pillsbury

Cybersecurity, Data Protection & Privacy

Recognized by *The Legal 500* as one of the world's foremost practices, Pillsbury offers unparalleled experience and knowledge in connection with critical cybersecurity, data protection & privacy law issues.

Proper management of information—its security, use and misuse—is now a top priority for businesses worldwide and the need to proactively address these issues has never been greater. Pillsbury's cross-disciplinary, multi-national Cybersecurity, Data Protection & Privacy solutions team has the unique skillset necessary to understand and properly respond to the broad spectrum of privacy and security considerations companies face today.

The group is comprised of regulatory authorities, litigators, transactional lawyers, intellectual property counsel, seasoned government contracts practitioners and legislative strategists, all of whom work closely with clients to monitor the changing data and cyber landscapes. After a comprehensive analysis of potential risks, we develop, execute and maintain tailored solutions to mitigate perceived threats and take advantage of underlying opportunities.

Pillsbury has advised businesses ranging from privately held startup companies to publicly traded global conglomerates on all manner of data privacy issues, with particularly deep knowledge in connection with the energy, communications, financial services, government/defense contracts, health care and technology sectors, as well as with critical infrastructure generally. Our uncommon insight, combined with an expansive network of government and regulatory connections at the highest levels, affords clients unparalleled resources for navigating and tackling their data-related challenges.

Cybersecurity & Data Breach Response

From external threats such as Distributed Denial of Service (DDoS) and ransomware attacks to insider threats, Pillsbury lawyers work with organizations of all sizes to develop and implement comprehensive cybersecurity programs, providing guidance on regulatory compliance issues, the creation and application of cyber policies, organizational training programs and incident response plans. We also conduct extensive cyber assessments to stress-test those policies, using the results to shore up technical and legal weaknesses.

On Capitol Hill, the team leverages its unrivalled access to U.S. policymakers to shape legislative proposals like the Cybersecurity Framework called for in President Obama's Executive Order. Our lawyers have also prepared more than 100 Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act applications, allowing clients to limit or eliminate liability in the event of a cyber attack. *Financial Times* recently recognized the firm as a legal innovator as a result.

And if a breach does occur, Pillsbury can help companies respond to the myriad legal and regulatory issues that emerge following a cyber-event. The Cybersecurity, Data Protection & Privacy team has investigated and resolved some of the largest data breaches on record, and maintains strong relationships with cybercrime units worldwide such as Interpol and Europol. The firm also offers unique collaborations with leading technical consultants, such as the joint FireEye/Pillsbury cyber M&A due diligence package.

Our lawyers have first-hand experience defending clients in class action lawsuits arising from cyber attacks and have successfully steered clients through related regulatory, governmental and criminal investigations. In addition, Pillsbury's market leading Insurance Advisory & Recovery practice help clients ensure insurance policies adequately cover cyber risk before a loss occurs and can successfully enforce coverage rights should litigation become necessary.

International Data Transfer Compliance, BCRs & Privacy Shield

While business practices demand fast and easy transmission of information across borders—and the cloud—those very activities can very easily run afoul of the laws, regulations and restrictions governing data transfers, whether relating to consumer, customer, employee, vendor or other data. Pillsbury has market-leading proficiency in the area of data transfers, being one of only a handful of law firms to have successfully secured Binding Corporate Rules for clients. Members of the Cybersecurity, Data Protection & Privacy solutions team maintain regular dialog with policymakers as to the implications and realities of the replacement of Safe Harbor, the EU/U.S. Privacy Shield scheme. We also have assisted numerous clients in the negotiation of cross-border data transfer agreements and the use of Model Contract Clauses, amongst other transfer and international data flow issues.

Global Data Protection and Risk Reduction

Pillsbury data protection lawyers have deep international experience that dates back to the very earliest days of the digital economy, with direct involvement in the development of groundbreaking federal and state legislation as well as the first EU Data Protection Directive in 1995. We regularly help clients ensure adherence to laws like the Red Flags Rule, Health Insurance Portability and Accountability Act (HIPAA) and Children's Online Privacy Protection Act (COPPA) in the United States; and the Data Protection Directive and The General Data Protection Regulation (GDPR) in Europe. We also understand and can help companies make the most of services such as online and mobile targeted advertising and consumer profiling, location-based technologies, and "club card" data capture programs. And, while making sure our clients are meeting existing regulations, we also proactively monitor and prepare for new ones.

Privacy, Digital Marketing and Consumer Protection

The safekeeping of customer and employee personally identifiable information (PII) is fundamental to the well-being of corporations today but privacy laws around the world pose numerous and difficult challenges. Our team works with companies across the globe to address privacy requirements, needs and issues in a way that balances compliance with flexibility.

We regularly provide assessments of our clients' privacy, information collection and sharing practices, implement or revise privacy policies and disclosures, provide privacy-related training, and prepare appropriate contract provisions, and have particular experience in relation to the U.S. and European consumer-related regulations pertaining to digital advertising, marketing, social media, customer profiling, targeting and mobile device data use. The team also advises clients on the risks they may face from particular information collection and sharing practices, as well as issues related to joint ventures and alliances.

We have broad experience in privacy-related litigation matters too, including roles as lead counsel in numerous class action suits relating to HIPPA, the Telephone Consumer Protection Act (TCPA), the Fair and Accurate Credit Transactions Act (FACTA) and other major privacy laws, and also provide legal advice in connection with information disclosure and discovery orders in litigation proceedings and governmental investigations.

Cyber Compliance in Government Contracts

Cybersecurity in the U.S. federal marketplace is governed by an array of statutes and regulations that continue to evolve. The requirements imposed by these laws are implemented in contract clauses in federal prime contracts, and are passed down to subcontractors. In addition, the Federal Risk and Authorization Management Program (FedRAMP) requires that federal contractors providing cloud computing services to the U.S. government demonstrate compliance with cybersecurity requirements at the appropriate risk level. FedRAMP has established processes for achieving a FedRAMP authorization and an agency authorization that is required to provide cloud services to federal agencies. Applicable regulations require mandatory reporting of cyber incidents and breaches, and federal agencies typically investigate any breach that exposes federal

information. Our specialized cybersecurity team within the government contracts and disputes group counsels clients on compliance with federal cybersecurity requirements, supports prime contractors and subcontractors in developing appropriate cyber intrusion response protocols, in promptly investigating cyber incidents and breaches, and assists contractors in navigating federal investigations.

Representative Experience

- Successfully resolved a major international data breach involving some of the world's highest profile web brands, including the pursuit of perpetrator across multiple countries to recover stolen data
- Advising a leading global technology and cyber security company on international data transfers issues and their Binding Corporate Rules application
- Advising one of the world's leading digital advertising and media businesses on a 'Privacy By Design' audit and the development of new policy to limit enforcement risks under the GDPR
- Handled high-profile data security breaches for large financial institutions, healthcare entities, a major airline and a national hotel operator, among other clients.
- Assisted FireEye in obtaining the first ever SAFETY Act Certification for a cybersecurity product.
- Counseled clients facing hacker attacks, data theft, unauthorized data disclosure by vendors and other data-oriented threats and crises.
- Handled employee data privacy matters for pharmaceutical companies in more than 40 countries.
- Represented a US-headquartered, international business in securing EU approval of its Binding Corporate Rules (BCRs) – the gold star standard when transferring data internationally in light of new EU regulatory changes.
- Represented one of the world's leading professional services organizations in structuring and negotiating the terms of their cyber insurance programs.
- Represented a global credit card and payment services company in structuring and negotiating the terms of their cyber insurance programs.
- Represented an internationally renowned network of hospitals and clinics in structuring and negotiating the terms of their cyber insurance programs.
- Represented a national health plan management company in structuring and negotiating the terms of their cyber insurance programs.
- Represented a biopharmaceutical company in structuring and negotiating the terms of their cyber insurance programs.
- Represented a leading medical claims processing company in structuring and negotiating the terms of their cyber insurance programs.
- Working with HR directors in 12 countries, represented a health care company in harmonizing privacy policies across business units in the wake of a major acquisition.
- Helped a major global electronics firm with a privacy audit and compliance issues related to emerging privacy concerns around the "Internet of Things."
- Advised a national retailer in connection with a DDoS cyberattack, including data breach issues arising from the attack and securing insurance coverage for costs stemming from the incident.
- Represented a global executive search firm in connection with issues relating to cross-border flows of candidate information.
- Advised a globally prominent game maker on privacy and data security issues related to virtual goods and virtual currencies.
- Representing Sony Pictures on insurance issues related to the November 2014 cyberattack on its network and IT infrastructure.
- Represented Sony on insurance claims arising out of attacks on its online gaming networks in 2011.

Practice Area Highlights

- Genuine thought leaders, including authors of leading books (*Regulation of the Internet and E-Business: The Practical Guide*) and regular broadcast, print and online media commentators.
- Deep experience stemming from the earliest days of web commerce and commercialized data use, from advising GE on their e-enablement project to representing GM on the first websites selling cars.
- Fully immersed in the cybersecurity, data protection and privacy law of today, from social media hacks, to e-payments to customer tracking and the Internet of Things.

Pillsbury Winthrop Shaw Pittman LLP
FS_v.02.27.18