Armstrong Teasdale

DATA INNOVATION, SECURITY AND PRIVACY

Data, often a company's most valuable asset, can also be one of its greatest liabilities if it is not properly protected and used. Developing and implementing appropriate contracts, policies and procedures is critical. In addition, the explosion of data innovation surrounding the development of distributed ledger technologies and related products such as blockchain (Web3) presents opportunities and risks for cutting-edge companies seeking to capitalize on these developments.

Armstrong Teasdale's Data Innovation, Security and Privacy team is highly experienced in guiding organizations through the thicket of federal, state and international rules governing personal information. We routinely counsel clients in connection with development and implementation of, and updates to, information privacy and security programs. Our team is also adept at handling data breaches and related incidents. When a client is the victim of a data breach – whether by a malicious hacker, a departing employee, a competitor or another third party – we provide responsive guidance to stop the dissemination of the data, recover it, provide notice to affected parties, and mitigate risks.

DATA INNOVATION

Web3 is a broad term encompassing blockchain technologies, cryptocurrencies and digital assets, and novel business models, among other things. While this nascent field is rapidly evolving, Armstrong Teasdale lawyers have already developed a deep understanding of the technologies involved and the relevant laws, regulations and industry standards. We also monitor and engage with government agencies establishing new, comprehensive safety and security guidelines. Working collaboratively with members of the Securities, Financial Services and Banking, Fintech and other relevant practices, the Data Innovation, Security and Privacy team counsels clients ranging from startups to Fortune 500 firms on innovative technologies and uses for data, and related concepts, including:

- Nonfungible Tokens (NFTs), digital assets stored on blockchain technology, created by computer code and often bought with cryptocurrency. The computer code underlying an NFT includes "smart contracts," is unique, and is noninterchangeable. Their investment potential is complicated by questions of ownership in agreements and the dramatic rise in illegal activity surrounding them, which has led to the increased likelihood of government regulations and legal oversight on the horizon.
- Decentralized Finance (DeFi), which encompasses a wide variety of applications (including blockchain technology) designed to eliminate intermediaries (such as banks). Their hallmarks of efficiency and responsiveness give rise to regulatory and compliance complications, as well as heightened transactional risks that have eroded consumer trust.
- Decentralized Autonomous Organizations (DAOs), entities governed by a community organized around a specific set of rules enforced on a blockchain via smart contracts. As prominent losses from cybersecurity incidents run into the hundreds of millions of dollars, calls for regulation have increased as consumers bear the brunt of these losses.
- Cryptocurrency, which has experienced a rapid—and volatile—evolution. Lacking a centralized regulatory authority, they present risks both for security as well as compliance. And like DeFi, their "borderless" nature makes it difficult to establish jurisdiction.

INFORMATION SECURITY AND PRIVACY

Armstrong Teasdale

Our cross-disciplinary team of lawyers has in-depth experience with matters involving both U.S. and international privacy and data security laws. Given the increasing opportunities for savvy data use, the commensurate risk to business and the steady influx of regulation, it's critical to understand your company's vulnerabilities and mitigate risk.

Our robust team includes a Certified Ethical Hacker (C|EH) and Certified Information Privacy Professionals (CIPP/US and CIPP/E). Members of the practice routinely advise clients ranging from internet startups to Fortune 100 companies in a variety of industries, including financial services, insurance, communications, health care, retail, legal, technology and energy and utilities. Our lawyers are experienced in handling multijurisdictional events, as well as working with the Office of Civil Rights and other state and federal regulators. The issues we routinely address for clients fall into three key categories: preparedness, response and litigation.

We counsel clients on a wide variety of matters, including:

- Compliance with the California Consumer Privacy Act (CCPA), the upcoming California Privacy Rights Act (CPRA), the Utah Consumer Privacy Act (UCPA), and the Colorado Privacy Act (CPA), as well as the emerging patchwork of other state-level privacy laws
- Compliance with federal privacy laws and regulations, such as the HIPAA privacy and security rules, the GLBA safeguards rule, the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), the FTC Act and the Telephone Consumer Protection Act (TCPA)
- Regulatory compliance and investigations, including with the Department of Health and Human Services and the Office of Civil Rights
- Breach response, including notification and state and federal compliance
- Litigation, including class action lawsuits
- Immediate injunctive relief to stop the proliferation of data
- Enhancing privacy and security programs and elevating privacy and security issues to boards and top-level management
- General Data Protection Regulation (GDPR) compliance, data protection impact assessments and cross-border data transfers
- Commercial contracts involving data use and data protection issues
- Security programs and policies, including Written Information Security Programs (WISPs) and Acceptable Technology Use Policies
- Confidential information and trade secret protection
- Computer tampering violations
- Data recovery
- Document retention and best practices
- Employee training programs
- Loss of customer, client or employee data
- Network security gap analysis
- Noncompete, nonsolicitation, nondisclosure and confidentiality agreements
- Privacy and security audits

- Privacy by design principles
- Enterprise risk management
- Software license audits

EXPERIENCE

Conducted Privacy Assessment and Advanced Compliance Efforts for Animal Health and Nutrition Clients

Advised multiple clients in the animal health and nutrition space in developing and updating privacy programs to address compliance with the ever-changing regulatory landscape – from state-specific to international cross-border requirements. Conducted reviews and assessments, and drafted and implemented policies and procedures tailored to industry-specific and client needs.

Advised Nonprofit Founder on Congressional Testimony

Advised the founder of a public interest-focused privacy nonprofit on the preparation of testimony that was presented before the House Energy and Commerce Committee regarding protections for children in existing privacy laws and the American Data Privacy and Protection Act, a federal omnibus privacy bill.

Counsel to Expert Witness in Multistate Data Breach Settlement

Advised an expert witness for U.K.-based insurance companies in a case brought in the U.K. courts by the insurers in connection with a multistate data breach enforcement action where the personal information of millions of consumers was exposed. Counsel was provided in regard to U.S. law concerning Section 5 of the Federal Trade Commission Act, the data breach and data security statutes of the 40 states whose attorneys general filed complaints, and the potential insurability of penalties in each of the states. The settlement reached in the case was due in large part to the insurability analysis, which was key during negotiations.

Created Governance Documents for National Institute of Corrections

Drafted governance documents and intergovernmental agreements relating to criminal justice information sharing among local justice and community health stakeholders adopted by the National Institute of Corrections in its revision of the *Guidelines for Developing a Criminal Justice Coordinating Committee.*

Advised Menswear Retailer in SMS Program Launch, Compliance

Advised a major American menswear retailer in launch a transactional SMS program allowing them to communicate via text message with customers who have opted-in. Armstrong Teasdale navigated a strict regulatory environment by identifying regulatory requirements for SMS programs, evaluating internal business processes to streamline compliance, and drafting the requisite consent language. The program required significant cross-collaboration to meet the expected deadlines.

Launch of New Social Media Network

Supervised and provided legal guidance for the successful launch of a new social media network that focuses on giveaways and user/company promotion and advertising.

Obtained Early Dismissal for Health Care Provider on Multiple Claims

On behalf of health care provider, obtained early dismissal of fraud, conspiracy, and Computer Fraud and Abuse Act claims brought by former IT vendor, and negotiated favorable settlement of breach of contract claim.

Information Sharing Agreement for Criminal Justice Council

Coordinated with a multi-agency Criminal Justice Coordinating Council to draft an information-sharing agreement. Regulatory limitations on sharing certain types of protected data were balanced with the agencies' need to facilitate a free flow of information in the interest of public health and safety.

Secured Motion to Dismiss for Hospital in Protected Health Information, Termination Case

Prevailed on a contested motion to dismiss in favor of hospital client. Plaintiff alleged employment termination in part, due to our client's allegedly inappropriate and unauthorized disclosure of protected health information. Plaintiff asserted a claim alleging breach of fiduciary duty of confidentiality, seeking both economic losses and punitive damages. Relying in part on HIPAA regulations, we filed a motion to dismiss and a motion to strike the punitive damages claims, and after oral argument, the judge granted the motion.

Dismissals Lead to Favorable Settlement

Obtained the dismissal with prejudice of multiple claims brought by one financial institution against another arising out of a data breach led by fraudsters, facilitating a favorable settlement of the sole remaining claim.

GDPR Compliance Program Implementation for Aviation Service Company

Facilitate the design, build-out and implementation of the client's GDPR compliance program.

Data Privacy, Antitrust and HIPAA Breach

Investigated and resolved matters involving violations of the Health Insurance Portability and Accountability Act (HIPAA), protected health information data breaches, and Office for Civil Rights (OCR) reporting and investigations, including the inadvertent misdirection of more than 1,500 patients' protected health information and the intentional disclosure by an employee of protected health information.

Data Privacy Compliance for Multinational Manufacturer

Represented multinational manufacturer in undertaking compliance with GDPR, including update of privacy policies, negotiation of data privacy addenda, and development of an international data transfer mechanism.

GDPR Compliance Program for University

Helped facilitate the design and implementation of all facets of international university's General Data Protection Regulation (GDPR) program.

Dismissal of $1 Billion Class Action Claim

Successfully defended the operator of a commercial website against a putative class action involving alleged interception of an online customer's personal information, including credit card information, and disclosure of that information to third parties without the customer's consent. The plaintiff argued that this information, which was stored in a browser file before being sent to the website, was not yet a communication to website and that the interception and transmission of that information via JavaScript commands was illegal under the Wiretap Act. The court agreed with the website operator's arguments and dismissed the action. Plaintiff's counsel was seeking over $1 billion in damages, making this a significant victory.