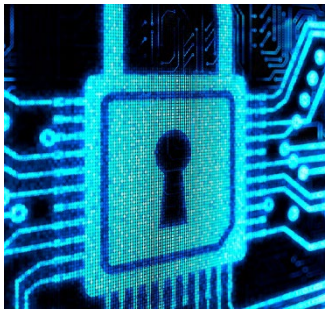
Return to Work—Privacy & Data Security Checklist



Today commercial landlords and tenants are preparing to safeguard their employees and customers from COVID-19 risks. Thermal cameras to measure temperatures, facial recognition, Bluetooth, Wi-Fi, and GPS are all being leveraged to track and trace the contagion. There are privacy notice requirements as well as security controls necessary to avoid privacy pitfalls. We can help.

PRIVACY TIPS

☐ Vet vendors by obtaining privacy and security assurances.

Make sure vendors can ensure compliance with privacy laws.

☐ Prepare a clear list of data to be collected and shared, and update privacy notices.

New types of health and location data will be collected. Privacy notices for customers, employees, and visitors need to be updated.

☐ Consider prominent notice in physical spaces.

The California attorney general, for example, has suggested use of a tablet or physical signage to comply with the California Consumer Privacy Act (CCPA).

☐ Pay attention to legal guidance now so there is not a brand backlash later.

- State laws (e.g., California Consumer Privacy Act (CCPA), California's Confidentiality of Medical Information, and Illinois' Biometric Info Privacy Act)
- U.S. federal guidance (e.g., issued by the Federal Trade Commission)
- Global laws (e.g., General Data Protection Regulation (GDPR), Chinese Network Security Law, Brazil's LGPD law)

SECURITY TIPS

- [ ] **Add new data collected for COVID-19 prevention or other related purposes to the company's information security plan (ISP).**

  An ISP needs to be updated to include the protection of sensitive health data.

- [ ] **Establish access controls to limit those who can view the data.**

  Consider limiting to a "need-to-know" the employees who can have access to the information.

- [ ] **Decide now how long the data is necessary and delete it thereafter.**

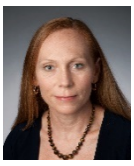
  Data minimization is a key issue that the Federal Trade Commission (FTC) insists upon.

- [ ] **Document steps taken to evidence reasonable security practices.**

  If health data collected for COVID-19 is breached, liability will hinge on whether a business had "reasonable security" practices in place. Reasonable security can be evidenced by mapping to an established data security standard (e.g., one issued by judicially respected sources such as the FTC, National Institutes of Standards and Technology (NIST), or the Center for Internet Studies). Lack of reasonable security is the trigger for class action lawsuits and can lead to nine-figure exposures.

Contacts

Dominique Shelton Leipzig
Partner
+1.310.788.3327 | VCARD
DSheltonLeipzig@perkinscoie.com



Jennifer Understahl
Partner
+1.602.351.8090 | VCARD
JUnderstahl@perkinscoie.com

Mindy Sherman
Partner
+1.312.324.8614 | VCARD
MSherman@perkinscoie.com