Capabilities

PRIVACY AND CYBER

Navigating today's maze of privacy laws is no easy task. From CCPA to GDPR, our team helps employers and businesses meet evolving data protection obligations, minimize risk, and safeguard sensitive information across every platform and workplace setting.

How we can help:

- Compliance & Risk Management
- Incident Response
- Litigation & Enforcement Defense

Although the U.S. hasn't yet enacted a federal consumer privacy law, businesses must contend with a growing patchwork of consumer protection and cybersecurity laws and regulations established by individual states. These laws typically provide consumers (including, where applicable, website or app users, employees, job applicants, independent contractors, and others) with new privacy rights that afford more transparency and control over the personal information that businesses collect about them. Each of these laws differs as to whom they apply, the personal information covered, data handling requirements, and potential penalties, among other provisions, so even if you're familiar with some of these state requirements, you shouldn't assume you're automatically compliant with all of them. This means ensuring compliance everywhere you do business. It's imperative to have trusted advisors help guide your compliance strategy.

The Fisher Phillips Privacy and Cyber Practice Group helps businesses nationwide with *all* aspects of state, federal, and international privacy and data security laws, including in the employment context, websites and applications, and all other

interactions that trigger privacy or data security obligations. We provide tailored plans to help you comply with every nuance of the myriad state, federal, and international laws and regulations, such as the California Consumer Privacy Act (CCPA) and its progeny across the U.S., as well as the European General Data Protection Regulation (GDPR) and other countries' privacy laws and regulations. We can help you to avoid costly litigation, government enforcement actions, and negative publicity, and to lawfully safeguard sensitive information. As part of a firm that focuses solely on employment law, we thoroughly understand every aspect of workplace law and policy that touches on privacy, and the unique privacy issues that can arise in the employment context.

Fisher Phillips' Privacy and Cyber Practice Group also works collaboratively with Fisher Phillips' Artificial Intelligence Practice Group to address privacy issues in the AI context and to counsel employers on changing laws and regulations, create policies with privacy concerns in mind, and to handle privacy-based concerns with the use of AI technology in the workplace.

Fisher Phillips is a member of the International Association of Privacy Professionals (IAPP). Several members of the Data Security and Workplace Privacy practice group hold IAPP certifications, including the CIPP/US, CIPP/E, CIPP/C, CIPM, and CIPT designations.

PREVENTION AND COMPLIANCE

Because so many laws now implicate privacy concerns, we'll proactively help you keep tabs on all federal, state and international laws and regulations such as the myriad U.S. state consumer privacy laws – for which the firm has a dedicated Consumer Privacy Team – as well as the Illinois Biometric Information Act (BIPA), and state laws enacted in Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia.

Our team can help you:

- Determine whether these laws apply to your business
- Advise on all steps necessary for compliance and provide templates
- Prepare or revise online privacy policies and notices to employees and consumers
- Craft and update policies on employee use of personal devices ("BYOD"), remote work or telework, social media, email, and the internet, as well as the use of evolving technologies for tracking and monitoring employees
- Perform cybersecurity audits

- Complete your annual privacy impact assessment (PIA) or privacy audit
- Manage vendor relationships and negotiate and draft effective data security agreements
- Adhere to government contractor regulations
- Comply with country-specific and European Union data protection laws and directives
- Advise on responses to consumer requests

Our other capabilities include:

- **DATA BREACH RESPONSE.** We will help you address data breaches if they occur. This includes complying with various notification requirements and teaming with you to develop a legally compliant response that also works to ease the concerns of your workforce. We can also help you respond to ransomware attacks and other incidents threatening the security of your sensitive data.
- **EMPLOYEE MONITORING.** Because employers, especially multistate employers, must be careful not to violate any of the various state, federal, or international laws that limit how they may lawfully collect, process, or use employee information, we'll help you navigate the maze of laws that control how you may engage in monitoring and surveillance in the workplace, on devices employees use for work (whether personal or company-issued), and in company vehicles.
- **DEFENDING CLASS ACTION LAWSUITS AND OTHER LEGAL ACTIONS.** We defend claims arising from alleged violations of privacy and data security laws and regulations, whether they arise in court or at the administrative level. This includes claims for wiretapping or other violations of state or federal privacy laws based on a website's use of third-party cookies, pixels, beacons, tags, and other tracking technology, as well as BIPA and data breach class action lawsuits. Our team of experienced litigators can help you achieve positive and cost-effective results, specifically tailoring the defense of your company to your individual needs. We'll help you prepare for – and handle – regulatory enforcement actions under the CCPA and other state consumer privacy laws and from the Federal Trade Commission, which have the potential to seriously disrupt your business. We'll also advise on how to handle consumer inquiries and requests.
- **INTERNATIONAL DATA TRANSFER**. Many countries have data localization rules or legal restrictions on outbound data transfers. If you are looking to share information regarding your employees across jurisdictions, including information relating to EU residents, or between the U.S. and China, we can provide guidance

on recommended strategies for compliance with GDPR, applicable U.S. regulations, and other international laws impacting the transfer of such data.

HOW WE CAN HELP

- *Your company collects, maintains, processes, sells, or shares sensitive data, and/or transfers such data across borders.*
  Our team can provide advice regarding compliance with applicable laws and regulations at the local, state, federal, and international level, and assist as necessary to help you comply with those laws and regulations.

- *Your business wants to use technology to monitor employee productivity, especially given the rise in remote working arrangements.*
  Our team can counsel you on applicable laws and best practices regarding employee monitoring, including conducting a privacy program review, reviewing, updating, and drafting appropriate notices, consent forms, privacy policies, and procedures, and negotiating and reviewing agreements with third-party vendors.

- *Your business relies on third-party vendors to collect, use, process, store, or transmit protected personal data the company uses to engage with consumers or manage employee information.*
  Our team can provide guidance to help assess your third-party service providers' information security or privacy information management systems to determine whether they comply with applicable laws, contracts, regulations, or frameworks with which the company must comply.

- *Your business has been the victim of a cyberattack and is seeking guidance on how to secure systems and determine whether any notification obligations apply.*
  Our team can provide guidance on best practices to secure your systems, investigate the incident, and improve security practices to decrease the likelihood of a similar incident in the future. We can also provide guidance on applicable data breach notification obligations, including drafting notices and communicating with state agencies, as necessary.

MEMBERSHIPS

RESOURCES

Wiretapping Litigation Map

SERVICE FOCUS

Consumer Privacy Team

Data Protection and Cybersecurity

Digital Wiretapping Litigation

RESOURCE HUBS

U.S. Privacy Hub

KEY CONTACTS

Risa B. Boerner

Partner

Philadelphia

610.230.2132

Usama Kahf

Partner

Irvine

949.798.2118

INSIGHTS

Insights	Mar 5, 2026
California Privacy Agency Hits Student Ticketing Company With $1.1M Fine: 3 Lessons About Tracking Consumers	

Insights **Mar 4, 2026**

Major Win in CIPA Case Signals Higher Hurdles for Privacy Plaintiffs: What You Should Do to Protect Your Organization

Insights **Mar 2, 2026**

8 Key HIPAA Compliance Items for Businesses with Self-Insured Health Plans

Event **Feb 26, 2026**

Navigating HIPAA and Privacy Considerations Across Healthcare, MedTech, and Life Sciences

Insights **Feb 25, 2026**

7 Best Practices for Employers Using AI Resume Screeners

Insights **Feb 25, 2026**

India’s New Data Privacy Rules Are Here: 8 Steps for Businesses as Key Compliance Deadlines Approach