Your organization's privacy policy — and privacy notice

John Bandler, Esq., Bandler Law Firm PLLC

OCTOBER 16, 2024

Privacy policies and privacy notices can cause fear and doubt for organizations and their compliance professionals and lawyers, but it does not have to be so.

Privacy is now an established profession and area of law, and every organization needs to think about their privacy program, policies, and notices.

As a general matter organizations should consider a "privacy policy" to be different from a "privacy notice." They have different functions and are for different audiences.

You have personally "agreed" to thousands of them in your lifetime, but how many have you actually read?

Simple definitions

Let's lay out some basic definitions realizing that terms (including "privacy policy") mean different things to different people and organizations.

- *Privacy* is an area of operations and law relating to consumer data and other information about people. Organizations have increasing responsibilities to protect the data they hold; consumers have increasing rights as to their personal information.
- A *policy* is an internal rule of an organization, usually general in scope. An organization could choose to make certain policies publicly available while others might have more restrictive classifications (such as "internal use only" or "confidential").
- A *notice* (or statement) is information you communicate to others.
- A *privacy policy* is an internal rule of an organization relating to privacy.
- A *privacy notice* is a public statement the organization communicates (e.g., to clients, customers, and consumers) to state how the organization handles privacy.
- A *privacy program* is everything the organization does relating to privacy.

These are simply my rough definitions, and terms are always subject to alternate meanings among different people and organizations. [A more authoritative glossary of privacy terms is provided by the International Association of Privacy Professionals (IAPP) on its website here: https://bit.ly/3TZIsG0].

Organizations should also think in a broader sense about **information governance** which is how they manage their information assets, including for privacy, cybersecurity, and to accomplish their mission.

Policy versus notice

As a general matter organizations should consider a "privacy policy" to be different from a "privacy notice." They have different functions and are for different audiences.

A notice (or statement) informs the public (or customers or clients) about the organization's privacy practices and how they will collect, store, use, and share a person's data. Some laws require a notice, and it provides transparency to let consumers know how their data is used.

A policy tells the organization and its employees what to do and what the organization's rules are regarding privacy. By writing down these rules nothing gets lost in the translation.

A policy may contain information that is not suitable for public disclosure or for people outside the business. For example, it may be appropriate to remind employees that they are required to follow the policies of their organization and that failure to do so could result in discipline, whereas customers have no such obligation.

Further, organizations may need to create rules about proprietary or non-public matters and these should not be within a public document. Other items suitable for a policy document would be what might be thought of as clutter in a public notice, such as revision history and details about who approves and who implements the policy.

A best practice is not a rigid rule

Though a policy and notice *should* be separate documents, organizations can [often] be forgiven if they use a single document for both purposes.

Compliance, action, and policy work — especially on privacy and other aspects of information governance such as cybersecurity — can be a nuanced endeavor. Minor inconsistencies, deviances, or differences of opinion do not automatically equate to non-compliance.

Even a lack of written policies on certain topics is not the end of the world, and my platform analogy allows for that, as discussed in an earlier article ("Building and updating organization policies and procedures," Reuters Legal News, June 18, 2024, https://reut.rs/4eAH44T).

Consider that a solid test for a policy or notice is whether it is clear, understandable, and appropriate for the audience. Employees should understand their internal policies and the average public should understand public notices.

Some organizations have merely a single privacy document (e.g., a combined policy and notice) to get started on privacy and reduce the number of governance documents they need to create and maintain.

Each organization should evaluate what laws require, what their mission requires, and plan and prioritize accordingly. Many privacy laws require organizations to provide notice to consumers about privacy practices, so that notice might be the starting point.

Privacy policy work with the five components

The Five Components for Policy Work are suitable for any topic and especially for complex areas of privacy and cybersecurity ("Management, policies, cybersecurity and compliance," Reuters Legal News, April 23, 2024, https://reut.rs/3RkwBAX). We consider:

- *External rules* such as applicable privacy laws.
- *Mission* — especially how consumer data is needed for the business of the organization.
- *Internal rules* such as policies (what they are now and what they should be).
- *Practice* (action) — what the organization does now, and what it should do
- *External guidance* — best practices (or any advice or tools) the organization could consider.

Samples and templates

Attorneys doing policy work have looked at other policies, and may ask:

- Why did they do it that way, should I do that too?
- Why did they include that, should I also?
- Should I add X to make it better and more ironclad?
- Should I add some legal language (or legalese) to make it more lawyerly?

Consider that a solid test for a policy or notice is whether it is clear, understandable, and appropriate for the audience. Employees should understand their internal policies and the average public should understand public notices.

To absurdity?

Privacy laws generally protect citizens of the government entity that issued the rule. The European Union's privacy law (General Data Protection Regulation or GDPR) protects citizens of the EU, including when they do business with (or visit the website of) a U.S. company.

The Federal Trade Commission (FTC) Act protects U.S. consumers (generally at least), the California Consumer Privacy Act (CCPA) protects residents of that state with detailed requirements, and so forth.

One tendency in public facing privacy statements is to inform consumers of various statutes that might apply depending on where they reside. This practice cannot continue to infinity and today there are many privacy laws from many places with more coming. Attempting to inform about all of them becomes less of a privacy notice and more a course on privacy law.

Years ago, it might have been reasonable to inform consumers of the one or two major privacy laws which might apply based on their residence, and to point them to that law for more details. But today that becomes unworkable.

To reason

Organizations need to prioritize the privacy laws they align to and notify consumers of, while being aware of what is out there. Prioritize the privacy laws based on where one is headquartered, have offices, and where significant populations of customers exist. Or prioritize based upon the most stringent and resolve to comply with those.

As organizations develop privacy programs, policies, and notices, the touchstones should be logic and reason. We should assume privacy regulators and enforcers will be guided by the same logic and reason and will not seek "gotcha" type enforcement actions. They are busy too.

As documents are crafted and communication is delivered to employees and customers, the benchmarks are clarity and transparency. The organization should not need a legal opinion to interpret their own policies, and consumers should not need one to interpret privacy notices.

The number of consumers who will read your privacy notice is close to zero, but that's not the point. It is a promise to the consumer and regulator that needs to be kept. A clear privacy notice and policy aids both organization and consumers.

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 manage information assets. His latest book is "Policies and Procedures for Your Organization" (2024). 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 October 16, 2024.