



BakerHostetler's award-winning **Digital Assets and Data Management (DADM) Practice Group**, selected for Vault's "Guide to Legal Practice Areas" for the eighth consecutive year, serves Fortune 500 clients as well as health systems, universities, global retailers, small and midsize businesses, and state and municipal entities. Our eight integrated teams address risks, disputes, compliance and opportunities throughout the life cycle of data, technology, advertising and innovation, including brand strategies and monetization. Our annual "Data Security Incident Response Report" is an industry-leading resource for cybersecurity trends, breach response and best practices for data protection.



A highly respected trailblazer in the field of data security and privacy, **Ted Kobus** leads the DADM Practice Group of more than 100 attorneys and technologists nationwide. Representative clients include AT&T, Dell Technologies, Marriott, Princeton University and Roblox. Under his leadership, the DADM Practice Group has earned recognition from industry heavyweights such as BTI, *Law360*, ALM and Vault. Ted also provides pertinent insights when contacted by major media outlets looking for comments on the latest news and trends in privacy and data security.

For more information, visit www.bakerlaw.com/DigitalAssetsDataManagement.

Baker & Hostetler LLP

Jiwon (Jamie) Kim, Associate, and Jennifer Mitchell, Partner— Privacy Governance and Technology Transactions

Jiwon (Jamie) Kim assists clients in navigating the legal and technical landscape to ensure compliance with developing privacy laws. Additionally, Jamie leverages her background in neuroscience to integrate legal requirements in the emerging areas of machine learning and generative AI with technical capabilities and business operations.

As BakerHostetler's Los Angeles, San Francisco, and Orange County digital assets and data management leader and the co-leader of the media and telecommunications industry team, Jennifer Mitchell leverages more than 15 years of legal, compliance, and operational experience as she helps clients navigate the complex landscape of global and strategic privacy matters. Having most recently served in executive privacy leadership roles for two global Fortune 100 companies, Jennifer provides practical business solutions for maintaining compliance with evolving privacy laws.

Describe your practice area and what it entails.

We are members of the privacy governance and technology transactions team within the digital asset and data management practice group at BakerHostetler, and we focus our practice on helping clients comply with international, federal, and state privacy laws. Our work often starts with analyzing what privacy laws are in scope for a client in this increasingly complex privacy landscape. From there, we provide guidance on all components of achieving privacy requirements under the applicable laws by, for example, drafting privacy policies, designing consent strategies, advising on technical website and ad tech implementation, and negotiating data processing addenda with vendors. We are also supporting an increasing number of privacy regulatory investigations at the federal and state levels.

What types of clients do you represent?

Our team represents a wide range of clients, including multi-national retailers, hospitality services, medical device and life sciences, financial services, tech conglomerates, hospitals, publishers, school districts, universities, media and entertainment companies, and research organizations.

What types of cases/deals do you work on?

We counsel clients on compliance with international, federal, and state privacy laws, including the General Data Protection Regulation, Health Insurance Portability and Accountability

Act, Family Educational Rights and Privacy Act, and California Consumer Privacy Act. We also specialize in scoping the applicability of enacted and pending U.S. state privacy laws, as well as state-level consumer health data and biometric laws. We help create and implement privacy programs, including drafting and implementing consumer-facing and employee privacy notices and policies, conducting privacy risk assessments, and advising on privacy-by-design for product launches and new data initiatives. Additionally, we negotiate vendor contracts to ensure legal and regulatory compliance, which includes assisting data importers and exporters with international data transfer restrictions and data localization requirements. We also provide privacy legal strategy for global acquisitions and divestitures, performing due diligence to identify privacy risks and develop post-close strategies.

How did you choose this practice area?

Jamie: I began my legal career thinking that I would be an intellectual property litigator because I was drawn to the intersection of science and law. I realized that privacy work offered a unique opportunity to address complex issues at the intersection of technology, law, and human behavior. Transitioning to privacy governance allowed me to leverage the skills developed during my years as a litigator while focusing on proactive strategies to ensure compliance with privacy regulations in a practical fashion for businesses.

Jen: My interest in privacy began when I was a white collar and government investigations lawyer, which is where my legal practice started. I had always enjoyed the fact-finding, strategy, and creative problem-solving components of my white collar practice, and these skills are also key to our privacy practice. I first pivoted from a white collar to a full-time privacy role at an academic medical center and never looked back. I love how dynamic our practice area is and the variety that this unique discipline brings to our daily work.

What is a “typical” day like and/or what are some common tasks you perform?

Jamie: My tasks are focused on helping clients navigate privacy laws and maintain robust data protection practices, such as drafting privacy policies, reviewing data ingestion points on websites and apps, and analyzing cookies in relation to a business' opt-out posture. I also review vendor agreements to ensure legal compliance and revise website terms of use to reflect evolving cookie litigation mitigation practices.

Jen: Most of my day is spent on video calls counseling clients on a range of privacy matters. Sometimes, we are working on large, ongoing projects together, and sometimes, we are responding to a discrete matter that just arose. Every day is different, and I enjoy pivoting between clients from different industries, sizes, and stages in their privacy program development. I also spend time each day collaborating internally with my partners and associates on legal developments, interpretation of laws, and client strategies.

What training, classes, experience, or skills development would you recommend to someone who wishes to enter your practice area?

There are a number of privacy certifications available through the International Association of Privacy Professionals. We also publish numerous articles and blogs through our website, <https://www.bakerdatacounsel.com>. Privacy practitioners need to stay continually informed of privacy updates, as information gets stale quickly.

What is the most challenging aspect of practicing in this area?

The U.S. privacy landscape is rapidly evolving and becoming increasingly complex to harmonize when building and maintaining a privacy program. It can be challenging for busy in-house lawyers to keep up with these requirements, so it is our job to be proactive and make our clients aware of changes in the law and ways that we can update their privacy program and try to future-proof it within the resources that they have. We understand that there may be some fatigue caused by the

magnitude of privacy changes in the past five years or so, and our job is to support our clients and to efficiently solve problems with them.

What do you like best about your practice area?

Privacy compliance work offers an incredible amount of variety. No client's privacy strategy is ever the same as another's, which means we are constantly facing new challenges and opportunities to learn. Additionally, the intersection of different privacy laws creates interesting fact patterns, making the work intellectually stimulating. This diversity keeps privacy work engaging and allows us to develop creative solutions tailored to each client's unique needs. There is never a one-size-fits-all approach.

How do you see this practice area evolving in the future?

As technology continues to advance and data becomes an even more critical asset, the complexity of privacy laws and regulations will undoubtedly increase. This will require privacy counselors to stay ahead of the curve by continuously updating their knowledge and adapting to new legal frameworks.

For example, the increasing focus on state consumer rights and data transparency in the absence of a U.S. federal consumer privacy law will continue to drive demand for more robust privacy programs. This demand will only increase as we gain more clarity from regulators through rulemaking, guidance, and enforcement examples. As a result, more businesses will need to implement comprehensive privacy policies, conduct regular risk assessments, and ensure compliance with evolving laws. Additionally, the rise of automated decision-making and AI will introduce new privacy challenges, requiring innovative legal strategies to address issues such as data bias, transparency, and vendor liability.

What are some typical career paths for lawyers in this practice area?

The possibilities are endless, as this is a very marketable area where skilled privacy attorneys remain in high demand. We enjoy the variety of work that private practice offers, but other enriching career paths are available in-house and in government and public policy roles. In private practice, attorneys work with diverse clients, helping them navigate privacy regulations and develop data protection strategies. In-house privacy roles are integral parts of a business' operations, and in-house attorneys work closely with different departments to ensure compliance with privacy laws and to manage data protection initiatives. Government roles include developing and enforcing privacy laws, leading investigations, and shaping public policy. Each path offers unique opportunities and fulfillment.

BAKER & HOSTETLER LLP

“Privacy work offered a unique opportunity to address complex issues at the intersection of technology, law, and human behavior. Transitioning to privacy governance allowed me to leverage the skills developed during my years as a litigator while focusing on proactive strategies to ensure compliance with privacy regulations in a practical fashion for businesses.”

Jiwon (Jamie) Kim, Associate