Maeve Malik

Associate, New York

"I like the advisory and problem-solving nature of the practice. Our clients come to us because they have complex issues and initiatives involving the use of data, and need help navigating new, and often untested, compliance requirements. We take pride in our ability to help them address these challenges in the face of a complicated and constantly evolving patchwork of potentially applicable privacy and data security requirements."

With over 900 lawyers in the United States, Asia, Europe and the Middle East, Hunton Andrews Kurth LLP serves clients across a broad range of complex transactional, litigation and regulatory matters. We are known for our strength in the energy, financial services, real estate, and retail and consumer products industries, as well as our considerable experience in more than 100 distinct areas of practice, including privacy and cybersecurity, intellectual property, environmental, and mergers and acquisitions. Our full-service litigation practice is one of the largest in the country, with particular depth in key litigation markets such as Texas, California, Florida and the Mid-Atlantic. Visit HuntonAK.com and follow us on X, Linkedln and YouTube.

HUNTON
ANDREWS KURTH

©2024 Hunton Andrews Kurth LLP | HuntonAK.com

Hunton Andrews Kurth LLP

Maeve Malik, Associate—Global Privacy and Cybersecurity Practice

Maeve Malik is an associate in Hunton Andrews Kurth LLP's New York office and a member of the firm's global privacy and cybersecurity practice. Maeve has extensive experience advising clients on cybersecurity incident response and has advised on data breach response and notification obligations for several large-scale cybersecurity incidents, including one of the largest breaches affecting 3.5 billion user accounts. Maeve also regularly advises clients on developing or enhancing existing global privacy compliance programs to help manage privacy risks. She works with clients on their proactive cyber incident readiness activities, such as data breach notification toolkits, tabletop exercises, and incident response plans and procedures (including ransomware procedures). Maeve is a co-chair of the firm's veteran's pro bono program and serves on the pro bono committee of Hunton's New York office. She received her J.D., *cum laude*, from William & Mary Law School, and her B.A. from Drew University, *summa cum laude* with specialized honors.

Describe your practice area and what it entails.

Our top-ranked global privacy and cybersecurity practice helps companies manage data and mitigate risks at every step of the information life cycle. We advise clients in identifying, evaluating, and managing complex global privacy and information security risks and compliance issues. For cybersecurity matters, we advise large, multinational companies on all aspects of catastrophic cybersecurity incidents, including providing strategic and legal advice in investigating and remediating the incident; fulfilling their data breach notification responsibilities; responding to multi-jurisdictional regulatory investigations; and managing inquiries from customers, business partners, media, and regulators. We also advise clients on conducting proactive breach preparedness activities, including developing incident response plans and information security policies, running executive-level tabletops, performing information security assessments and tests, and engaging third-party experts in advance of an incident. In relation to our privacy compliance practice, we advise clients on state, federal, and international privacy laws; conduct privacy and data security impact assessments; and counsel companies on managing risk in connection with leading-edge and innovative technologies.

Our privacy and cybersecurity practice is augmented by The Centre for Information Policy Leadership (CIPL) at Hunton Andrews Kurth, a privacy think tank associated with the firm.

What types of clients do you represent?

We represent a diverse group of clients of all sizes, including retailers, consumer goods companies and manufacturers, energy companies and utilities, technology companies, financial institutions and private equity firms, fintech startups, insurance providers, health care providers, media companies, hospitality and gaming companies, direct marketers, telecommunications and Internet service providers, cloud providers, cybersecurity companies, government agencies, and risk management specialists.

What types of cases/deals do you work on?

We advise clients on:

- compliance with all U.S. federal and state privacy and cybersecurity requirements, and international data protection laws;
- cybersecurity and data breach incident response;
- drafting and negotiating complex privacy and data security provisions and indemnities in vendor agreements;
- managing federal, state, and international regulatory inquiries in connection with alleged privacy and data security violations;
- evaluating cybersecurity and privacy risks and negotiating purchase agreements in connection with potential mergers, acquisitions, and other corporate transactions;
- advising on cross-border data transfer strategies;

©Copyright 2024 Vault.com, Inc. Photocopying is illegal and expressly forbidden.

- designing and evaluating privacy impact assessments;
- developing and enhancing comprehensive records management programs; and
- information product life cycle issues, including marketing and analytics activities.

How did you choose this practice area?

When I was a summer associate at Hunton, I met one of the partners on my current team, Brittany Bacon, who helped foster my interest in privacy work. Brittany became a mentor to me and quickly saw privacy and cybersecurity as a potential area of focus for me. If it weren't for her identifying that early on, I never would have known to ask. At the time, the practice area was still very new, and I didn't know anyone else from my law school class who would be pursuing a career in privacy and cybersecurity after graduation.

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

Each day varies based on our clients' needs. On a given day, I might help a client respond to and analyze notification obligations related to a cybersecurity incident; prepare or revise an incident response plan or privacy policy; negotiate privacy and data security provisions in a contract; or provide guidance on how to comply with a new U.S. state privacy law. While every client faces a different set of challenges, questions, and concerns, there are commonalities in terms of privacy and cybersecurity being a top priority for organizations in all industry sectors.

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

Privacy and cybersecurity is a hot area of focus. Follow industry trends and various industry publications and learn as much as possible. Additionally, I encourage law students and lateral associates to subscribe to Hunton's Privacy and Information Security Law blog, www.huntonprivacyblog.com, which we update on a near-daily basis with news items and analysis. Our team also has published a Privacy and Cybersecurity Law treatise, updated annually, which provides a comprehensive primer on U.S. and international privacy and data protection laws. Organizations like the International Association of Privacy Professionals (IAPP) are great resources as well.

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

The most challenging aspect of practicing in this area is keeping up with the most recent updates in global laws, regulations, guidance, and civil and regulatory actions. This is a constantly evolving practice area that is a primary focus of lawmakers and consumers around the world, so there is always something new on the horizon.

What do you like best about your practice area?

I like the advisory and problem-solving nature of the practice. Our clients come to us because they have complex issues and initiatives involving the use of data and need help navigating new (and often untested) compliance requirements. We take pride in our ability to help them address these challenges in the face of a complicated and constantly evolving patchwork of potentially applicable privacy and data security requirements.

What is unique about your practice area at your firm?

Our practice has been recognized by *Computerworld* magazine, Chambers and Partners, and The Legal 500 as a top firm for privacy and data security counseling. With nearly 50 privacy professionals, including lawyers located across the globe in New York, Washington, DC, London, Brussels, and Beijing, we have 20 years of experience assisting clients of all sizes with various aspects of privacy and data security. We are supported by a carefully vetted worldwide network of knowledgeable data protection lawyers covering more than 100 countries. Our team works together seamlessly to provide customized, creative, and practical solutions to our clients' privacy and data security issues.

What are some typical tasks that a junior lawyer would perform in this practice area?

Junior lawyers on our team play a key role in supporting senior attorneys and are introduced to substantive matters from day one. They learn quickly how to draft a variety of documents that privacy and cybersecurity lawyers prepare in their day-to-day practice, such as privacy policies, data breach notification letters, contractual provisions addressing privacy and data security, incident response plans, internal policies, and training materials.

©Copyright 2024 Vault.com, Inc. Photocopying is illegal and expressly forbidden.

HUNTON ANDREWS KURTH LLP

> "Each day varies based on our clients' needs. On a given day, I might help a client respond to and analyze notification obligations related to a cybersecurity incident; prepare or revise an incident response plan or privacy policy; negotiate privacy and data security provisions in a contract; or provide guidance on how to comply with a new U.S. state privacy law."
>
> ***Maeve Malik, Associate***

©Copyright 2024 Vault.com, Inc. Photocopying is illegal and expressly forbidden.