photo.

The supervisor is an avid Trump supporter and tells you that he wants to discharge Susan for violating the company's code of conduct, which prohibits lewd and obscene behavior.

Can the company legally discharge Susan?

Hypothetical #4

The Law

- If you are a private employer, there is no federal law protecting this conduct.
- If your state does not have a statue protecting political activity or lawful off duty conduct, then you are not prohibited from taking adverse employment action in response to her conduct
- No privacy concerns – conduct occurred in public place.

Employer Policy

- It violates the code of conduct.

But is it a good idea?

Artificial Intelligence in the Workplace

The Economist

AI-spy

The workplace of the future

As artificial intelligence pushes beyond the tech industry, work could become fairer—or more oppressive

MIT Technology Review

Inside Amazon's Warehouse, Human-Robot Symbiosis

Amazon's newest warehouse is testing the limits of automation and human-machine collaboration.

THE WALL STREET JOURNAL.

How AI Is Transforming the Workplace

Artificial intelligence is changing the way managers do their job—from who gets hired to how they're evaluated to who gets promoted

UnitedLex Littler

Hypothetical #5

The CISO for a large global technology company wants to implement user behavior analytics monitoring that relies on continuous activity profiling performed using artificial intelligence.

Can the CISO implement user behavior analytics across offices in the US, the EU and China?

Hypothetical #5

- Privacy, data protection and export control laws for each country must be reviewed before implementation of automated user behavior monitoring. The EU's new GDPR law in particular places significant restrictions on accessing and processing "personal data" for EU residents.

Apply What You Have Learned Today

- Next week you should:
  - Review your employee consent and acceptable use policies
  - Talk to HR about the company's stance on employee surveillance
  - Understand your potential risk under GDPR
- In the first three months following this presentation you should:
  - Rethink your approach to employee surveillance and monitoring
  - Define a narrow approach based on legitimate business needs balanced against employee privacy considerations
- Within six months you should:
  - Communicate and train managers AND employees on surveillance/monitoring – transparency = deterrence

Questions

APPENDIX

Stored Communications Act (SCA)

- **Federal law that generally prohibits intentional unauthorized access of communications in storage with a third party.** 18 U.S.C. §§ 2701-2712.
  - **Courts have interpreted this 1980s-era law to apply to new forms of service providers:** Gmail, Skype, Facebook, etc.
  - **Civil liability**: injunctive relief, statutory damages of $1,000, actual damages, defendant's profits, punitive damages, attorney's fees, and costs.
  - **Criminal liability**: fines and jail time.

- **No liability for access:**
  - With consent;
  - To communications "readily accessible to the general public"; or
  - To employer's own systems.

Invasion of Privacy?

- "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."
  - U.S. v. Jones, 132 S.Ct. 945 (2012) (Sotomayor, concurring)
- NY's Inspector General tracked surreptitiously tracked the vehicle of a NYDOL executive 24/7 for 30 days and obtained evidence that he was falsifying time records.
- **NY Court of Appeals:** Tracking was an unreasonable search, and location data could not be used to support discipline.
  - Cunningham v. NY Dept. of Labor, 974 N.Y.S.2d 896 (2013)

Biometric Identifiers

- **Illinois Biometric Information Privacy Act (BIPA)**
  Prohibits collecting "biometric information" without:
  - "Written release";
  - Publicly available, written biometric privacy policy; and
  - Reasonable safeguards.
  - Also imposes limits on disclosure.
- **Civil remedies:**
  - Greater of actual damages or $1,000 ($5,000 for intentional/reckless violation),
  - Injunctive relief, attorneys' fees and costs
- Similar law in Texas
- Bills pending in Alaska, Connecticut, Montana, New Hampshire, and Washington

Implications of Political Activity Under the NLRA

- Section 7 of the NLRA generally protects employees who engage in concerted activity for mutual aid or protection.
- May include political advocacy such as contacting legislators, testifying, joining demonstrations etc.
- Pay attention when off-duty speech or conduct arguably relates to employment terms – e.g., minimum wage, equal pay, paid leave, healthcare, immigration

Wisconsin Social Media Protection Act

- Prohibits employers from “requesting or requiring” that employees and applicants provide “access information” for their “personal internet account” or “to otherwise grant access to or allow observation of that account.”
- A "personal Internet account" is any “internet-based account that is created and used by [an employee or applicant] exclusively for purposes of personal communications.”
- “Access information” means the “password or any other security information” that protects access to a personal Internet account.
- Damages available: fine up to $1,000, back pay, reinstatement, attorney’s fees and costs.
- Wis. Stat. § 995.55