The Legal Intelligencer

Our Take: Minimize Your Personal Data, It's Good for Business

Data privacy obligates us as attorneys to think about the proper handling of personal data in virtually every aspect of the legal work we do.

By Tess Blair, Tara Lawler and William Childress | June 22, 2021 at 1:40 PM

(l-r) Tess Blair, Tara Lawler, and William Childress, of Morgan, Lewis & Bockius.

Information is the currency of our digitally powered economy, and that includes our profession. No one appreciates the challenges and opportunities that data presents more than the digital lawyer. Our series for The Legal Intelligencer aims to address the myriad challenges and opportunities that the proliferation of data presents, and we write this installment to add the emergence of domestic data privacy laws to the layers of complexity in the information governance, discovery, and contract analytics work of the digital lawyer. Data privacy obligates us as attorneys to think about the proper handling of personal data in virtually every aspect of the legal work we do.

Historically, data privacy laws have had a modest reach in the United States. As other parts of the world embraced data privacy regulations, the United States lagged and resisted widespread regulation. Federal privacy laws are sector based, focusing on areas such as health care and financial services, but are limited in reach. A patchwork of state laws has emerged, but these laws typically regulate discrete data sources and lack broad application. In litigation, data privacy

issues emerge most often when data with medical records, Social Security numbers, or financial account information is at issue.

The General Data Protection Regulation (GDPR) has emerged as the global gold standard for data privacy. Although attorneys who deal with cross-border discovery or represent global clients have been addressing European data privacy issues for more than a decade, all attorneys should be thinking of data privacy regulation and compliance now. Domestic privacy laws will soon have a far-reaching impact and will regulate data central to our practices. These laws provide consumers with an array of new rights and controls over their data and impose new obligations on businesses and the law firms that touch this personal data.

In 2018, California became the first state to pass a comprehensive privacy law with the California Consumer Privacy Act (CCPA). Although inspired by the GDPR, the CCPA is far more limited. Less than a year after it went into effect, California voters dramatically expanded the CCPA with the California Privacy Rights Act of 2020 (CPRA). The amendments, which go into effect on Jan. 1, 2023, give consumers more rights over their data, impose more burdens on companies, and better align California's privacy law with the GDPR.

In 2021, in a watershed moment for domestic data privacy laws, Virginia passed the Consumer Data Protection Act, which like the CPRA goes into effect on Jan. 1, 2023. And in early June, the Colorado legislature passed a similar data privacy bill, which is awaiting the governor's signature and is expected to become law.

As of this spring, broad data privacy laws are under active consideration in the Illinois, Massachusetts and New York legislatures and bills were considered in more than a dozen other states this year. Given this landscape, we anticipate that privacy legislation will accelerate as more states move to catch up with the early data privacy leaders. A lack of consensus over issues such as a private right of action for consumers and preemption make passage of a federal data privacy law with omnibus standards unlikely, at least during this Congress. The Uniform Law Commission is currently drafting a uniform model data privacy law for states to enact in the future, but a patchwork of varying and, in some cases, conflicting data privacy laws will likely continue to be passed by legislatures across the country. Attorneys will need to be attentive as these new data privacy laws go into effect and quickly learn how to navigate the nuanced requirements and differences that are sure to follow.

Considering this new reality, attorneys should be prepared to adopt scalable and repeatable approaches to compliance for their practices and their clients. In practical terms, we can start by understanding the basic ways that data privacy impacts the discovery of personal data before and during the litigation process.

Data minimization is a core tenet of the GDPR and limits an organization's collection of personal data to only the data necessary to accomplish a specified business purpose. The new California and Virginia data privacy laws import the concept of data minimization to the United States. Data minimization requires an organization to know what personal data it collects and why long before a legal hold is triggered. With this knowledge, the organization can then determine what data has a clear nexus to the business purpose for which the data was collected and where and for how long it is used. For a hilarious example of this concept, recall the Norton Lifelock commercial where the kid is logging on to a video game website and asks his mom: "Mom, what's your four

hundred and one K number?" See https://www.ispot.tv/ad/t8F9/norton-360-with-lifelock-caf-v1. Simply stated, this principle requires companies to identify the minimum amount of personal data needed for their defined business purposes and to retain only what is needed for those purposes. When personal data is no longer needed (or should not have been collected in the first instance), disposal in accordance with a sound information governance program should be a best practice.

Unfortunately, U.S. organizations tend to retain personal data for long periods because of its potential future value, low cost of storage, and lack of virtually any incentive not to. So do the people in these organizations, which of course you already know. The same natural human impulse that leads some of us to fill our closets with items we will never wear again is the same one that leads us to hoard email. Whether compulsive or otherwise, this type of data accumulation is clearly not the road to data minimization. And when litigation or an investigation arises, this personal data can be swept up in a legal hold, creating a potential conflict with data privacy laws.

When a legal hold is triggered, data privacy laws make carefully scoping out the hold more important than ever. In current practice, there is little downside to casting a wide net to preserve data, however remote its potential relevance to the matter, especially where there is real downside (read: spoliation motion) for not preserving relevant data. Consequently, legal holds are often quite overbroad, sweeping in dozens (and dozens and dozens of sometimes marginally relevant) custodians and vast quantities of data. However, data minimization should get attorneys in the practice of using a scalpel instead of a backhoe to craft a legal hold. This obligation requires a careful analysis of the issues involved, an individualized determination of who should be placed on hold, and an understanding of the relevant time frame. Proper scoping ensures that unnecessary data won't be put on legal hold.

Further, attorneys need to reconsider the "set it and forget it" approach to legal holds. While it is common for counsel to add individuals and data sources to expand a hold as the matter progresses, it is pretty rare to see any of us narrow a hold or release custodians as additional facts emerge making their irrelevance clear. Legal holds are no more static than litigation. Reevaluating and narrowing a hold as a case matures is a good practice that is likely to become a necessary one as data privacy law expands across the United States.

To further the principle of data minimization, legal holds should also be released promptly when the obligation to preserve ends. Figuring out when to release can be challenging, particularly in investigations or threatened litigation. Too often, legal holds continue for months or even years out of caution, lack of information, inattention, or the absence of a process identifying legal holds that should have expired.

Of course, lifting the hold is the easy part. Disposing of data on hold is another story. Add personal data to the equation and now you have a real challenge. For one thing, personal data requires as much protection and care during disposal as it does when collected, processed, used, and stored. Compliance with Department of Defense or National Institute of Standards and Technology deletion standards and certification of destruction from third parties responsible for deletion should be required. For personal data produced in litigation, there should be a clear mechanism in place, such as a protective order and ESI protocol that addresses data privacy and specifies a process for the destruction or return of such data. If your protective order and ESI protocol templates do not address data privacy, now would be a good time to update them.

Domestic privacy laws will also impact how attorneys handle client data during an engagement. Depending on the circumstances and the personal data at issue, law firms may be required to enter into data processing agreements with their clients. These agreements often include contractual terms related to permissible processing and security of personal data received from or on behalf of a client, notice and cooperation terms related to data breaches, and ownership and disposition of data at the end of an engagement.

Although some attorneys believe that data minimization conflicts with U.S. document-retention and legal-hold obligations, it does not have to. Indeed, minimization, retention, and preservation can work together with proactive information governance and smart (not kneejerk) discovery strategy. As it turns out, "data minimization" is a sound business and information governance practice because it lowers costs and reduces risk. It will soon be an important legal obligation as well.

Morgan, Lewis & Bockius partner Tess Blair is the founder and leader of the firm's eData practice. Partner Tara Lawler 's practice focuses on e-discovery, information management, and data privacy. Associate William Childress counsels clients on electronic discovery.