ACC NCR PRIVACY FRIDAY: CYBERSECURITY, DATA PRIVACY AND INSURANCE DURING THE COVID-19 PANDEMIC: IS YOUR COMPANY PREPARED?

OCTOBER 2, 2020 | PRESENTED BY: SELENA J. LINDE, PERKINS COIE LLP
KARIN SCHERNER ALDAMA, PERKINS COIE LLP
AUDREY JEAN, AARP

MODERATOR: ILONA LEVINE, INTERNET SOCIETY

Moderator: Ilona Levine

Ilona Levine is General Counsel of Internet Society in Reston, and prior to that, General Counsel of China Telecom America. She's an ACC NCR Leadership Academy alum, frequent speaker on ACC NCR panels and a cochair of the ACC NCR Privacy and Data Protection Forum. As part of her job, she has been in charge of building out Privacy and cybersecurity compliance programs at her current and former companies.

Presenter: Selena Linde

Selena Linde is a nationally ranked Insurance Recovery Partner and the Chair of Perkins Coie's Insurance Recovery Practice. Ms.Linde is a primary author and editor of the first edition of the Association of Corporate Counsel's Policyholders Primer on Insurance and has been honored as a worldwide recipient of *Business Insurance's* Women to Watch, a leading insurance attorney in *Best* Lawyers, and one of eleven National Insurance Stars and top 250 Women Litigators by *Benchmark.*

Ms. Linde has recovered more than two billion dollars for her clients and has an active trial practice representing policyholders in complex insurance coverage cases throughout the country and an equally active arbitration, mediation, and counseling practice. She has assisted dozens of clients with cyber and privacy claims ranging from small counseling matters to high profile claims in excess of $500M.

Ms. Linde is on the Perkins Coie Coronavirus Task Force and is currently representing more than two dozen clients with Covid-19 claims.

Join Ms. Linde's LinkedIn network for updates and articles on insurance coverage topics. She can be reached directly at (202) 654-6221 or SLinde@perkinscoie.com.

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

PERKINSCOIE

Presenter: Karin Aldama

Karin Aldama is an Insurance Recovery Partner at Perkins Coie. Karin focuses her practice on complex insurance recovery matters. She has represented policyholders on a number of complex issues under a variety of policies, including property and business interruption, cyber, and third-party liability. In addition, Karin has extensive experience with complex general commercial and appellate litigation, including in the international context and with respect to cross-border disputes.

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

PERKINSCOIE

Presenter: Audrey Jean

Audrey Jean is currently SVP, Senior Associate General Counsel and Privacy Officer at AARP, the largest tax-exempt organization dedicated to social mission, with 38 million members. Audrey manages privacy compliance for the organization and its various subsidiaries, and advises the public policy and government advocacy teams on privacy trends and legislation as it impacts older Americans. She also oversees the legal work for M&A, Innovation, IP, Real Estate and Media Transactions at AARP. Audrey serves as a Co-Chair of the Privacy Forum for ACC-NCR.

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

PERKINSCOIE

Overview

Is your cybersecurity program, data privacy controls and Cyber Policy still adequate for your company? Covid-19 has changed the way companies conduct business and created additional risks in almost every area. For many industries, remote working is now the new normal , employees are using their own electronic devices instead of company electronic devices, and new vendors are being hired in large numbers. At the same time, cyberattacks have increased worldwide as sophisticated criminals find new ways to hack vulnerable networks. Further, privacy issues have also increased.

Companies are now conducting Covid-19 testing and collecting data from employees, vendors and customers that they never imagined they would collect just a mere nine months ago. In this presentation the speakers will walk through scenarios for companies who may face a breach in this heightened risk environment, the changes in risks for cyberattacks and privacy issues, and discuss key items to review in your current coverage and for renewal.

Poll Question #1

What is the current “opening status” at your company?

Poll Question #2

Is your company requiring any sort of health monitoring related to COVID-19?

Poll Question #3

If your company is requiring monitoring, what type?

SCENARIOS

SCENARIO #1

A multi-national retailer hires security personnel that ask employees health screening questions and take their temperatures upon arrival. If the health screening questions are answered appropriately and the employee does not have a fever, they are allowed to work. If the health screening questions leave the possibility that the person has been exposed to a confirmed case of COVID-19 or has had any symptoms, the employee is not allowed to work.

Poll Question #4

If your company is requiring monitoring of any sort, do you know what is happening with the data?

EXAMPLE

Incident: Employee sues after not being allowed to work. Employee states in complaint some individuals were allowed to work that had the same statistics.

Poll Question #5

If your company is requiring any sort of monitoring, what department at your company is in charge of directing the monitoring?

NEXT STEPS

- Privacy/Data Protection
  - How does the employee know that others with the same stats were allowed to work?
  - Privacy violations?
- Insurance Issues
  - Investigation
  - Notice to carrier—are you covered by insurance? EPL?
  - Consent to incur costs requirements
- Other
  - Discriminatory conduct?

SCENARIO #2

Employer mandates employees to install a Covid-19 application on their smart phone that requires employees to (1) answer health screening questions and (2) self-report their temperature. Employees are required to access the application and enter the information at least ½ hour before each shift.

Poll Question #6

If your company is requiring monitoring of any sort, have you been transparent with employees/customers/vendors on how the resulting data will be used, shared, and retained?

Poll Question #7

If your company is requiring any sort of monitoring, have your insurance policies been reviewed to determine whether you have coverage for potential claims associated with the monitoring?

SCENARIO #2 – QUESTIONS, Cont'd

- Insurance Issues
  - BYOD Issues?
  - Property Policies — exclusion for medical testing? Voids policy?
  - Industry-standard safeguards for collected data?
  - Any vendor implications?
- Other
  - Who owns the phone? Who pays for the service? What if an employee does not have a phone?
  - Vendor issues—who created the app? To what extend does that party have access to the data?
  - Indemnification? Additional insured status?

EXAMPLE

Incident: The application was breached and the data has been downloaded by an unknown hacker who is threatening to place it on the internet unless a ransom is paid.

Poll Question #8

Has your company experienced a ransomware or data breach since Feb 2020?

NEXT STEPS

- Privacy/Data Security
  - Privacy violations?
  - Notice to individuals? Regulators? Others?
- Insurance Issues
  - Investigation
  - Notice to carrier—are you covered by insurance?
  - Mitigation?
  - Insurer consent to costs?
- Other

SCENARIO #3

Large accounting firm that has been closed for three months and wants to reopen. It decides to hire a vendor to conduct actual COVID-19 testing. How should the firm implement that testing, and what should it consider prior to testing?

Poll Question #9

Has your company required COVID-19 testing of any employees?

EXAMPLE

Incident One: Testing is taking place in the lobby of the building. Employee refuses to be tested and brings suit against the employer for invasion of privacy related to the forced medical testing.

EXAMPLE

Incident Two: The testing center was set up under a tent in the parking lot of the building. Testing was conducted by a vendor the employer hired. During testing an employee was injured (swab stuck too far into the nose resulting in excessive bleeding and pain). The employee files a lawsuit.

EXAMPLE

Incident Three: Vendor informs employees that all data associated with the testing was hacked.

SCENARIO #4

Professional Service firm closes its offices indefinitely and asks all employees to work remotely. The firm will purchase select office equipment for those who do not have computers at home.

Poll Question #10

If you have employees working from home, how is your company handling electronic devices?

EXAMPLE

Incident: A secretary was using a personal computer for work and was hacked allowing cybercriminal to download confidential communications. Two weeks later the firm receives a ransom demand.

SCENARIOS #5 AND #6

After reopening, a consumer-facing store decides to implement health screening questions and to take the temperatures of customers. Customers cannot enter the store unless they comply. Further, the store is also requiring employees to install an additional app that monitors their location and sends an email to the employee and the employer if the employee has been in confirmed proximity to someone who has been confirmed to have COVID-19.

Questions??

Selena Linde

202-654-6257

Karin Aldama

602-351-8270

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

PERKINSCOIE