Legal Landmines in Data Investigations

Secure Iowa Conference

October 6, 2021

BROWNWINICK LAW

Nate Borland

Counsel

515-242-2408

nate.borland@brownwinick.com

www.brownwinick.com

Overview

- Collecting, Storing, Searching, and Analyzing Data
- Using Collected Data to Make Decisions
- Publishing or Sharing Collected Data
- Scenarios
- Q & A

Collecting, Storing, Searching, and Analyzing Data

Iowa: Employment at Will

- Employment at will is the default rule
- Employment agreements may displace general rule
- Employee or employer may terminate the relationship at any time, for any reason or no reason
- Exception: Employer may not discharge an employee for an illegal reason (harassment, discrimination, retaliation, public policy)

Employment at Will (cont.)

- Because the default rule is employment at will, employees' workplace-specific rights are mostly contained in laws passed by the legislature
- Absent a statute, an employment agreement, or some other enforceable promise, employers in Iowa are generally free to dictate the terms and conditions of employment
- Resignation is typically an aggrieved employee's only recourse

Sources of Law

- Statutes and Regulations
  - State
  - Federal
- Common Law
  - Torts
  - Contracts

Relevant Statutes and Regulations

- Data investigations may involve the collection of electronic communications, audits of access and event logs, forensic imaging of entire devices, or searches of other data stores
- May occur live, with targeted monitoring of a subject's activity
- May be limited to the collection of stored (existing) data

Collection of Live Data Intercepting Electronic Communications

- State Laws
  - Iowa Code Ch. 715 – Computer Spyware and Malware Protection
  - Iowa Code Ch. 715C – Personal Information Security Breach Protection
  - Iowa Code Ch. 808B – Interception of Communications
- Federal Law
  - 18 U.S.C. Ch. 119 – Wire and Electronic Communications Interception

Collection of Live Data

- Violating state or federal law exposes the company (and those performing the work) to civil and criminal liability, including punitive damages
- State and federal laws recognize **prior consent** as an exception to the prohibition on the interception of live electronic communications and oral communications

Prior Consent - Policies

- Courts have recognized consent to the interception of electronic communications when an employer notifies an employee:
  - Communications will be monitored
  - Handbook/manual provides that all electronic communications are subject to archiving
  - Specifies that electronic communications sent, viewed, or routed through company equipment are not private

Prior Consent - Policies

- Courts have **refused** to recognize consent to the interception of electronic communications when:
  - Employer occasionally threatened to monitor calls
  - Employer failed to provide details on monitoring, such as who would be subject to monitoring
  - Employee merely knew of monitoring **capability**

Prior Consent – Best Practices

- Detailed policy specifying that **all** electronic communications exchanged using employer's equipment, or personal (BYOD) equipment on employer's infrastructure, is subject to monitoring, recording, and storage
- Written consent (such as a policy acknowledgement page)

Stored Data

- Federal Law
  - 18 U.S.C. Ch. 121 – Stored Wire and Electronic Communications
- Protects electronic communications in "electronic storage"
  - Temporary, intermediate storage of an electronic communication incidental to the electronic transmission thereof; and
  - Storage of such communication by an electronic communication service for purposes of backup protection
- Must have authorization to access (and must not exceed that authorization)

Stored Data (Cont.)

- Generally, information stored by the employer, and accessed by those with appropriate authorization, will not be problematic
- Employer should notify employees, through a policy or handbook, that electronic communications will be stored and may be accessed and reviewed by the employer
- Investigators should ensure they stay within the confines of the policy

Stored Data (Cont.)

- Accessing an employee's data on third-party infrastructure, such as using the employee's credentials to access a social media account or personal email account, without proper authorization, is problematic and should be avoided. Consent is essential.
- Consult with legal counsel if there is a need for such information and the subject has not consented

BYOD

- Same rules apply for BYOD and company devices, but expectation of privacy is heightened for BYOD
- If the subject of your investigation has not provided consent to the interception of electronic communications (or if the consent or underlying policy is deficient) consult legal counsel
- Confirm consent **before** intercepting electronic communications as part of a data investigation

Forensic Imaging

- Imaging and analyzing a company-owned device is generally permissible. Again, policies and acknowledgement can be used to prove consent.
- For personally owned devices, the employer should obtain the employee's consent in writing and obtain the image through cooperation.
- Employees who refuse to cooperate may be disciplined, but human resources or legal should be consulted.

Using Collected Data to Make Decisions

Sensitive Information

- Several state and federal laws prohibit the consideration of protected characteristics in making employment decisions
- Iowa Civil Rights Act: Age, race, creed, color, sex, sexual orientation, gender identity, national origin, religion, disability
- Federal Laws: Race, color, religion, sex, national origin, age, disability

Sensitive Information

- State and federal laws prohibit the use of genetic information in making employment decisions. Investigators should avoid analyzing, or producing to decisionmakers, confidential health information (e.g., Health app data)

Sensitive Information

- State and federal laws prohibit employers from retaliating against employees who exercise a right afforded to them by law
- In Iowa, this includes complaining about harassment or discrimination, making a claim for workers' compensation, complaining about illegal activity, reporting illegal activity to the authorities, and the like
- An investigation may reveal this type of protected activity

Sensitive Information

- An investigation may make obvious an otherwise "invisible" characteristic. Information obtained during an investigation that reveals a protected characteristic should not be considered in making business decisions.
- An investigation may reveal protected activity that was not previously known. This should not be considered in making business decisions.

Business Decisions

- Depending on an organization's size, investigators may be consulted about potential sanctions like disciplinary action or termination
- The investigator must not allow a protected characteristic or protected activity to influence their position
- Consider excluding the investigator from such discussions – they provide sanitized results and allow others (whose views could not be tainted by sensitive information) to make decisions

Publishing or Sharing Collected Data

Common Law – Tort Claims

- Employers' liability for violating an employee's privacy generally comes in the form of tort claims
- Invasion of Privacy
  - Unreasonable intrusion upon the seclusion of another
  - Appropriation of a person's name or likeness
  - Unreasonable publicity given to another's private life
  - Publicity unreasonably placing another in a false light

Invasion of Privacy
Intrusion Upon Seclusion

- "It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man."
- For example, clandestinely obtaining a forensic image of a personally owned device, in the absence of any policy or consent regarding the same.

Invasion of Privacy
Publicity of Private Life

- One who gives publicity to a matter concerning the private life of another if the publication would be highly offensive to a reasonable person and is not of legitimate concern to the public.
- For example, publishing (or even sharing with internal users who have no need to know) private information of another obtained during an investigation

Invasion of Privacy
False Light

- One who gives publicity to a matter concerning another that places the other before the public in a false light, if the false light would be highly offensive to a reasonable person and the actor had knowledge of or acted in reckless disregard as to the falsity of the matter and the false light.
- For example, publishing (or even sharing with internal users who have no need to know) information obtained during an investigation in a misleading manner (or with a negative implication)

Iowa Laws

- Iowa Code §§ 730.1-730.3:
  - May not, after discharging an employee, "prevent or attempt to prevent, by word or writing of any kind, such discharged employee from obtaining employment with any other person…"
  - May not "authorize or allow any of its or their agents to blacklist any discharged employee, or attempt by word or writing or any other means whatever to prevent such discharged employee, or any employee who may have voluntarily left said company's service, from obtaining employment…"
  - May not falsely allege dishonesty against an employee

Maintain Confidentiality

- The best way to avoid liability for libel, defamation, or invasion of privacy is to maintain the confidentiality of all information obtained during an investigation
- Do not disclose to others (without a need to know) the results or specific findings of the investigation
- Implement and enforce policies requiring investigators to maintain confidentiality

Scenarios

Scenario 1

I know an employee has a company-owned computer in their backpack, and I want to look at it. Can I open their backpack and take out property that the company owns?

Thoughts?

Scenario 1

- Company policy may provide for searches of employee belongings on the premises.
- Company policy should provide that company-owned computers are subject to monitoring and search at any time.
- Generally, you may demand that the employee produce the company-owned laptop for analysis/investigation.
- Do not resort to self help if the employee refuses.

Scenario 2

A manager is out to get an employee, so they go to the IT team and tell them to dig around in the employee's digital activities on company devices to see if they're up to no good. Is the manager justified in this kind of fishing expedition? Who else should be involved in that decision?

Thoughts?

Scenario 2

- Lawyers will want to know **why** the manager is out to get an employee. If it's based on a protected characteristic or protected activity, it may expose the company (and manager) to liability.
- If the investigator suspects an illegal motivation, the investigator should seek assistance from human resources or legal.
- The search should be conducted in accordance with company policies.

Scenario 3

If we discover digital employee activity that is likely to get law enforcement involved, how should I proceed in terms of doing my own digging into the records? Could I damage evidence that the police/FBI need? Could I create liability for my company?

Thoughts?

Scenario 3

- Follow forensic best practices if you suspect illegal activity could be involved. Preserve the original device and work from an image.
- If you discover evidence of illegal conduct, **immediately** contact human resources or legal.
- Consult with law enforcement before taking any additional action.

Scenario 4

How do you effectively craft BYOD policies when the lines are so blurry between personal and business activities, devices, time, etc.?

Thoughts?

Scenario 4

Check out Trevor's blog post: https://pratum.com/blog/510-what-to-include-in-an-effective-byod-policy

- Work with human resources and managers to identify potential issues
- Provide for monitoring, collection, and analysis of electronic communications and stored communications

Q & A

Be Bold. Be Wise.