Data law: a part of cyberlaw we all should know about

By John Bandler, Esq., Bandler Law Firm PLLC

FEBRUARY 19, 2025

Data laws are those laws specifically created to address issues regarding the collection and use of data about people. Data law is a part of cyberlaw, and cyberlaw is a part of all law.

If any of that sounds unfamiliar to you now, it won't be after this five-minute article.

Cyberlaw recap

In the last column we discussed cyberlaw, what it is, and how it is everywhere. We adopted an expansive definition that includes all the ways technology intersects with law. ("Cyberlaw: An area of law for all of us," Reuters Legal News, Dec. 16, 2024, https://reut.rs/3WUmoOA).

All "traditional" areas of law have adapted for our new cyberworld. Criminal law, contract law, negligence law, intellectual property law, and more now address the once novel situations created through cyberspace's infiltration of all areas of life and law.

Still, the existing bodies of law were insufficient for some of the unique and pressing aspects of our cyber age. Rampant cybercrime with regular data breaches meant new laws were needed to try to address those issues. Massive collection of data about people and the use and sale of this personal information for commercial profit meant new laws for that.

Data law is a part of cyberlaw, and cyberlaw is a part of all law.

In the last article we touched on these data laws, and as promised we now bring some additional discussion.

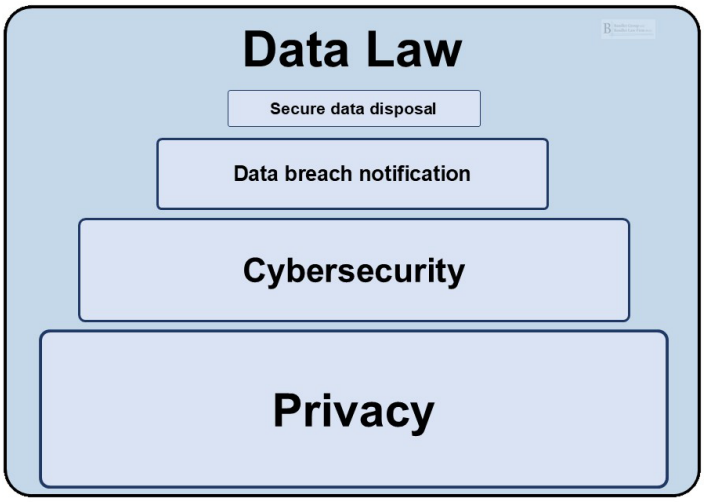
Data law introduced: simple to complex

Data laws were enacted to fill a void and address some of the new issues in our cyberworld with consumer data, cybercrime, and privacy.

From simple to complex, we can list four main categories of data law as:

- Secure data disposal;
- Data breach notification;
- Data protection (cybersecurity);
- Privacy.

That is also a rough chronology of how many of them came to be, at least from one perspective. We can depict this progression and relationship in this diagram:



Data Law (evolution and complexity)

Courtesy and copyright John Bandler from his book: Cyberlaw: Law for Digital Spaces and Information Systems

Secure data disposal laws essentially require secure deletion of consumer data. This includes wiping residual data from computers before reselling or recycling them, or securely shredding paper documents instead of simply dumping them in the trash or recycle bin. It was a first step and now the most obvious part of a solid cybersecurity law or program.

Data breach notification laws created the right for consumers to learn when their data had been breached and created the duty for a compromised (hacked) organization to make that notification to those consumers and the government. Before breach notification laws, many breached companies did what they thought was in their own best interests: often pretending nothing happened to preserve their business or reputation, and to avoid lawsuits or regulatory actions. Now they have a legal duty to report, and those that refuse face potential legal consequences.

Data protection laws seek to prevent data breaches in the first place by requiring cybersecurity measures. Most of these laws came after breach notification laws. We can imagine government regulators receiving and reviewing hundreds of breach notification

reports and quickly realizing that improved cybersecurity could prevent many of them. Soon enough, cybersecurity laws were enacted.

Many privacy laws came next. In our cyber age, privacy is a heightened concern as data about all of us is collected, shared, and sold. It is used to target us for marketing, persuasion, influence, and even manipulation. Fewer existing laws could be applied to this, so new laws are being created and updated regularly. Privacy laws started appearing slowly to our view, such as the European Union's General Data Protection Regulation (GDPR) which went into effect in 2018, and the California Consumer Privacy Act (CCPA) of 2018 which became effective in 2020. Then many states followed suit, and more will.

Privacy laws give rights to consumers and impose legal duties on organizations and how they collect, store, use, and share consumer data. Consumer notice and consent are an important part of these privacy laws.

Some cynics might argue that most of these laws do not impose significant burdens on companies, but merely allow them to do whatever they want, so long as they tell consumers what they are doing through their privacy notice (or privacy policy). These notices can be voluminous torturous reads, perhaps undertaken only by lawyers for that organization, or lawyers for another needing a template or ideas.

Clearly the word count and complexity of many privacy laws are significant, and they impose costs to comply with consequences for noncompliance.

Whether the privacy notice is read by a consumer or not is largely irrelevant because it is the organization's promise to the world, and that comes with legal significance.

More precision on the privacy chronology

From a state law perspective, the chronology from data disposal, data breach notification, cybersecurity, and privacy is helpful and aligns with simple to complex.

That chronology is not fully accurate because privacy has been around since long before our cyber data explosion. Privacy frameworks with legal weight go back decades. Fair Information Practice Principles (FIPPs) started in the U.S. in the 1970s. Then came privacy guidance from the international Organisation for Economic Co-operation and Development (OECD) in 1980, and Asia-Pacific Economic Cooperation (APEC) in 2004.

The federal Privacy Act of 1974 addressed federal government use of consumer data, then the 1996 Health Insurance Portability and Accountability Act (HIPAA) was a major privacy law for the health sector, which spawned health care regulatory rules for privacy (2000), security (2003), and breach notification (2009). Also consider the Gramm-Leach-Bliley Act (GLBA) of 1999 for the financial sector.

In that sense, basic privacy laws predated the outbreak of commercial and black market demands for our data. Those demands further underscore the need for privacy protections because now we have regular cybercrime breaches of consumer data plus tech companies who know all about our lives, movements, friends, interests and thoughts.

Other types of data law?

Should we be thinking about other types of "data law"? Maybe or maybe not.

Artificial intelligence (AI) definitely belongs within the realm of "cyberlaw" and some of it can be addressed within data law. AI is both a powerful tool and a persuasive marketing buzzword that presents many issues for law and society. The next question is which areas of law to look at. New laws specific for AI will come, but we will also look to data law (privacy) and "traditional" laws (such as copyright) which will continue to adapt to cyber changes.

Privacy laws give rights to consumers and impose legal duties on organizations and how they collect, store, use, and share consumer data. Consumer notice and consent are an important part of these privacy laws.

The traditional rules for attorney professional responsibility certainly apply to AI (as we covered a while back; see "AI's promise and problem for law and learning," Reuters Legal News, Feb. 21, 2024, https://reut.rs/3CJ1R8V). Lawyers were always responsible for what they submitted and did, and it was never acceptable for an attorney to tell the judge, "Sorry, that brief and research were done by an intern, and I didn't have time to review it or supervise it." It is no surprise that blind reliance on a computer tool or generative AI is not a valid excuse either. Attorney duties remain even as technology changes.

Considerations outside of law

With AI and other cyber issues, we should resist viewing the law as the sole tool or forum. A hammer tends to think everything is a nail, and attorneys should recognize some limits on their domain.

First, law sometimes gets shaped according to a process that is not always focused purely on the good of the country or its citizenry. No surprises that law is not perfect.

Second, we should look beyond our legal realm to broader issues of society, learning, decision making, and the power of technology over our lives and systems of government.

We must remember that technology is not simply an amorphous autonomous thing. It is made up of platforms and tools built and controlled by humans. People have power to shape that technology

or platform; sometimes it is a group of people, sometimes even a single person.

That technology or platform can, in turn, shape, persuade, and even manipulate other humans to achieve specific results. That result might simply be a view, click, or purchase, but sometimes it is for deeper reasons that can greatly affect society, thought, and even our government through pre-election voter persuasion.

John Bandler is a regular contributing columnist on cybercrime and cybersecurity for Reuters Legal News and Westlaw Today.

About the author

John Bandler is a lawyer, consultant, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps protect organizations from cybercrime, improve cybersecurity, and better protect and manage information systems. His latest book is "Cyberlaw: Law for Digital Spaces and Information Systems" (2025). His firm, based in New York, is **Bandler Law Firm PLLC**, and he can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on February 19, 2025.