Privacy in a Pandemic, Part II

Discussion of privacy issues during the COVID-19 pandemic

WINSTON & STRAWN LLP

Speakers

Sheryl Falk

Partner, Houston
sfalk@Winston.com

Aviva Grumet-Morris

Partner, Chicago
agmorris@Winston.com

Alessandra Swanson

Partner, Chicago
aswanson@Winston.com

Privacy Challenges

Employee Privacy	▪ Employee health screenings ▪ Communications related to employee positive COVID-19 diagnoses ▪ Teleworking
State & Federal Privacy Law Guidance	▪ Privacy issues in collection of employee data ▪ Facial scanning technology in the workplace ▪ CCPA Update
Data Security Issues	▪ Verizon data breach report - guidance on data security risks ▪ Remote work tip: How to secure a VPN ▪ Cyber-attack breach response and notification legal update

WINSTON & STRAWN LLP

Employee Privacy Questions

Aviva Grumet-Morris

The ADA

- The Americans with Disabilities Act (ADA):
  - Regulates “disability-related inquiries” and “medical examinations” of job applicants and employees.
  - Requires employers to maintain the confidentiality of medical information.

COVID-19 and Employee Privacy

- 3 Situations:
  - Employee health screenings
  - Communications related to employees' positive COVID-19 diagnoses
  - Teleworking and employee privacy

Question 1 – Employee Health Screenings

- Q. An employer's health screening program requires that before entering the workplace, employees take their own temperatures (or submit to onsite temperature testing) and answer questions regarding symptoms and COVID-19 exposure. An employee refuses to allow her temperature to be taken or to answer the COVID-19 questions. Must the employer admit her to the workplace?

- A. No. COVID-19 presents a **direct threat to employee health and safety**, permitting the exclusion of employees who refuse to submit to screening processes designed to assess COVID-19 symptoms and exposure.

Question 2 – Employee Health Screenings

- Q. Can a manager ask only one employee – as opposed to asking all employees – questions designed to determine if he has COVID-19, or require that this employee alone have his temperature taken?

- A. Yes, *if* the employer has a **reasonable belief** based on **objective evidence** that this employee might have the disease.

Question 3 – Communications Regarding Positive Diagnoses

- Q. A supervisor receives a call from an employee who has tested positive for COVID-19. The supervisor knows that the information is confidential, but she also knows that it is important to report an employee's positive COVID-19 diagnosis. What should she do?

- A. Report to the company's COVID-19 point person, following pre-established protocols for confidentially transmitting the information.
  - The identity of the sick employee is confidential medical information.
  - Both the supervisor and the COVID-19 point person should minimize the number of people who know the identity of the positive employee.

Questions 4 – Communications Regarding Positive Diagnoses

- Q. An employee tests positive for COVID-19 and reports that information to his or her manager. A notification goes out to employees that "an employee" has tested positive for COVID-19. The manager believes other employees must be told the identity of the sick employee. Can the manager disclose the name of the sick employee?

- A. No. The ADA does not allow this disclosure.

Question 5 – Teleworking

- Q. An employee diagnosed with COVID-19 begins to telework (work from home) while he is self-quarantining. Can his managers tell the sick employee's coworkers that he is teleworking? Can they tell others why he is teleworking?

- A. The managers may tell the coworkers that the employee is teleworking but not the reason why he is teleworking.

Question 6 – Teleworking

- Q. While the workforce of a company continues to telework, a manager is informed that one of his direct reports has tested positive for COVID-19. How should the manager maintain the confidentiality of this information, given his own remote work situation?

- A. Follow confidentiality protocols:
  - Confidentially report the information to the designated COVID-19 point person.
  - Safeguard the information.
  - Do not store documentation electronically where others have access.
  - Consider how to confidentially transmit information.

WINSTON & STRAWN LLP

Complying with State & Federal Privacy Law

Alessandra Swanson

Question 1

- Q. What does my company need to think about when collecting personal information in connection with employee health checks?

- A. Consider the following as you develop and implement your health check program:
  - Minimize the personal information you collect.
  - Understand the data flow and who may have access to the personal information.
  - Enable appropriate data security controls.
  - Provide notice as necessary to comply with applicable laws (e.g., the California Consumer Privacy Act).

Question 2

- Q. My company is looking for an effective method to take employee temperatures without having to do so manually. Can we use a tool that will use facial scanning technology to identify employees, take their temperatures and record the results?

- A. Yes, BUT…
  - Think about what jurisdictions in which you will use the tool, as some states strictly regulate biometric data.
  - Research the vendor and conduct diligence to understand whether the vendor is equipped to capture and/or store biometric information.
  - Ensure appropriate contractual (e.g., data security) insurance provisions are in place.
  - Ask whether you REALLY need the biometric data.

Question 3

- Q. Whatever happened with CCPA? Did the California Attorney General ever finalize the implementing regulations? Will the regulations impact my company's collection of employee information?

- A. The California Attorney General issued the final set of CCPA implementing regulations on June 1.
  - The regulations do not yet have the force of law.
  - The regulations did not substantively change from the third draft set of implementing regulations that were issued in March.
  - The regulations formalize the employment privacy notice requirement.
  - This provision sunsets on December 31, but the ballot initiative for the California Privacy Rights Act of 2020 contemplates extending the related CCPA exemption until January 1, 2023, to allow time for additional regulation.

WINSTON & STRAWN LLP

Data Security Challenges

Sheryl Falk

Verizon DBIR 2020 Update

Most common attacks:

- Credential theft & social engineering – 67%
  - Stolen or weak credentials, phishing, human error
- Cloud-based attacks have doubled in the past year – 24%

Guidance:

1) Strong credential management
   - Instruct employees not to use work email for personal accounts
   - Never reuse passwords
2) Multi-Factor Authentication for all critical systems
3) Phishing education for employees

Question 1

Q. If our company uses a VPN for our remote work force, does that mean we are safe from Cyber-attacks?

A. No. A secure VPN is a good start, but it doesn't mean you won't get hacked.

- A VPN encrypts computer traffic between your computer and VPN provider
- VPNs have been a popular attack vector
- VPNs must be securely configured
  - Multi-factor authentication
  - Use the strongest encryption method for VPN access
  - Secure wireless networks for remote employees
  - Keep updated with security patches

Question 2

Q. Our company had a data breach and hired a data security vendor. Is the incident response report privileged?

A. It depends.

- New Court ruling: In re: Capital One. Held report was not privileged
- Best practices:

1. Engage legal counsel at the beginning to lead the investigation
2. Have outside counsel retain forensic firm and direct the work
3. Ensure report is prepared for the purpose of anticipated litigation
4. Pay for the forensic work out of the legal budget
5. Limit dissemination of report

Question 3

Q. What new data security laws should be on in-house counsel's radar?

A. Vermont Breach Notification

- 14-day notice to Office of the Attorney General
- 45-day notice to consumers
- Effective July 1, 2020

- New California Ballot initiative
  - Expands reasonable security requirement

- Federal Privacy legislation

Take Aways & Wrap up

Sheryl Falk

Partner, Houston
sfalk@Winston.com

Aviva Grumet-Morris

Partner, Chicago
agmorris@Winston.com

Alessandra Swanson

Partner, Chicago
aswanson@Winston.com

WINSTON
& STRAWN
LLP