



# Andrew Baer

## Chair, Technology, Privacy & Data Security

### Philadelphia

[abaer@cozen.com](mailto:abaer@cozen.com) | (215) 665-2185

Andrew Baer is the founder and chair of Cozen O'Connor's Technology, Privacy & Data Security practice. He was among the first attorneys in the country to launch a dedicated technology practice and has led development of a unique multidisciplinary approach to tech, privacy, IP, cyber, and internet law.

Today, Andrew's practice focuses on advising sophisticated clients on cutting-edge technology transactions and privacy/cybersecurity compliance. He represents diverse clients ranging from startups to Fortune 500 giants, including financial institutions, SaaS/laaS/PaaS companies, digital interactive agencies, adtech companies, online ad networks, data brokers, mobile app developers, life sciences companies, media monitors, and e-commerce companies. Andrew also represents AI developers and crypto companies.

Andrew regularly leads mission-critical deals — from both the buy-side and sell-side — that implicate issues in cloud computing, software, data privacy, security compliance, copyrights and trademarks, digital advertising systems and platforms, and interactive marketing compliance. He is deeply knowledgeable about state, federal, and international legal regimes relating to data privacy, cybersecurity, and artificial intelligence.

Since joining Cozen O'Connor, Andy has built a technology practice leading the way on team training, client service, and alternative fee structures. Before coming to Cozen O'Connor, Andrew served for 10 years as managing partner of Baer Crossey McDemus, a technology and venture capital boutique that he co-founded. Prior to that, he was lead tech/IP/privacy counsel at Advanta Corp., chief legal officer to a life sciences technology company, and an attorney in the intellectual property and information technology practice groups of WolfBlock.

Andrew is a frequent speaker, author, podcaster, and blogger. He is a lecturer at The Wharton School, a faculty member with the Pennsylvania Bar Institute and other continuing legal education groups, and a national contributor to online and print legal publications on technology and cybersecurity law. In 2010, Andrew co-authored the "Corporate Security and Privacy Duties, Policies and Forms" chapter of West's Data Security and Privacy Law treatise.

Andrew earned his bachelor's degree from Dartmouth College and his law degree from University of Chicago Law School.

### Experience

Represented an AI developer in structuring and negotiating its customer contracts and mitigating potential risks associated with algorithmic bias.

Counseled companies leveraging generative AI on copyright fair use and web scraping issues.

Represented a national financial institution in outsourcing and technology acquisition and development transactions, including negotiating deals for enterprise cloud services with Salesforce, Microsoft, Oracle, First Data, and other leading vendors.

### Practice Areas

- Technology, Privacy & Data Security
- Privacy Litigation – Emerging Trends
- IP Transactions & Licensing
- Artificial Intelligence

### Industry Sectors

- Cryptocurrency and Blockchain Technology
- Retail
- Software

### Education

- University of Chicago Law School, J.D., 1996
- Dartmouth College, B.A., 1993

### Bar Admissions

- New York
- New Jersey
- Pennsylvania

### Awards & Honors

- 2022 Law Firm Innovators, The Legal Intelligencer
- Best of the Bar, Philadelphia Business Journal, 2022

### Andrew Baer

[abaer@cozen.com](mailto:abaer@cozen.com)

P: (215) 665-2185 | F: (215) 372-2400

©2024 Cozen O'Connor. All rights reserved.



Represented an international financial services company in developing contracting strategies and updating its vendor contract templates to address federal and New York vendor management and cybersecurity regulatory guidelines and industry best practices.

Counseled data brokers, predictive analytics companies, and numerous other small and medium-sized companies on GDPR and CCPA compliance, including preparing and negotiating data processing and service provider agreements with vendors and customers; updating privacy disclosures; consent mechanisms and procedures for handling data subject requests; lawful basis for processing analysis; and developing anonymization, pseudonymization, and data minimization strategies to reduce compliance costs.

Represented a well-known international e-commerce company in connection with technology procurement transactions, online marketing transactions, and privacy compliance.

Developed and negotiated all customer and partner contracts, as well as contracting playbooks, for data brokers, adtech companies, retargeting companies, and lead generation and aggregator companies.

Developed contracting templates and playbooks, and negotiated deals with many of the world's largest pharmaceutical companies, on behalf of a leading SaaS vendor in the life sciences space.

Counseled emerging growth and marketing clients on maximizing trademark strength and protection in branding.

Successfully prosecuted numerous challenging and disputed trademark applications to registration in the U.S. Trademark Office.

Counseled adtech companies, advertising networks, and lead generation/aggregator companies in matters relating to FTC privacy, behavioral tracking, and online advertising compliance.

Represented a respected news organization in negotiations for development of its news and information website, and creation of its internal and external social media policies.

Developed a fair use compliance strategy and negotiated all customer contracts on behalf of a broadcast media monitoring and intelligence company.

Represented a nationally known charity in technology, data security, and HIPAA privacy compliance matters related to the launch of a new website.

Represented a major corporate client in all aspects of responding to and remediating the effects of an internationally mounted cyberattack, including retaining and working with forensic investigators, communicating with state and federal authorities, counseling on notification requirements and preparing notices, and negotiating vendor contracts for implementing remedial services, systems, and applications.

Represented Kinetiq, Inc., a cutting-edge TV intelligence platform, in a significant data integration agreement with a UK-based digital intelligence services suite. Our team was involved in the early discussions between the companies, drafted the initial letter of intent, and led the subsequent negotiations. In the course of those negotiations, we navigated a robust set of restrictions, developed specific remedies should those limits be breached, and won key concessions around contract jurisdiction and enforcement.

Negotiated a model combined software development and cloud service agreement on behalf of an international medical diagnostics company with a digital services provider. In negotiating the

**Andrew Baer**

abaer@cozen.com

P: (215) 665-2185 | F: (215) 372-2400

©2024 Cozen O'Connor. All rights reserved.



agreement, our team first resolved multijurisdictional privacy and intellectual property questions, then addressed the interconnected issues of service level and liability, and ultimately developed a unique agreement that combines requirements for the vendor to develop and operate specialized back-up systems as well as a liability structure that incentivizes quick resolution of problems and establishes compensation metrics for a sustained outage.

Represented an international e-commerce company in a technology procurement transaction with a SaaS vendor hired to modernize and manage the client's digital returns process. Our team analyzed how the new system would materially impact the client's operations and obligations, focusing heavily on the interconnected issues of privacy and security, designing parameters around everything from text message language to opt-out protocols and ensuring compliance with all international, federal, and state data protection and privacy laws.

Represented a community care organization that had entrusted all of its critical systems, including email, to a cloud service provider which suffered a ransomware attack and did not provide adequate notice that patient and employee information had been compromised for thousands of individuals. The service provider was not cooperative in providing the information the client needed in order to comply with its data breach notice obligations under HIPAA and state law, so the client filed suit to force cooperation and recover other damages. We negotiated agreements with the previous and a new cloud services provider to migrate the client's applications and data.