WINSTON & STRAWN LLP

Privacy & Data Security

Winston takes a strategic approach to privacy and data security, integrating our extensive capabilities across practices to provide our clients with cutting-edge privacy and data security counseling, crisis management, security incident investigation and notification management, defense of data security class action litigation and regulatory inquiries, and international data protection. Our Global Privacy & Data Security Practice features a core team of privacy professionals and is bolstered by more than 40 attorneys from a variety of other disciplines firmwide. Our team combines compliance counselors, transactional lawyers, former government regulators and federal prosecutors, seasoned investigators, and experienced litigators. Few firms can rival our in-depth, sophisticated, and integrated experience in this area.

Our practice is anchored by lawyers who regularly advise our clients on their most complex and highly sensitive data issues, spanning from the highly regulated financial and health care industries to the specific and complex online and retail sector. While Winston's practice rivals the best in class, it is the manner in which Winston dispenses this advice that sets it apart from other firms. By leveraging a pragmatic business approach and deep knowledge of the laws at issue, our lawyers provide valuable strategic advice with a keen understanding of the practical composition of each client's business needs and issues. That experience and approach ensure that the team translates legal and regulatory expectations into specific business decisions and actions that put clients in the strongest position to mitigate risks and successfully address challenges.

Key Contacts

Alessandra Swanson

Sean G. Wieber

Areas of Focus

Privacy Counseling & Compliance Program Building

Our privacy and data security attorneys help our clients assess what personal information they collect, how they internally use and how they externally share it, in order to analyze and create practical strategies to address their obligations under the myriad of privacy laws in the United States, including the California Consumer Privacy Act (CCPA) and other similar state laws, the NY SHIELD Act, Children's Online Privacy Protection Act (COPPA) and the Federal Trade Commission Act, and sector-specific laws in industries including health care, education, and financial services. We do this in many ways, spanning from enterprise-wide privacy assessments to answering discrete questions that arise in daily business operations. In addition, many of our clients engage in marketing activities using email, automated telephone dialing systems, text message marketing or artificial or prerecorded calls. In the United States, the CAN-SPAM Act, TCPA, and related state laws impose strict requirements around how this marketing must be conducted. Our clients rely on us to assist them in building marketing programs that address and mitigate related risk without impacting customer experiences or business goals.

Regulated Personal Information

We leverage both the firm's counseling and litigation offerings for companies looking for practical and solution-oriented assistance navigating the compliance, regulatory enforcement, and class action risks presented by the emerging patchwork of complex (and often conflicting) privacy laws with *private rights of action*. We have deep experience with the privacy statutes that have become active breeding grounds for debilitating class action litigation: the federal Telephone Consumer Protection Act (TCPA); Illinois' Biometric Information Privacy Act (BIPA); and the California Consumer Privacy Act (CCPA), the California Invasion of Privacy Act (CIPA) and other similar state laws; the Florida Telephone Solicitation Act (FTSA); the Florida Security of Communications Act (FSCA); and the Video Privacy Protection Act (VPPA). These laws contain private rights of action and provide for uncapped statutory damages, often leading to "bet-the-business" class action damage calculations. Consequently, they are heavily used by the plaintiffs' bar. We help companies across all industries understand and address their obligations under these laws while proactively taking steps to mitigate potential regulatory and class action exposure.

Learn More

Privacy Investigations & Security Incident Response

We lead our clients through potentially catastrophic privacy events with a steady hand and work closely with stakeholders throughout our clients' organizations, such as chief executives, general counsels, and information technology teams, to forge a path forward. We have handled privacy investigations that include ransomware, phishing, cyber extortion, theft of personal information, loss or theft of devices containing sensitive information, rogue employee access to information, infiltration of unauthorized foreign nationals, unauthorized use or disclosure of customer data, and other cyber events. Winston works closely with its network of forensic, notification, and other providers to help clients navigate these complicated investigations, along with related remediation, restoration, and notification efforts.

Government Investigations

Winston is well-versed in government investigations and actions brought by federal, state, local, and international authorities related to security incidents, and has developed relationships with many of these government authorities. In particular, we have deep experience defending clients in front of state Attorneys General, the Department of Health and Human Services (HHS), Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), Congress, and the Consumer Financial Protection Bureau (CFPB). Our attorneys work closely together to ensure a consistent and intentional defense strategy across all areas of potential liability.

Similarly, security incidents are frequently followed by class action litigation filed in multiple jurisdictions, as a company may have employees or consumers who live in many different states at the time of the incident. Our privacy attorneys are particularly experienced with handling actions on multiple fronts at once. We approach all security incident response investigations with an eye towards potential litigation and regulatory inquiries to help ensure that we are considering all possible areas of risk and liability when helping our clients with critical decision-making early on in the process.

Data Security Incident Response Preparation

We work with our clients to ensure that if, and when, they experience a security incident, they are prepared and ready to respond in a highly strategic and efficient manner. We help our clients develop and revise security incident response plans and pressure test their response procedures. This includes evaluating response vendors and working with cyber carriers to ensure that these vendors are accessible and fully prepared in the event of an incident. Our team also frequently provide executive-level tabletop exercises to help raise awareness of issues that may arise in the course of an incident response and hammer out potential strategies to be utilized during an actual response.

Privacy & Data Security Litigation

Winston's privacy attorneys have robust experience defending clients in the rapidly developing field of privacy and data security litigation. We are well-versed in the best ways to litigate privacy statute cases to minimize the likelihood of a class being certified. If it is in the client's best interest to negotiate a settlement, we understand the best way to structure a deal, whether on a class-wide or individual basis. Our record of success obtaining favorable results for clients in privacy class actions is exceptional, and, due to our unique approach to working with opposing counsel and assessing early in the litigation process which matters are truly bet-the-company versus those that are ripe for dismissal, we are frequently able to resolve these matters in the early stages.

We have defeated privacy class actions in multiple jurisdictions for clients across a wide range of industries, including health care, insurance, financial services, lending, pharmaceutical and life sciences, cable/telecommunications, manufacturing, retail, consumer goods, and private equity. In the health care space, our litigators have worked closely with our counseling team to navigate the complications that HIPAA often creates in other privacy-related actions, such as lawsuits that are filed following security incidents.

Technology Outsourcing & Vendor Contracts

We work with clients to develop, negotiate, and execute major contracts, including business associate agreements, that implicate the use, sharing, disclosure, and safeguarding of personal information. As companies increasingly rely on vendors (including cloud platform and data transfer companies) to perform tasks like administering employee benefits, hosting consumer or patient data, and contacting customers on their behalf (e.g., via text message), they must transfer the sensitive personal information under their purview into the care of third-parties. We help clients develop strategies to address material risks in this area, including assigning responsibilities related to breach notification and indemnification, and negotiating contracts that give them maximum protection. We also assist in vetting potential vendors and negotiating licensing and service agreements, particularly with respect to the privacy and data security provisions in such contracts.

Emerging Technologies & Data Implications: AI, Blockchain, Facial Recognition, Internet of Things

Our team has extensive experience working with emerging technologies, including artificial intelligence (AI), blockchain, facial recognition, and Internet of Things (IoT). We have built data-privacy compliance programs applied to new technology. We provide strategic counseling to help companies best position themselves to comply with existing privacy and data-security laws and employ privacy by design in anticipation of future legal requirements. We take a comprehensive approach to these deeply complicated matters by working with our Intellectual Property lawyers, who bring technical know-how to help our clients protect the technology and data, and data-security experts, who help meet the challenge of applying best practices and reasonable security. The Privacy and IP teams also work closely together to counsel clients regarding building, protecting, and commercializing proprietary technology and data and the use of third-party or open-source AI technologies and data.

Privacy Policies, Consumer Privacy Choices & Cross-Contextual Advertising

We represent some of the world's largest and most well-known brands and retailers, and we help their business teams understand how they can best reach their intended customer base while still addressing the rapidly changing requirements for privacy policy disclosures, consumer privacy choices and disclosure of cookie use. In particular, we assist with the creation of consumer-facing privacy policies and website terms of use, and the development of back-end compliance infrastructure to address various levels of consumer notice, choice, and opt-outs that satisfy the requirements of global companies interacting with a myriad of laws. We also work with our clients to review websites and develop mobile applications to identify privacy-related issues like marketing consent and cookie consent language. In addition, we assist clients with respect to issues surrounding the analysis of large data sets and the de-identification, aggregation, and sharing of personal information.

Cross-Border Data Transfers & Worldwide Privacy Compliance

Our clients operate on a worldwide basis and constantly encounter issues related to complying with the various privacy and data-security laws in jurisdictions in which they operate, as well as navigating data localization and cross-border data issues. In the EU and UK, our attorneys work together to address GDPR and member-state implementing measures.

Data Rights & Data Utilization

Our privacy counselors work closely with our intellectual property team to help our clients assess how they wish to leverage their cache of data and what rights they need to secure in order to meaningfully do so. Our attorneys help our clients navigate complex regulatory and contractual obligations to understand what rights they have to the data and what they can do with it. On the other side of the equation, we also help clients create frameworks for allowing their vendors to use their data, including negotiating and revising the relevant agreements.

Information Governance & Records Retention

Our team regularly helps clients navigate the complexities of information governance and records retention. We address cutting-edge issues like the impact of encrypted messaging apps and ephemeral data, and the proliferation of personal information on corporate data retention and compliance. Our team starts with a comprehensive data landscape assessment (including mapping and risk identification) to develop customized policies for data access, retention, personal information handling, and litigation and regulatory discovery response. We advise on record retention schedules, navigate regulatory compliance hurdles, and implement strategies to manage information effectively at every stage. We go beyond retention to help clients devise strategies to protect sensitive data from unauthorized access and use. By staying at the forefront of regulatory and technological changes, we help clients build robust data governance frameworks tailored to their organization's and industry's unique nuances, while supporting their overall data management strategy.

Health Care & HIPAA Privacy & Security

Our team includes a former federal regulator from the U.S. Department of Health and Human Services – Office for Civil Rights, uniquely positioning us to provide practical advice about how to navigate HIPAA and HITECH compliance obligations and address related risks. Outside the United States, our capabilities extend to some of the most challenging jurisdictions, such as the UK and EU, where our locally qualified data lawyers advise multinational health care services providers on the collection, storage, process, and transfer of health care data and assist in designing and implementing local data strategies, including telemedicine.

We emphasize not only meeting regulatory requirements, but also creating compliance infrastructure that can be effectively and successfully implemented in our clients' business environments. Our goal is to create a compliance program where employees understand how to appropriately secure and maintain the privacy of patient information without these obligations interfering with the critical care that they provide. We also assist in reviewing business associate and other vendor agreements, advising on the use of patient information for marketing and advertising purposes, and crafting incident response and breach-notification plans.

Financial Privacy

We represent more clients in the financial services industry than in any other sector. Our extensive financial industry knowledge includes a long history of representing companies before domestic and international regulatory agencies, including the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, the Financial Crimes Enforcement Network and the Office of Foreign Assets Control, among others. Our attorneys also represent financial institutions before courts and legislatures, and assist clients navigate through arbitration panels and international tribunals. Our experience includes advising and assisting financial institutions on risk management and regulatory compliance, including within the FinTech and payments space where we support both banks and FinTech companies throughout the entire FinTech product lifecycle—from proof of concept through maturity. This includes advising financial institutions on their privacy and data security obligations, including Gramm-Leach-Bliley/Regulation P and Fair Credit Reporting Act compliance.

Employee Privacy Investigations

When investigating a privacy incident or security breach in the workplace, complicated questions often arise when it appears that an employee may be at the center of the issue. Our privacy team works closely with Winston's labor and employment attorneys to ensure that all relevant laws are considered when investigating, interviewing and sanctioning employees in connection with how their actions may have impacted an employer's obligations under privacy and security laws.

“ Sean Wieber and his team are excellent. They know the law inside and out and they take the time to understand your business needs. They provide actionable guidance and enable the client to make informed decisions in oftentimes untenable positions. ”

Legal 500 US 2024

Related Capabilities

Advertising Litigation | Class Actions & Group Litigation | Commercial Litigation & Disputes | Compliance Programs | eDiscovery & Information Governance | Employee Benefits & Executive Compensation | Intellectual Property | International Trade | Labor & Employment | Mergers & Acquisitions | Privacy: Regulated Personal Information (RPI) | Trade Secrets, Non Competes & Restrictive Covenants | White Collar & Government Investigations | Automotive & Mobility | Financial Services | Health Care | Life Sciences | Retail & Luxury | Technology, Media & Telecommunications | Europe | Latin America & Caribbean | North America

Recent Experience

GenNx360’s Majority Investment in Whitsons Culinary Group

Resources

Class Action Insider

Related Insights & News

RECOGNITIONS

Winston & Strawn Recognized in *The Legal 500 U.S.* 2025

JUNE 12, 2025

RECOGNITIONS

Winston Partners Featured on the 2025 *Lawdragon* 500 Leading Global Cyber Lawyers 2025

MAY 7, 2025

IN THE MEDIA

Sean Wieber Discusses Growth of Privacy Class Actions Involving Biometrics and Genetics with *Law.com*

MARCH 12, 2025

NEWS

Trump Administration Confirmation Hearings: Secretary of Homeland Security Kristi Noem

FEBRUARY 19, 2025

WEBINAR

Privacy Problems Webinar Series

FEBRUARY 18, 2025

WEBINAR

AI-Enabled Drug Development: Best Practices for Mitigating Risks and Ensuring Good Governance

JANUARY 31, 2025

SEMINAR/CLE

Winston Hosts 2025 Financial Services Symposium in Charlotte

JANUARY 30, 2025

WEBINAR

Public Readiness – Are Your Cybersecurity Controls Ready?

JANUARY 22, 2025

IN THE MEDIA

Sara Susnjar Discusses "Dark Patterns" in Noyb Privacy Complaint Against BeReal with *Lexology*

DECEMBER 16, 2024

WEBINAR

Decoding AI Law - Fall 2024 Edition

NOVEMBER 5, 2024

BLOG

Key Compliance Strategies: NY Department of Financial Services' Guidance on AI and Cybersecurity Threats

OCTOBER 22, 2024

RECOGNITIONS

Three Winston Attorneys Named as 2024 Law360 MVPs

OCTOBER 22, 2024