The Future of Employee Privacy

Michael J. Gentry
414-298-8715
mgentry@reinhartlaw.com

Reinhart Boerner Van Deuren s.c.
1000 North Water Street, Suite 1700, Milwaukee, WI 53202
www.reinhartlaw.com

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Roadmap

1. Managing Employee Privacy in the U.S.

2. Emerging Issues with Managing Employee Privacy

3. New State and International Data Privacy and Security Obligations

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Traditional Employee Privacy: Public vs. Private

- Public employers: Individuals do not give up their rights under the Fourth Amendment to be free from unreasonable searches and seizures by going to work for the government
- Private employers: Right of privacy only exists to the extent granted by state law or agreement with employees

Traditional Employee Privacy: Invasion of Privacy Claims in Wisconsin

- Statutory claim for Invasion of Privacy applies in workplace: four types of claims. Wis. Stats. § 995.50.
  - Intrusion upon the privacy of another of a nature highly offensive to a reasonable person
  - The use, for advertising purposes, of the name, portrait or picture of any living person, without consent
  - Publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person
  - Violating Wisconsin's law against taking nude pictures of another without consent

Using Employee Handbooks to Manage Employee Privacy Expectations

- More than general "no expectation of privacy"
- Technology policy: Whose device? Whose data?
- Use of company equipment/Internet, e-mail and social media policies
- Reserve right to modify
- Keep signed acknowledgement of receipt for changes made to handbook or policies

Using Handbooks and Contracts to Manage Employee Privacy Expectations

- Does employee handbook define:
  - An employee's responsibilities regarding data privacy and security (mobile devices, work devices, remote access)?
  - What happens (who owns) data when an employee leaves?
  - Levels of data authorization (or cross-reference an acceptable use policy)?
- Vendor contracts — you must inform us if you suspend/terminate an employee with access
- HR — first line of defense — investigate before terminating

Using Contracts and Litigation to Manage Employee Privacy Expectations

- Confidentiality agreements — under what circumstances?
- Return of company property agreements — data = property
- Do agreements allow you to search for and delete your data?
- Do agreements require employee to notify? Delete? Cooperate after quitting?
- Litigation: preserve and document
  - Most sensitive material taken within week of quitting
  - Document steps taken to retrieve data or uncover theft of data

Emerging Issues with Managing Employee Privacy

What counts as data?

- Individual data: State laws typically define personally identifiable information (PII) as an individual's first name or initial with last name and one or more of the following (unencrypted) data elements:
  - Social Security number
  - Driver's license number or state or military identification card number
  - Financial account, credit card, or debit card number in combination with any required security code, access code, or password that permits access to an individual's account
- Sensitive company data:
  - Trade secrets, customer lists, pricing information, vendor contract terms
  - Salary history, EEO information, human resources investigation files

Emerging Issues with Managing Employee Privacy (cont.)

Reasonable Security Measures

- Nineteen states now require employers (of residents of their states) to implement "reasonable security measures" with regard to their maintenance or destruction of employee data
- Some states define "reasonable security measures" while others do not
- Some states require written policies specifying practices
- Requirements when data breached: enhanced notification requirements, fines. Less frequent: private right of action.

Emerging Issues with Managing Employee Privacy (cont.)

Reasonable Security Measures

- Wisconsin
  - Has not adopted reasonable security measures requirement
  - Employers must abide my data breach notification requirements. Wis. Stats. § 134.98.
- Illinois
  - Has adopted reasonable security measures requirement
  - Biometric information privacy act requires reasonable care and protection of biometric information. 740 ILCS 14.

Emerging Issues with Managing Employee Privacy (cont.)

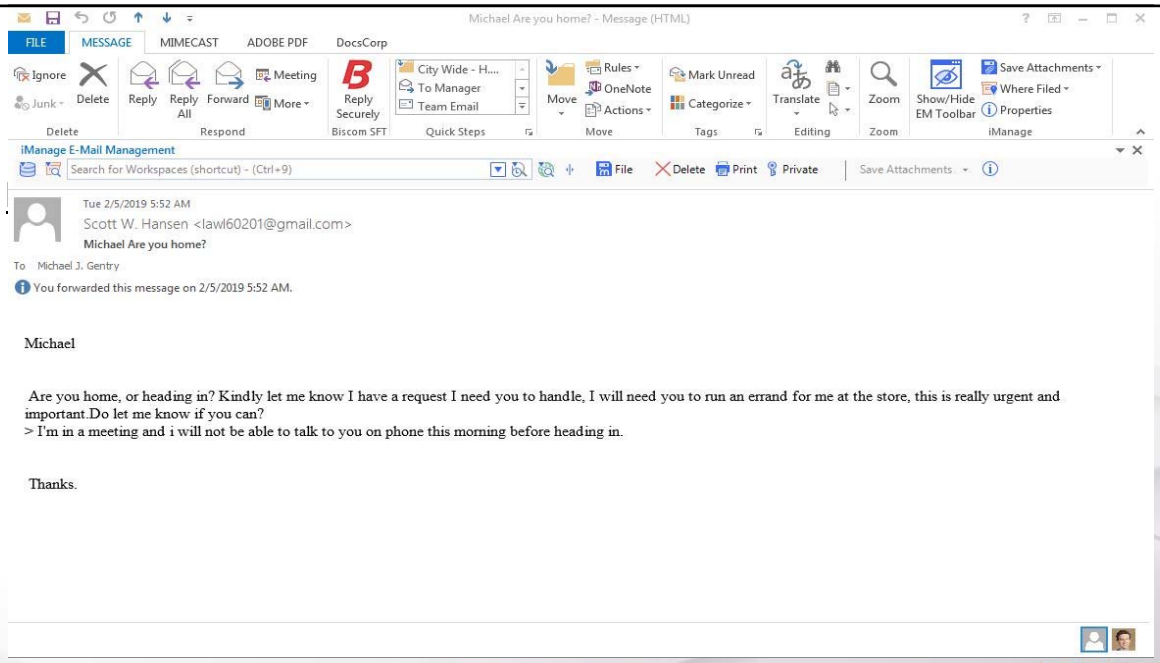
Recent Litigation Update

- Illinois' biometric information privacy law
  - Key update: Employees need not show particular harm to bring a claim under the biometric privacy law
  - *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 1, 2019 WL 323902, at *1.
- Wisconsin social media privacy law. Wis. Stats. 995.55.
  - DWD only recently received first complaint under this law
  - Employers may require access to employer devices, or require observance of data transfer

Emerging Issues with Managing Employee Privacy (cont.)

Preventing Employees From Becoming Insider Threats

- How are insiders a threat?
  - Phishing — not necessarily new tactic but still effective
  - Email addresses — public; identical; easy to guess (name@company.com)
  - Fake Gmail accounts of coworkers/team members
- Disgruntled employees
  - Employees have access to sensitive data until the access is turned off
  - Employees know they are leaving before you do



New International Obligations: Who Does the GDPR Apply to?

Established in the EU	Offering Goods or Services to people in the EU	Monitoring of data subjects in the EU
• HR company located in Germany • Data hosting service provider located in Ireland • Company with a distribution center in Italy	• U.S. online retail store sells and ships to customers in the EU with a website that offers payment in euros	• U.S. company with a website that places cookies on and tracks the IP addresses of EU-based website visitors • U.S.-based company that traces e-mails to customers in the EU

New International Obligations: GDPR Requirements

- Data subject rights
  - Right of access
  - Right of rectification
  - Right of erasure
  - Right of data portability
  - Right of restricted processing
  - Right to lodge a complaint
- Lawful basis
  - Contract with data subject
  - Consent
  - Necessary to comply with a legal obligation
  - Necessary to protect the vital interest of the data subject or another person
  - Public interest
  - Legitimate interest of processing

New State Law Obligations: California Consumer Privacy Act

- Effective January 1, 2020
- Protects California residents' "personal information" — broad definition
- Applies to any company that receives California resident personal information, and meets one of the following criteria:
  - Annual gross revenues of $25 million
  - Obtains "personal information" on 50,000 residents
  - Receives at least 50% of annual revenue from selling California resident "personal information"

New State Law Obligations: California Consumer Privacy Act (cont.)

- If CCPA applies:
  - Consumer/employee right to request disclosure of what personal information is collected and why
  - Consumer/employee right to request deletion of personal information (with exceptions)
  - Consumer/employee right of access and portability of their data
  - Consumer/employee right to be forgotten
  - Enforced by the Attorney General of California and provides for a private right of action

Questions?

Thank You!

This presentation provides information of a general nature. None of the information contained herein is intended as legal advice or opinion relative to specific matters, facts, situations or issues. Additional facts and information or future developments may affect the subjects addressed in this presentation. You should consult with a lawyer about your particular circumstances before acting on any of this information because it may not be applicable to you or your situation.