Building a Privacy Program That Works Across Borders

HOW A COMMON LEGAL FRAMEWORK SHAPED GLOBAL PRIVACY LAWS

John Williams Amundsen Davis

Since Sweden passed the first privacy law in 1973, 171 countries have adopted national laws regulating how personal information can be collected, used, and shared. The U.S. is not one of those countries. Instead of one comprehensive federal privacy law for the private sector, we have dozens of industry- and state-specific laws that vary based on what kind of information businesses collect and where their customers live.

While managing this global patchwork of privacy laws can feel overwhelming, it may be easier than you think. Almost all privacy laws share a common, easily recognizable structure: they create rights for the people whose personal data is collected ("data subjects") and obligations for the entities that collect and use the personal data ("data controllers"). Data subjects generally have the right to know what information a data controller has about them and correct or delete that information. For their part, data controllers are prohibited from over-collecting or misusing personal data, and they must keep it secure.

Understanding why privacy laws around the world are so similar is an interesting story; it can also help businesses comply with these laws efficiently and sensibly.

THE COMPUTER NERDS WHO INVENTED PRIVACY LAW

The common elements in today's privacy laws were very intentionally developed by a small group of computer policy experts in the 1970s. Probably the most important American member of this group was Willis Ware, a Rand Corporation scientist and lead author of the famous 1973 U.S. government report, "Records, Computers, and the Rights of Citizens." This report proposed five basic rules to govern the relationship between humans and computers, which it called "fair information practices" (FIPs).

The policy debate during the time Ware and his team developed the FIPs was similar in some ways to today's debate about artificial intelligence (AI). As the capability of computers to process and store personal information (in so-called "data banks") quickly advanced, the technology faced backlash from people who worried that it would eliminate their jobs and threaten their personal autonomy. Professor Arthur Miller published a bestselling book titled "The Assault on Privacy: Computers, Data Banks, and Dossiers," and Congress held hearings examining whether the U.S. was turning into the surveillance state depicted in George Orwell's novel "1984."

Ware and his colleagues were optimistic computer nerds, confident that technology could help governments and businesses operate more efficiently while respecting important human values. They emphasized the "mutuality" of the relationship between data controllers and data subjects. In the

digital age, data subjects may have to share their personal information with a third party to receive services or government benefits. But in exchange, the third party must agree to limits on data use. This insight formed the basic structure of Ware's FIPs and many later versions of "fair information principles" that form the core of today's global privacy laws.

FIPS BECOME LAWS

Congress liked Ware's ideas so much that they used his FIPs as the foundation for the Privacy Act of 1974, one of the earliest national privacy laws that, more than 50 years later, still governs how federal agencies must treat the personal information of U.S. citizens. The law requires federal agencies to disclose what kinds of personal "records" they gather about U.S. citizens and limits how they may use those records. It correspondingly gives individuals the right to access and correct any records the agencies hold about them, and to sue agencies that misuse the records.

Ware had colleagues in other countries who were developing similar rules of the road for humans and computers. In 1980, two important multinational organizations, the Council of Europe (CoE) and the Organization for Economic Cooperation and Development (OECD), published "data protection" (i.e., privacy) guidelines for their member countries. The dual goals of these guidelines were to protect personal information and "harmonize" the privacy laws that individual countries were beginning to adopt.

Following Ware's approach, the CoE and OECD guidelines are based on a set of high-level privacy principles. For the CoE's authors, the purpose of this "common core" set of principles was to "guarantee to data subjects in all countries…a certain minimum protection with regard to automated data processing of personal data." If different countries' privacy laws shared a common baseline of privacy protections, then people's privacy would be protected and the data could cross national borders without restrictions. Although the OECD proposed eight fair information principles (instead of the five FIPs developed by Ware), they followed the same pattern: a few basic rights for data subjects and obligations for data controllers.

These guidelines were, and remain, hugely influential models for national privacy laws all over the world. The CoE document, known as "Convention 108," is still in effect and has been ratified by 55 countries, including almost a dozen non-European countries.

From our 2026 perspective, however, the most important impact of these guidelines comes through the privacy laws that the European Union adopted in 1995 and then revised and updated in 2016. Article 5 of the 2016 law, commonly known as the General Data Protection Regulation (GDPR), lists six fair information principles that descend directly from the OECD list. Article 5 requires that personal data must be:

- Processed with "lawfulness, fairness, and transparency."
- Collected for limited purposes ("purpose limitation").
- Used only to perform agreed-upon services ("data minimization").
- Maintained in an accurate and up-to-date condition ("accuracy").
- Disposed of when no longer needed ("storage limitation").
- Protected from unauthorized use ("integrity and confidentiality").

A final, seventh "accountability" principle requires data controllers to comply with the previous six principles.

THE "BRUSSELS EFFECT"

The GDPR's Article 5 fair information principles may seem familiar to you because they have almost literally been copied and pasted into the privacy laws of dozens of countries around the world and many U.S. states. For example, the authors of the ballot initiative that created the California Consumer Protection Act (CCPA) used the principles listed in Article 5 as the model for the CCPA's section setting out the "General Duties of Businesses that Collect Personal Information" (Cal. Civ. Code § 1798.100).

One of the reasons the GDPR has been so widely imitated by the rest of the world is the GDPR's "adequacy" provision (Article 45). This section says that if a non-EU country has privacy protections that are "essentially equivalent" to those that the GDPR provides European citizens, the personal information of European citizens can be transferred to that country without additional legal protections.

Countries eager to increase their digital trade with the large and wealthy European market have a strong incentive to achieve "adequacy." The European Commission currently recognizes 15 countries (including Brazil, Japan, and—at least for now—the U.S.) as "adequate," but many others are vying for this favored status. This global interest in meeting Europe's privacy standards (sometimes called the "Brussels effect") means that most national privacy laws adopted over the past two decades have been modeled on the EU laws.

WHAT THIS MEANS FOR YOUR PRIVACY PROGRAM

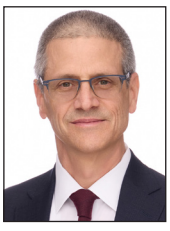
It is easy to dwell on the quirky nuances and vocabulary of individual privacy laws. In one law, a data controller needs to have a "legitimate interest" to use personal data, while in another it must have a "business purpose." An entity can be a "processor" in one law, but a "service provider" or "business associate" in others. And, of course, no privacy law defines "personal information" or "personal data" in exactly the same way.

But when you look closely, you will see they are built on the same basic chassis that Ware and his colleagues designed many decades ago. Following Ware's "mutuality" model, the laws give data subjects certain rights over their personal information and hold data controllers accountable for honoring these rights.

For businesses trying to follow the letter and spirit of these privacy laws, accountability means:

- Clearly disclosing to data subjects (through a privacy policy or other documents) what information they are collecting and what they are doing with it.
- Giving data subjects access to their information and the ability to update, correct and delete it.
- Keeping track of the personal information they hold, using it only for purposes they have disclosed to data subjects, and getting rid of it when they no longer need it.
- Implementing security measures that protect the information from improper use or sharing.

A business that has implemented and maintains this framework has done most of the work necessary to comply with any privacy law in the world. In other words, if a business following these global "fair information principles" decides to enter a new market, it has already done most of the work necessary to comply with the privacy laws of the new jurisdiction. While the details of each law are important, it is equally important to recognize that privacy law is a global language.



John Williams, partner in Amundsen Davis's Cybersecurity & Data Privacy Service Group, advises companies of all sizes on data privacy and cybersecurity practices, helping them distinguish themselves and build trust. He can be reached at jwilliams@amundsendavislaw.com.