BCLP. Client Intelligent

AMY DE LA LAMA

Partner
Boulder

Partner; Chair – Global Data Privacy and Security Practice; and Global Practice Group Leader – Technology, Commercial and Government Affairs

E: amy.delalama@bclplaw.com
T: +1 303 417 8535

BIOGRAPHY

Amy is the Global Practice Group Leader for Technology, Commercial & Government Affairs and also the Chair of the Firm's Global Data Privacy and Security Practice. She has nearly two decades of experience in global privacy, data security and cyber security with a specific focus on health care privacy and security issues. She provides advice to a wide range of multi-national pharmaceutical, life sciences and medical device companies, as well as retail companies, online businesses, B2B companies, and other types of organizations regarding these issues. Amy has deep experience guiding health care clients through the development and implementation of broad-based privacy compliance programs as well as advising on GDPR and similar global privacy laws in addition to CCPA, HIPAA and other US privacy law issues. She assists regularly with transactions involving

complex health privacy issues and also advises organizations on emerging health tech issues, including those related to the collection of health and medical data in the context of digital advertising and the use of this and other sensitive data for AI/machine learning purposes. Amy regularly assists organizations navigate the full life cycle of security incidents and data breaches as well as with breach preparedness and remediation.

CIVIC INVOLVEMENT & HONORS

- *The Best Lawyers in America*, Privacy and Data Security Law (2023)
- *Chambers USA*- Nationwide, Privacy & Data Security, "Up and Coming" (2023)
- *Legal 500 US*, Next Generation Lawyer in Cyber Law (including Data Privacy and Data Protection), 2019 - 2020

PROFESSIONAL AFFILIATIONS

- Certified Information Privacy Practitioner
- Illinois State Bar Association - Member
- Colorado Bar Association – Member

AI LEGISLATION SNAPSHOT

To help companies achieve their business goals while minimizing regulatory risk, our team actively tracks proposed and enacted AI regulatory bills from across the Unites States to enable our clients to stay informed in this rapidly-changing regulatory landscape.

ADMISSIONS

- Illinois, 2004
- Colorado, 2001

EDUCATION

- University of Colorado, J.D., Order of the Coif, 2001
- University of Virginia, B.A., high honors, 1996
- University of Virginia, B.A., summa cum laude, 1996

RELATED PRACTICE AREAS

- Data Privacy & Security
- Healthcare & Life Sciences
- Corporate
- Investigations
- Regulation, Compliance & Advisory

RESOURCES

PUBLICATIONS

- Schrems II,' data transfers and Brexit — What are the implications?, IAPP, July 2020
- How to Know if Your Vendor is a 'Service Provider' Under CCPA, IAPP, July 2019
- Navigating Disclosures and Sales of Personal Information Under the CCPA, IAPP, August 2019
- Business Implications of Colorado's New Data Privacy Law, October 2018

SPEAKING ENGAGEMENTS

- Navigation of Health Data Laws Beyond HIPAA, BCLT Privacy Law Forum: Life Sciences, November 2023

RELATED INSIGHTS

Insights
Apr 08, 2024
New York May Lead the Pack Through Imposition of Data Excise Taxes

Insights
Mar 05, 2024
Washington My Health Data Act FAQ's: processing biometric data

News
Feb 20, 2024
Chambers Global 2024

Insights
Feb 14, 2024

Washington My Health My Data Act FAQS: data subject rights

On April 27, 2023, the Washington State governor signed into law the My Health My Data Act or the MHMDA. In spite of the onerous and at times confusing requirements of the MHMDA, the Washington Attorney General (AG) has only published a short set of Frequently Asked Questions to help address some of this uncertainty. Nevertheless, most of the law's provisions take effect on March 31, 2024, meaning that, at this point, companies have a very short runway to meet their obligations and brace for the private right of action allowed for under the act. Like so many other features of the MHMDA, data subject rights are deceptively complicated and have the potential to create significant administrative hurdles to getting it right. As promised in our recent summary of the MHMDA (MHMDA: Time to Comply), we are examining in more detail these tricky issues in our MHMDA FAQs and have done a deep dive into data subject ri…

Insights
Feb 12, 2024

Colorado adopts universal opt-out requirements

Webinars
Feb 08, 2024

Public Company Update, Cybersecurity Issues and Other Trending Topics

Insights
Feb 02, 2024

Reviewing SaaS agreements in the age of AI

The development and implementation of AI-powered tools, including in SaaS platforms, have experienced a meteoric rise over the course of the last year. Businesses are understandably looking to realize competitive advantages from leveraging these new AI technologies, but adding AI to a tech stack can present serious risks related to bias, data ownership, privacy, accuracy and cybersecurity. As with many new tools, an organization's procurement team is its first line of defense in de-risking AI, and AI literacy is essential in this process. Fortunately, while AI presents unique issues and considerations, the incorporation of AI into SaaS does not require a wholly novel SaaS agreement. Nevertheless, there are key provisions that must be considered carefully to meaningfully address the new risks and issues triggered by the incorporation of AI and the nascent state of the law and contract norms in this space. With …

Insights
Jan 29, 2024

Time to Comply: Washington My Health My Data Act

On April 27, 2023, the Washington State governor signed into law the My Health My Data Act or the MHMDA. In spite of the onerous and at times confusing requirements of the MHMDA, the Washington Attorney General (AG) has only published a short set of Frequently Asked Questions to help address some of this uncertainty. Nevertheless, most of the law's provisions take effect on March 31, 2024, meaning that, at this point, companies have a very short runway to meet their obligations and brace for the private right of action allowed for under the act. With this in mind, we have prepared this brief recap of the law and the steps companies should consider as they gear up for compliance. Our more detailed summary of the MHMDA is available in our original insight, and we will also be releasing a series of short FAQs over the coming weeks to help companies prepare.

Insights
Jan 04, 2024

Pressure-testing your privacy program for 2024

With the onslaught of new privacy legislation and cyber threats coupled with upticks in enforcement, running a well-functioning and flexible privacy program is now, more than ever, a critical component of an organization's overall risk compliance strategy. As part of this process, companies must pressure-test their privacy programs regularly to make sure they appropriately address existing and emerging risks while maximizing business gains. A comprehensive review is not always possible, but it is important to keep in mind that the last several years have seen a wave of new state privacy laws as well as activity at the federal level that promises to challenge even the most well-developed privacy team. To help companies develop a strategy tailored to 2024, we have highlighted a few key issues below that will be particularly relevant over the coming year.