POLSINELLI

Privacy & Cybersecurity

The protection of data and personal information is of utmost importance to all organizations. Polsinelli recognizes this and has assembled a deep, diverse team whose sole focus is assisting organizations as they strive to protect the information, comply with ever-evolving privacy and security regulations, and respond to data incidents, regulatory investigations and litigation. Polsinelli's privacy team includes:

- Attorneys with international backgrounds, qualifications, and experience who are equipped to counsel organizations on evolving international data protection regulations.
- Former in-house data privacy attorneys who understand not only the regulatory landscape but the logistical and business considerations associated with creating and maintaining privacy and cybersecurity programs.
- Incident response attorneys who are some of the most experienced in the country.
- Alumni of enforcement agencies charged with enforcing privacy and security regulations, such as the Department of Health and Human Services Office for Civil Rights.
- A deep bench of technology transaction attorneys with experience working on privacy and security issues for mid-market to Fortune 500 companies.

Privacy Counseling

Polsinelli takes an interdisciplinary approach to privacy and cybersecurity by teaming attorneys with both data privacy and industry-specific experience. Polsinelli attorneys counsel clients on state, federal and international privacy laws, including CCPA/CPRA and other emerging comprehensive state privacy laws, HIPAA, GLBA, CAN-SPAM, COPPA and FCRA.

Polsinelli's privacy group also has deep experience in international privacy laws such as the EU General Data Protection Regulation (GDPR) and its UK equivalent, as well as the laws of other countries such as Brazil, Australia, Canada, India, and China.

Polsinelli attorneys also counsel clients on payment card processing (PCI) regulations, technology transactions and third-party data transfer, vendor and business associate agreements.

Our privacy team prides itself on providing practical, pragmatic advice using a risk-based approach that takes into account both the business and legal needs of our clients. Representative examples of our work include:

- Developing and implementing enterprise-wide privacy compliance programs to include GDPR, CCPA/CPRA, and other U.S. and international laws.
- Overseeing privacy and security risk assessments and gap analysis.
- Providing outside privacy counsel services including a dedicated privacy hotline.
- Undertaking data mapping assignments in order to assist clients with EU Records of Processing Activities and general data inventories as necessary under CCPA and other privacy laws.
- Formulating and implementing organization-specific policies and procedures.
- Advising on domestic and international cookie and web tracking regulations.

- Providing privacy and data security counseling and training.
- Developing data subject response policies and procedures.
- Conducting privacy due diligence in M&A-related transactions.
- Counseling on complex areas of privacy compliance in industries such as ad tech, use of clinical trials, machine learning, and artificial intelligence (AI).

Data Incident Response & Preparedness

Polsinelli attorneys have a long history of counseling clients impacted by data breaches and other cyber incidents. In fact, one of our shareholders handled one of the first data breach cases after California passed its breach notification law in 2003. Our attorneys collectively have handled more than two thousand data security incidents and have counseled clients through nearly every conceivable breach, from system-wide malware and ransomware attacks, network intrusions and misconfigurations, third-party/vendor breaches and business email compromises to misdirected emails. Our incident response team provides a full spectrum of services — from data breach response, internal investigations and litigation, to policy development and industry-specific compliance and regulatory counseling.

Our interdisciplinary approach encompasses all aspects of data and system security, both before and after an incident. When an incident occurs, we provide comprehensive assistance, including overseeing forensic investigations and crisis management activities, notifications to affected individuals, regulators and payment card issuers, responding to federal and state regulatory inquiries and litigation defense. Additionally, Polsinelli's rapid response capability is augmented by the strong working relationships we have with other vitally important professionals that may be needed to respond to a breach, such as forensics, crisis management and public relations services, providers of identity theft protection services and call and mail centers.

Polsinelli attorneys have served a broad range of clients in multiple sectors, including consumer brands, franchise, banking and financial services, health care, pharmaceutical, technology, e-commerce, trade associations, for-profit and not-for-profit education, retail, manufacturing, life sciences, food and beverage, accounting, legal and other professional services. Our attorneys also have extensive litigation experience and have represented clients in a broad range of privacy, data security, technology and other cyber-related individual lawsuits and class actions in state and federal courts across the country.

Matters

Our privacy team prides itself on providing practical, pragmatic advice using a risk-based approach that considers our clients' businesses and legal needs. Representative examples of our work include:

- Developed and implemented enterprise-wide privacy compliance programs to include GDPR, CCPA/CPRA and other U.S. and international laws.
- Oversaw privacy and security risk assessments and gap analysis.
- Provided outside privacy counsel services, including dedicated privacy hotline.
- Undertook data mapping assignments in order to assist clients with EU Records of Processing Activities and general data inventories as necessary under CCPA and other privacy laws.
- Formulated and implemented organization-specific policies and procedures.
- Advised on domestic and international cookie and web tracking regulations.
- Provided privacy and data security counseling and training;
- Developed data subject response policies and procedures.
- Conducted privacy due diligence in M&A-related transactions.
- Counseled on complex areas of privacy compliance in industries such as ad tech, use clinical trials, machine learning, and AI.

- Served as breach response and litigation counsel for financial institution that lost backup tapes containing account information of approximately two million customers.
- Served as breach counsel for academic health system in connection with an incident arising from a threat actor's deletion and attempted extortion for the return of the ePHI of approximately 80,000 patients residing across the U.S. and in multiple foreign jurisdictions.
- Served as breach counsel for financial institution that was the target of ransomware and extortion attack involving the acquisition and posting on various social media sites the sensitive member information and personal information of more than 46,000 of the institution's members and other affected individuals.
- Served as breach response counsel for an international financial institution whose Office 365 e-mail accounts of users in the United States and the United Kingdom were compromised, potentially triggering the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies and the United Kingdom's Data Protection Act of 2018.
- Served as breach response counsel for more than one hundred incidents involving credit unions across the United States, including ransomware, extortion, fraudulent wire transfers, Office 365 e-mail account compromises, network intrusions and employee misconduct.
- Served as counsel for manufacturer whose production line system was compromised, resulting in intentional alteration of product specifications and demand by threat actor for payment to cease further product alterations and information on past product alterations.
- Served as breach response counsel for health care system that experienced a malware attack potentially impacting approximately four million customers and 40,000 employees.
- Served as breach counsel to a university following a brute-force password attack, compromising personally identifiable information (PII) of over 60,000 students, alumni and employees residing in more than 40 states and several foreign countries.
- Served as breach response counsel for website/e-commerce hosting services provider that sustained a malware attack impacting hundreds of third-party companies that used client's hosting services as well as thousands of those companies' customers.
- Served as breach response counsel for health care system in connection with potential exposure of radiological records of approximately 400,000 patients.
- Served as breach response counsel and law enforcement liaison for a national restaurant chain in connection with possible insider theft of payroll records.
- Served as breach response counsel for community bank that sustained malware attack on an online banking portal, impacting customers across numerous states.
- Served as breach response counsel for health care provider investigating whether patient information was stolen as part of an identity theft ring focused on illegally acquiring prescription medications.
- Served as breach response counsel for law firm following theft of the firm's servers containing PII and protected health information (PHI) of approximately 20,000 clients, adversaries and witnesses in multiple states.
- Assisted major financial institutions to update and improve information security and data privacy practices, including data breach response procedures and conducting data privacy audits to identify potential privacy and data security issues.
- Conducted tabletop exercises for members of a New York-based hedge fund community.
- Counseled numerous entities in situations involving ransomware and other types of cyber-extortion.
- Counseled numerous entities in situations involving wire fraud and other types of cyber fraud.
- Conducted review of multinational food and beverage company information policies to ensure compliance with data privacy and security best practices.
- Conducted privacy and risk management audits for multistate retailers and life science companies.
- Developed employee training programs on information security and data privacy compliance for several investment advisers, broker-dealers and other financial service institutions.
- Performed comprehensive regulatory compliance and privacy audit of a Fortune 500 company with internal and external data flows spanning dozens of countries worldwide.
- Drafted and revised approximately 15 enterprise-wide internal privacy, security, access, and technology use policies for a well-known large-cap technology company.
- Advised client regarding response obligations, agency and public notice, and best practices to quickly and effectively identify, contain, and remedy a data breach involving PII and PHI.

- Counseled a Fortune 500 company on breach analysis and potential obligations related to encrypted laptops and mobile device theft.

Publications

May 7, 2026
U.S. and Allies Release “Careful Adoption” Guidance for Agentic AI

May 2026
California Consumer Privacy Act Enforcement in Review: Ensuring Privacy Programs Work in Practice
Co-Author, Pratt's Privacy & Cybersecurity Law Report Vol 12 No 4

April 20, 2026
Alabama Becomes Latest State to Enact Comprehensive Privacy Law

March 25, 2026
Not a Vibe: The Rise of the agentic AI hacker in cybersecurity
Author, The Daily Journal

March 6, 2026
New GSA Guidance on Protecting CUI in Contractor Systems, Plus a Look Ahead at Pending FAR Changes

February 25, 2026
Court Rules on How Client Use of AI for Legal Strategy is Not Protected

February 20, 2026
Escalated CCPA Enforcement Delivers Record $2.75M Settlement and Expanded Focus

February 17, 2026
The Hidden Risks of AI Notetakers: What Organizations Need to Evaluate Before Deployment

January 30, 2026
Utah Approves AI for Prescription Refill Process as States Test AI Governance Models

January 22, 2026
CCPA 2025 Enforcement in Review: Ensuring Privacy Programs Work in Practice
Co-Author, 2026 Technology Transactions & Data Privacy Report

January 22, 2026
Cross-Border Data Transfers: New Obligations, Stable (For the Moment) Frameworks and Harmonizing Compliance
Co-Author, 2026 Technology Transactions & Data Privacy Report

January 22, 2026
Seizing the Moment: Leveraging CMMC as an Opportunity to Enhance Cyber Risk Management
Co-Author, 2026 Technology Transactions & Data Privacy Report

January 22, 2026
Leveraging Cyber Insurance Trends to Strengthen Information Security Programs: Insights from M3 Insurance
Co-Author, 2026 Technology Transactions & Data Privacy Report

January 12, 2026
2026 Technology Transactions & Data Privacy Report

December 19, 2025
New Executive AI Order Mandates Minimally Burdensome Approach by States

November 25, 2025
White House Draft EO Targets State AI Laws as New EO Emphasizes Security

November 5, 2025
Steps to Address the New California Audit Rule That Seeks to Reset Reasonable Security
Quoted, Cybersecurity Law Report

October 10, 2025
$19M in Settlements Underscore Cybersecurity Risks for TPAs and Insurers

October 2, 2025
$1.35M CPPA Fine Signals New Focus on Privacy Disclosures

October 1, 2025
CMMC Is No Longer Optional: Final Rule Launches November 10

August 27, 2025
Bluesky's Mississippi Exit Highlights Cost of Age Verification
Quoted, Bloomberg Law

August 5, 2025
What You Need to Know About California's Finalized CCPA Amendments: Part Two

July 31, 2025
A Closer Look at America's AI Action Plan: What's Inside and What You Need to Know

July 29, 2025
America's AI Action Plan is a "National Security Imperative"

July 25, 2025
What You Need to Know About California's Finalized CCPA Amendments: Part One

July 9, 2025
California AG Reaches Record $1.55M CCPA Settlement with Healthline

July 7, 2025
A New Executive Order Signals Administration's Cybersecurity Priorities

June 2025
Tell Me Lies: The Legal Risks Associated with Misrepresenting Data Security and Privacy
Quoted, Pratt's Privacy & Cybersecurity Law Report Vol 11 No 5

May 27, 2025
1 Year In, Firms Grapple With Scope Of Wash. Health Data Law
Quoted, Law360

May 9, 2025
Two New AI Laws, Two Different Directions (For Now)

May 2025
Pixel-Tracking, the Video Privacy Protection Act and the Problem with Class Certification
Co-Author, The Computer & Internet Lawyer Vol 42 No 5

May-June 2025
Examining Cybersecurity Critical Infrastructure Regulations in the European Union and the United States
Co-Author, Global Regulatory Developments Journal Vol 2 No 3

May 2025
Rule of Lenity as a Shield Against Statutory Damages: Massachusetts Supreme Judicial Court Takes a Fresh Look at 1970s Era Wiretap Statutes
Co-Author, Intellectual Property & Technology Law Journal Vol 37 No 5

April 28, 2025
Cybersecurity litigation emerges as fresh threat
Quoted, Regulatory Compliance Watch

April 2025
When Startups Get Hacked, Investors Might Share the Pain
Quoted, WSJ Pro Venture Capital

March-April 2025
Securities and Exchange Commission Settles With Companies Over Charges Relating to Cybersecurity Disclosures
Co-Author, Pratt's Privacy & Cybersecurity Law Report Vol 11 No 3

March 28, 2025
Calif. Privacy Action Drives Home Need To Look Under Hood
Quoted, Law360

March 20, 2025
Valenzuela v. The Kroger Co. Chatbot Wiretapping Case Dismissed; Implications and Takeaways for Businesses

March 17, 2025
What Honda's CCPA Penalty Means for Your Privacy Compliance

March 14, 2025
Unpacking First Consumer Claim Under Wash. Health Data Act
Co-Author, Law360

February 28, 2025
Examining Cybersecurity Critical Infrastructure Regulations in the U.S. and EU

February 26, 2025
Tell Me Lies: The Legal Risks Associated with Misrepresenting Data Security and Privacy

February 26, 2025
Recent Developments Relating to the SEC’s Cybersecurity Disclosure Requirements

February 26, 2025
Threat Actor Trends and Practical Guidance —A Conversation Between Polsinelli and Coveware

February 25, 2025
Some States Step Up Early to Regulate AI Risk Management

February 24, 2025
Pixel-Tracking, the VPPA and the Problem with Class Certification

February 24, 2025
Developments in Online Tracking Litigation: Risks Hiding in Plain Sight on Your Site

February 24, 2025
Rule of Lenity as a Shield Against Statutory Damages: Massachusetts Supreme Judicial Court Takes a Fresh Look at 1970s Era Wiretap Statutes

February 6, 2025
2025 Technology Transactions & Data Privacy Report

February 5, 2025
Hackers, regulators, and lawsuits: The growing privacy and cybersecurity challenges
Co-Author, Daily Journal

February 2025
OCR Proposes Regulatory Facelift to the HIPAA Security Rule
Co-Author, Houston Medical Times

January 27, 2025
Energy Demand for AI Drives the Midwest's Focus on Resource Adequacy

January 7, 2025
Cybersecurity Compliance in 2025 – Know Your "Technology" Assets

January 6, 2025
OCR Proposes Regulatory Facelift to the HIPAA Security Rule: Addressing the Current Cybersecurity Environment with More Specificity and Additional Requirements

November 19, 2024
CPPA Board Adopts New Data Broker Regulations

November 4, 2024
CMMC 2.0: Department of Defense Publishes Final Rule to Establish its Cybersecurity Maturity Model Certification 2.0 Program

November 4, 2024
SEC Penalties Relating to Cybersecurity Disclosures

October 28, 2024
Cybersecurity for Critical Infrastructure Update – Incident Response Improves, Industry Standards Evolve

October 21, 2024
FTC's "Click-to-Cancel" Rule on Subscriptions and Renewals

September 26, 2024
CMMC 2.0: Department of Defense Releases New Proposed DFARS Rule to Implement its Cybersecurity Maturity Model Certification 2.0 Program

July 26, 2024
The EU AI Act is Here, and the Clock is Ticking!

June 10, 2024
Do I Really Have To? A Two-Part Framework for Determining if the EU AI Act Applies to You
Part 1: What's Your Role?

June 2024
It's Not Your Fault, But It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks
Author, The Banking Law Journal Vol 141 No 6

May 24, 2024
NIST Releases Risk 'Profile' for Generative AI

May 2024
Cybersecurity Insurance: Practical Steps Businesses Can Take to Become More Insurable
Co-Author, Pratt's Privacy & Cybersecurity Law Report Vol 10 No 4

April 19, 2024
Critical Infrastructure Cybersecurity – Evolving Incident Response Obligations, Integral to Effective Risk Management

April 15, 2024
The European Union Has Assigned Your AI Some Homework

May-June 2024
International Privacy Law Update: India and Saudi Arabia
Co-Author, The Global Regulatory Developments Journal Vol.1, No. 3

March 27, 2024
Legal Frontiers: Navigating the Rapid Evolution of Privacy Laws and Tech Governance
Featured, The State of Identity Podcast

February 29, 2024
The USPTO's AI Inventorship Guidance

February 6, 2024
AI is Fueling a Major Contract Dispute in the Music Industry: Why it Matters for Your Business

January 24, 2024
2024 Tech Transactions & Data Privacy Report

January 24, 2024
The SEC Raises the Stakes: New Cybersecurity Rules for Publicly Traded Companies Hit the Books in 2023

January 24, 2024
It's Not Your Fault, but It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks

January 24, 2024
Looking Ahead to the FTC's Implementation of the Data Breach Notification Rule for Nonbanking Financial Institutions

January 24, 2024
The VPPA Class Action – Is This Tide Still Coming In? Or Going Out?

January 24, 2024
Beyond the Blockchain: Legal Challenges and Opportunities in the Era of Digital Assets

January 24, 2024
Considerations for Artificial Intelligence and Employment Law

January 24, 2024
Cybersecurity Insurance: Practical Steps Your Business Can Take to Become More Insurable

January 17, 2024
California's Amended Data Broker Registration Law

December 22, 2023
FTC Settlement with Rite Aid Mandates AI System Assessment

December 12, 2023
The EU AI Act, The World's First Comprehensive AI Regulatory Scheme

November 29, 2023
Is the EU AI Act Faltering?

November 16, 2023
Unpacking the Executive Order on AI (for Data Privacy)

November 13, 2023
FTC Adopts Data Breach Notification Obligations for Non-Banking Financial Institutions

November 3, 2023
Unpacking the Executive Order on AI (for Cybersecurity)

October 25, 2023
Analyzing the CFPB's Personal Data Financial Rights Rule: What You Need to Know

August 8, 2023
Data Breach Rulings Stress Duty For Protecting Worker Data
Co-Author, Law360

August 7, 2023
Concerns and Considerations for Using Generative Artificial Intelligence as Part of Routine Business Operations

July 31, 2023
SEC Adopts Cybersecurity Incident and Risk Management Disclosure Rules

July 25, 2023
Generative AI's 'Industry Standards' for Cybersecurity and Data Privacy Could be Here Sooner Rather than Later

June 29, 2023
HHS OIG Releases Final Information Blocking Enforcement Rule Applicable to Non-Provider Actors

June 22, 2023
Leveraging "Public-Private Collaboration" for Critical Infrastructure Cybersecurity

May 16, 2023
Institutions Subject to FTC's Enacting Regulations to GLBA Must Implement Information Security Programs by June 9, 2023

May 10, 2023
Proposed Regulatory Oversight on the Emerging Use of Artificial Intelligence in Digital Health

May 4, 2023
Artificial Intelligence Has a NIST Framework for Cybersecurity Risk

April 26, 2023
Tennessee Information Privacy Act

March 23, 2023
Iowa Joins Privacy Law Trend, Putting More Heat On Congress
Quoted, Law360

March 7, 2023
FTC Targets Disclosure of Health Data for Web Tracking Again

March 2, 2023
It's Here – The New National Cybersecurity Strategy

February 21, 2023
National Credit Union Administration Finalizes 72-Hour Cyber Incident Reporting Rule

February 16, 2023
What's up with Illinois' BIPA

February 14, 2023
Cybersecurity To-Dos in 2023

February 13, 2023
For Data Misuse, Karma's an FTC Enforcement Action

February 13, 2023
"Fortnite" Creator Agrees to Pay a Record Penalty for Violating Children's Privacy Laws

February 7, 2023
"First-of-Its-Kind" FTC Breach Enforcement Case on Hot-Button Website Tracking Issue

February 2, 2023
Tech Transactions & Data Privacy 2023 Report

January 23, 2023
Blockchain Developers Urge Congress – Be Bold About Data Privacy and Security

January 23, 2023
The metaverse brings a new breed of threats to challenge privacy and security gatekeepers
Quoted, CSO

January 17, 2023
HHS-OCR Guidance for Online Tracking Technologies

January 12, 2023
Looting of Local Governments Leads to Cybersecurity Standards for the Water and Wastewater Sector

January 11, 2023
New York Department of Financial Services Announces a $1.9 Million Settlement With Insurance Agency For Violations of New York's Cybersecurity Regulation

January 2, 2023
Privacy Legislation And Regulation To Watch In 2023
Quoted, Law360

December 30, 2022
Top Privacy Developments of 2022: Year In Review
Quoted, Law360

December 21, 2022
For OT Cybersecurity, Extra Time is Running Out

December 15, 2022
Emerging Threats: Cyber Attacks and Side-Channel Evolution

December 2, 2022
National Security Focus on Cybersecurity for Critical Infrastructure Sharpens

October 31, 2022
EU Cyber Resilience Act

October 27, 2022
FTC Announces Decision "with a 100% chance of far-reaching" Impact for Data Breaches

October 21, 2022
Colorado Consumer Privacy Rules Add to Looming Business Mandates
Quoted, Bloomberg Law

October 21, 2022
Colo. Privacy Rules Spotlight Emerging Patchwork Of Laws
Quoted, Law360

October 11, 2022
Cybersecurity Awareness Means, at a Minimum, Doing the Basics (Again and Again)

August 30, 2022
CPRA and Employee Data – What Businesses Need to Know

August 2, 2022
National Credit Union Administration Issues New Proposed Rule Requiring 72-Hour Cyber Incident Reporting

June 23, 2022
Legal Matters: When The Feds Find Out! Lack Of Data Security Leads To Novel and Hefty Settlements
Co-Author, Houston Medical Times

June 20, 2022
Is it Legal? IP & Metaverse Law
Speaker, W3BTHR33 L0UNG3 at NFT NYC

March, 2019
Understanding the Scope and Impact of the California Consumer Privacy Act of 2018
Co-Author, HSTalks