



aalrr Atkinson, Andelson
Loya, Ruud & Romo
A Professional Law Corporation

2018 EMPLOYMENT LAW CONFERENCE
MISSION=POSSIBLE

**THE ADVERSE IMPACT OF
TECHNOLOGY ON THE WORKPLACE**
SESSION 4

Presented by:
Jonathan Judge, Partner
Allison Scott, Associate

www.aalrr.com Cerritos • Fresno • Irvine • Marin • Pasadena • Pleasanton • Riverside • Sacramento • San Diego



AGENDA

- Introduction
- Privacy
- GPS, Biometric & Smart Devices
- Harassment & Technology
- Data Security
- Conclusion

aalrr 1



TECHNOLOGY

- Employers face many challenges
- Using technology in the workplace
 - Email communication
 - GPS tracking
 - Biotechnology
 - Timekeeping Apps
- Adverse effects on the workplace
 - Privacy
 - Harassment
 - Confidential information
 - Data breaches

aalrr 3



FEDERAL PRIVACY CONCERNS

- Privacy in Electronic Communications
 - Federal Electronic Communications Privacy Act (ECPA)
 - Stored Communications Act (SCA)
 - Prohibitions
 - Greater rights with internally operated systems and networks
- Electronic communications stored on a third party system
 - May preclude employer access
 - *Quon v. Arch Wireless Operating Co.* (2008)
- How is information stored?
 - *Lazette v. Kulmatycki* (2013)

CALIFORNIA PRIVACY CONCERNS



- California Privacy Act
- Intentional wiretapping
- Eavesdropping | Recording
- Interception of cellular phone conversations
- Unauthorized opening of sealed envelopes containing telephone or telegraph messages

EXPECTATION OF PRIVACY



- Policies & procedures setting expectation of privacy in the workplace
 - *TBG Insurance Services Corp. v. Super. Ct. of Los Angeles County* (2002)
 - *Holmes v. Petrovich Development Co.* (2011)

COMMUNICATION POLICY POINTERS

1. Electronic equipment is the property of the employer and communications thereon are to be solely for employer's business during working time.
2. Employer-issued laptops, electronic communication devices, and cell phones are included within the coverage of the policy. Because these items are regularly taken home by employees, specific notice is necessary to defeat the increased likelihood of formed expectations of privacy.

COMMUNICATION POLICY POINTERS

3. The employer reserves the right to inspect and confiscate any hardware devices issued to or used by employees.
4. The employer will keep copies of Internet or e-mail passwords, and the existence of such passwords is not an assurance of the privacy or confidentiality of the communications.

SEARCHING ELECTRONIC COMMUNICATIONS

- Maintain policies advising employees of the possibility of searching company technology systems
- Legitimate business reason for search
 - *O'Connor v. Ortega* (1986) 480 U.S. 709
 - Used reasonableness test to balance employer's legitimate business needs against public employee's expectation of privacy
 - *City of Ontario, Cal. v. Quon* (2010) 560 U.S. 746
 - Reasonable expectation of privacy in text messages sent on city-provided pager
 - Review of text messages constituted a search
 - Search was reasonable when narrowly tailored to the factual circumstances

SEARCHING SOCIAL MEDIA

- Employers cannot request or require employees or applicants to:
 - Disclose username or passwords of social media accounts;
 - Access personal social media accounts in the presence of an employer; or
 - Divulge any personal social media.
- Exception
 - Investigating employee misconduct or unlawful activity
 - May request an employee to divulge personal social media reasonably believed to be relevant to the investigation
 - Can only be used for the purposes of the investigation or related proceeding





GPS MONITORING

- Use caution when using smart devices with GPS to track employees
 - Restrictions under Penal Code
 - Exceptions
- Tracking during non-working hours may violate an employee's right to privacy
 - *Myrna Arias v. Intermex Wire Transfer, LLC* (2015)
- Obtain acknowledgements

BIOMETRIC TECHNOLOGY

- Fingerprint use in timekeeping systems
- Retina/iris scans
- Some states have biometric privacy laws regulating consent, notice, & disclosure procedures
- CA does not have regulatory statutes; however, in CA it is a misdemeanor to share fingerprints or photographs with third parties if it could be used to employee's detriment
 - Ensure that fingerprints or photographs are NOT shared with the vendors of the systems

SMART DEVICES

- Considerations before providing a smart device
 - Maintaining confidential data;
 - Complying with recordkeeping requirements;
 - Searching an employee's personal device for violation of employer's policies; and
 - Reimbursing employees for use of personal smart devices versus providing company smart devices.

REIMBURSING FOR SMART DEVICES



Cochran v. Schwan's Home Service, Inc.
(2014) 228 Cal.App.4th 1137

- Employers are obligated to reimburse employees a reasonable percentage of an employee's personal cellular phone used for company business regardless of whether:
 - 1) Employee incurs additional charges for work-related activity;
 - 2) A third party pays for the phone; or
 - 3) Employee has made any changes to plan.

HOURS WORKED ON SMART DEVICES

- *Non-exempt employees need to be compensated for time spent accessing company e-mail and other technology systems during non-working time*
- *Employers should maintain policies prohibiting non-exempt employees from performing off-the-clock work and provide a mechanism to report time worked when accessing the company's information systems.*

APPS

There are several “apps” that may be used for timekeeping, to track employee locations or mileage.

Employers must be mindful of the following:

- What type of information does the app collect from the employees’ smart device?
- Can the information collected be limited?
- Can the timekeeping app be customized for California use?
- Can the app notify the company of meal period violations?



HARASSMENT & TECHNOLOGY



- Technology often allows harassment to go unnoticed in the workplace
- What can employers do when an employee is harassing another via text messaging, or social media outside the workplace

TEXTUAL HARASSMENT

- Text messages maybe interpreted differently as they do not convey tone or body language
- Difficult to monitor
- The high cost of textual harassment
 - *Whitney Wolfe v. Tinder et al.* (2014)
 - *EEOC vs. Frys' Electronics* (2010)
 - *Jane Doe v. Starbucks, Inc.* (2009)
- Ensure that employees understand that company polices against harassment extend to all electronic communications between employees

HARASSMENT VIA BLOG POSTS AND SOCIAL MEDIA

- Employee posts on social media or blogs that implicate the workplace or involve a protected characteristic of another employee may result in a claim for harassment.
- *Espinoza v. County of Orange* (2012) 2012 WL 420149
 - In 2012, a jury awarded over \$800,000 to an employee who was harassed by co-workers when the co-workers anonymously posted on a blog ridiculing the employee's birth defect.
- Employees may also post complaints about workplace harassment on blogs or social media
 - Once employer receives notice, employer should investigate

AN APP TO REPORT HARASSMENT

- #MeToo movement has spurred companies to develop apps and other web-based platforms for reporting harassment
 - Anonymous reporting
 - Encourage reporting without fear of retaliation
 - Provides employers with data regarding complaints
- Apps and web-based programs are relatively new and may have some "kinks" to work out
 - Employers should carefully vet any program that they use for employees to report complaints



TRAINING

- Train & educate employees about data security:
 - Acceptable use of company electronic systems
 - Not opening e-mails or attachments from unknown sources
 - How to identify potential “phishing” e-mails
 - Explain the potential dangers with peer-to-peer file sharing and the necessity backing up of important information
 - Delineate the appropriate use of cellular telephones and other smart devices that contain company information
 - Password best practices

BEST PRACTICES



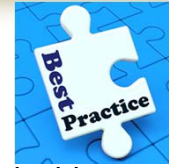
1. Know what data is stored and where it is stored on the company's electronic systems
2. Confine access to confidential information to authorized users
3. Consider separating confidential information (e.g. placing certain information on different servers/systems from other confidential information)
4. Limit ability for employees to download information to personal computer (e.g. mobile or remote desktop servers)

BEST PRACTICES



5. Monitor employees' use of the company's electronic systems for large downloads of data or use of USB devices
6. Limit and control vendor access to company's electronic systems and obtain assurances of responsibility of vendors to maintain confidentiality of such information
7. Maintain a central list of data providers, software vendors with key contact information
8. Consider insurance options for data security

BEST PRACTICES



9. Create a written response plan for data security incidents
10. Revoke terminated employees' access to the company's electronic systems
 - Return company property, such as laptops, I.D. badges, and access cards
 - Forward terminated employee's e-mails and voicemails to an individual who will be responsible for responding
 - Coordinate with IT to ensure remote access is appropriately and timely restricted.

RESPONSE PLAN

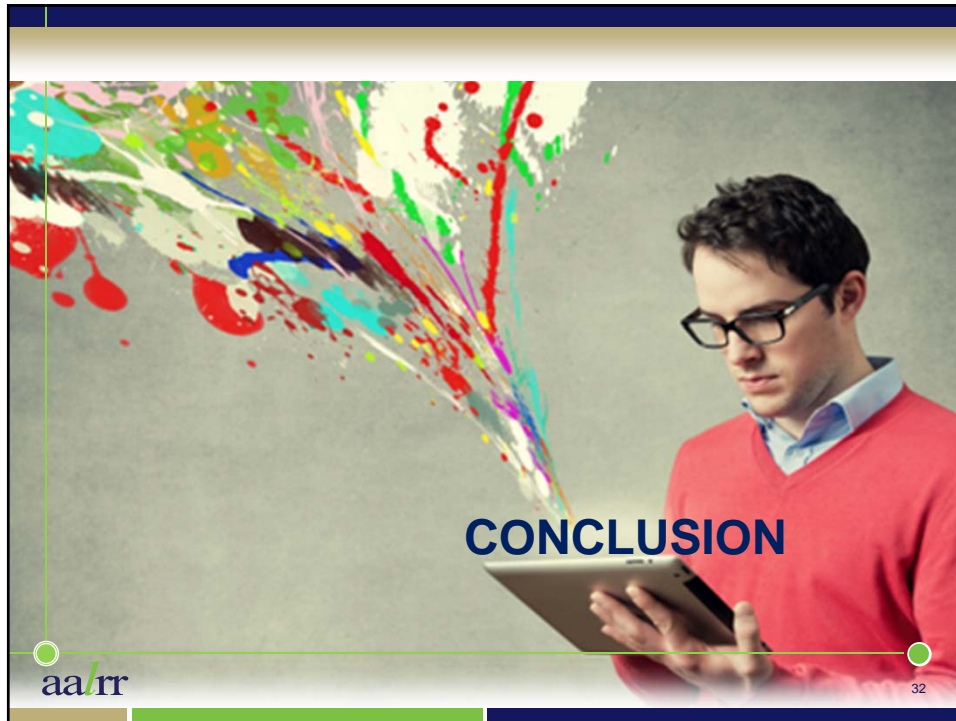
1. Who is responsible for different parts of the employer's data security response;
2. How to contact critical personnel at any time, day or night;
3. How to proceed if critical personnel are unreachable, including who will serve as back-up;
4. What data, networks, or services should be prioritized for the greatest protection;

RESPONSE PLAN

5. How to preserve data related to the intrusion in a forensically sound manner;
6. What criteria will be used to ascertain whether data owners, customers, or business partners should be notified if their data or data affecting their networks is stolen; and
7. What procedures exist for notifying law enforcement and/or computer incident-reporting organization(s).

SERVICES BEFORE INTRUSION

- In addition to a response plan, identify such additional services as:
 - Off-site data back-up;
 - Intrusion detection capabilities;
 - Data loss prevention technologies; and
 - Devices for traffic filtering or scrubbing.

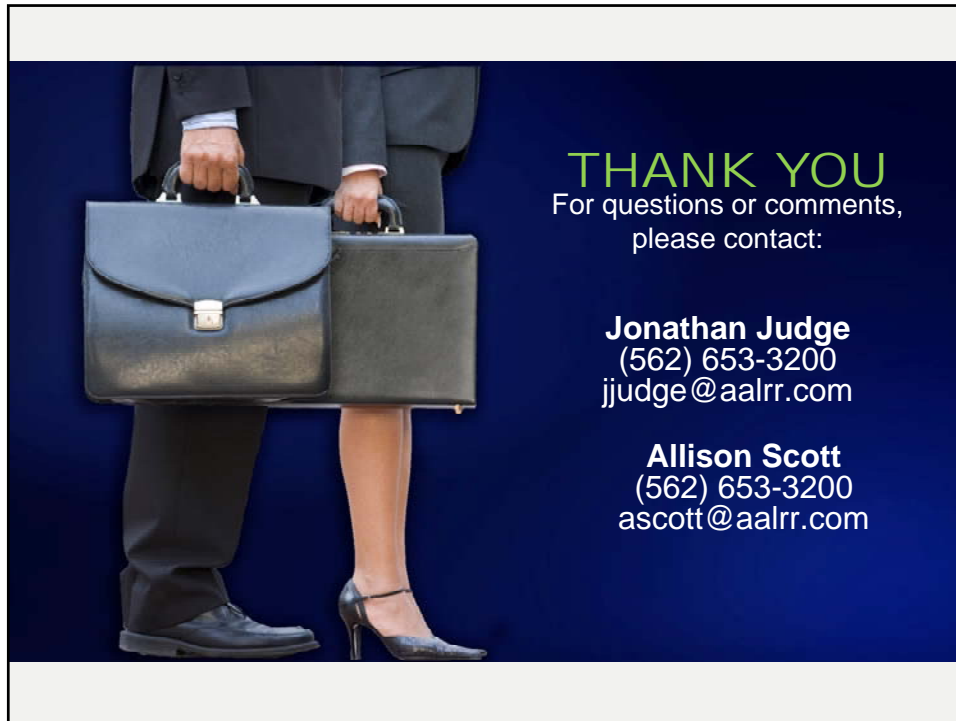


Disclaimer

This AALRR presentation is intended for informational purposes only and should not be relied upon in reaching a conclusion in a particular area of law. Applicability of the legal principles discussed may differ substantially in individual situations. Receipt of this or any other AALRR presentation/publication does not create an attorney-client relationship. The Firm is not responsible for inadvertent errors that may occur in the publishing process.



© 2018 Atkinson, Andelson, Loya, Ruud & Romo



THANK YOU
For questions or comments,
please contact:

Jonathan Judge
(562) 653-3200
jjudge@aalrr.com

Allison Scott
(562) 653-3200
ascott@aalrr.com