ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Product Privacy Done Right

Technology, Privacy, and eCommerce

Banner artwork by Viktoria Kurpas / *Shutterstock.com*

What is privacy?

The International Association of Privacy Professionals (IAPP), a respected community for global privacy practitioners, has a useful glossary of definitions for all things privacy related. The IAPP refers to an influential 1890 Harvard Law Review article by Samuel Warren and Louis Brandeis, who later became a Supreme Court Justice, that famously defined privacy as “a right to be let alone.”

> ... [T]he right of individuals to "determine for themselves, when, how, and to what extent information about them is communicated to others."

In the context of information privacy, in particular, the usage of data relating to individuals (aka “data subjects” in General Data Protection Regulation [GDPR] parlance), and specifically the “identified or identifiable living individual to whom personal data relates,” this generally refers to the right of individuals “to determine for themselves when, how, and to what extent information about them is

communicated to others.” Businesses often have a related concern: They also wish to control the processing and use of their confidential information. These are often treated in concert when building privacy-respectful products.

This concept of information privacy is particularly relevant to data subjects in today’s highly connected environment, in which many peoples’ entire digital lives are carried everywhere with them on a mobile device and is accessible from anywhere in the globe through cloud-based networks.

How does privacy relate to security?

For most practical purposes, privacy and security are two sides of the same coin, and they are often closely related in the minds of data subjects. The IAPP has a useful discussion of the difference between privacy and security, where privacy relates to controls, procedures, and guardrails around the usage of user data relating to a data subject, and security relates to preventing unauthorized access to this personally identifiable information.

Data can be secure but not private, depending on controls, procedures, and guardrails. Artwork by Brian A. Johnson / *Shutterstock.com*

This security approach follows the CIA triad of confidentiality, integrity, and availability, including using techniques such as firewalls and cloud security in the online world and locked filing cabinets in the offline world. Security also involves preventing misuse of the personally identifiable information in

the event it is accessed (e.g., using encryption, compartmentalization of information, etc.). In layperson's terms, privacy is generally about "what someone is allowed to do with my data" and security is generally about "what attackers have the capability to access and make use of my data, and in what ways."

> Privacy is about "what someone is allowed to do with my data" and security is about "what attackers have the capability to access and make use of my data, and in what ways."

Data can be quite secure but used in inappropriate ways can be inconsistent with privacy concerns. For example, certain regimes have quite securely kept secret files or dossiers on individuals that they used without consent to infringe on human rights of certain groups, or to embarrass and deter political dissidents.

Similarly, data can be protected by privacy rules while remaining poorly secured. For example, in the United States, a table of healthcare information (protected under the Health Insurance Portability and Accountability Act [HIPAA] in the United States) or financial information (protected under Gramm-Leach-Bliley Act [GLBA] in the United States) relating to individuals can be stored in an open S3 bucket on the cloud. Secure? No. But the privacy rules remain in place, though poorly enforced.

In many situations, even though there are strong legal obligations in force relating to the privacy of personal information, there is often insufficient security to protect that personal information.

What is privacy by design?

Privacy by design is closely related to the concept of data protection by design. Specifically, designers of products or services that process personal information of data subjects are "...encouraged to take into account the right to data protection when developing and designing such products." In practical terms, this means that designers and architects of information-based products and services should build privacy protections into their products and must make privacy the default option for their products to ensure that personal data is protected.

Where did privacy by design originate?

The concept of "privacy by design" initially stemmed from the efforts of Ann Cavoukian, the information and privacy commissioner of Ontario, Canada. This concept, which began taking shape in 1995 through collaborations with various partners, was further elaborated during the 2009 workshop titled "Privacy by Design: The Definitive Workshop."

What regulations require privacy by design?

Companies and organizations that are established in the EU, or that target residents of the EU, are subject to the GDPR. Artwork by Ivan Marc / *Shutterstock.com*

The GDPR requires privacy by design and by default. Specifically, Article 25, titled “Data Protection by design and by default,” and Recital 78 — which notes that “the controller should adopt internal policies and implement measures which meet the principles of data protection by design and data protection by default” — clearly state this.

Why is this relevant to customers of security providers?

Companies and organizations that are established in the European Union, or that target residents of the European Union, are subject to the GDPR. This is referred to as the extraterritorial effect of GDPR, under which Article 3 defines the extraterritorial effect under the Establishment criterion via Article 3(1) and under the Targeting criterion via Article 3(2).This means that a provider of tools or services that are used by European Union residents, or process the personal information of European Union residents, are subject to the GDPR. Similarly, this also applies to UK residents under the UK GDPR.

Why does privacy by design matter in the context of security?

Security is intended to prevent access, by persons without permission (i.e., an attacker), to information or physical property. However, if the attacker does manage to bypass security controls and access the underlying information, then having the right design approach can greatly reduce the scope of both security and privacy violations which can occur, sometimes referred to as limiting the "blast radius." Security is about what's possible to do with the data, and privacy is about what is the right thing to do with the data. You need to consider both when designing products or services.

Service and software providers should consider privacy through the product lifecycle and in practice, including how products are built. Artwork by Terrance Emerson / *Shutterstock.com*

In particular, a designer of products or services which processes personally identifiable information should endeavor to follow the principles below, which were outlined originally by the Office of the Information and Privacy Commissioner (IPC) of Ontario, Canada:

- The design should be proactive, not reactive, and consider privacy concerns up front in the design of products and services. Similarly, techniques used should be preventative to avoid a privacy incident, rather than just reactive. Reactive tools are certainly helpful and can provide a backstop in the event of a security or privacy incident, but ideally privacy should be considered as part of the initial design.

- Privacy should be the default setting, meaning that the options as initially presented to the user should be the most privacy-preserving options (if such exist), which a user can then choose to change if they so desire.

- Privacy should be embedded into the design from the get-go, and not "bolted on" after the fact.

- Privacy should be additive to the design functionality and security, rather than detract from it. While tradeoffs may be necessary in practical terms, the goal is to keep both security and privacy at the forefront of any decisions.
- Privacy should follow the entire lifecycle of data, from initial collection to final disposal.
- The privacy techniques used should be open and transparent, and subject to independent verification.
- User-centric privacy should be a key element of the design, where the privacy interests of the users are protected by default.

By taking these steps, the designer of products and services that process personally identifiable information can demonstrate both their intent and commitment to privacy by design and by default.

Privacy by design in software and SaaS security

As providers of products that help secure customers' most critical data and information assets, software and cloud security providers should take care to design products that protect customers' information and, importantly, do not cause additional risk to our customers.

The authors' philosophy is that we should strive to make customers more secure and more private, both in the products used by the customers, and the internal process for supporting those customers.

Offerings that utilize SaaS technology must take extra precautions to design secure products. Artwork by venimo / *Shutterstock.com*

Privacy by design in product offerings

The authors' approach is to ensure that products, services, and solutions are all designed to ensure that privacy is built into products and how those products are delivered, to protect both our customers

and *their* customers. It is key to architect products from the ground up to incorporate privacy by design and by default as keystone features. A key aspect here is to minimize the risk of customer data leaving the customer environment.

In practical terms, products should be designed with a strong privacy ethos at the core, with privacy designed in from the start. Earning customer trust starts with respecting and protecting the privacy of customers' information and that of their customers also, as well as robustly securing it from threats and attackers both from the outside and the inside.

Privacy by design in internal processes

Service and software providers should consider privacy through the product lifecycle and in practice, including how products are built. Privacy is never a job "done." Providers should consider privacy both during the development of new features as well as when determining how to continue adding new privacy-specific enhancements to existing products. One example of applying privacy by design is in operating the business; it is recommended to undertake a privacy and security assessment on all new vendors as standard, as part of the procurement vendor onboarding process.

Why does this matter to customers and prospects?

Customers care deeply about both the security and privacy of the data they hold. In many cases, customers are processors of personally identifiable data — even personal health information, financial information, or other particularly sensitive data — on behalf of their own end-customers, who are often data controllers. Where customers are processors (or subprocessors), they are obligated to have appropriate technical and organizational measures to protect such data. If they engage an additional organization to process their end-customer's data further (another sub-processor in effect), they are generally required to inform and provide a right of objection to the data controller.

By architecting solutions with privacy by design implemented from the start, and avoiding removing customer's underlying data outside of the customer environment, this can avoid the need to be listed as a sub-processor, thus providing a benefit to customers and reducing their compliance burden.

Building privacy and trust in every step

We encourage customers, partners, and users of software and services to consider privacy as an important feature in their security solutions. It is necessary for building the trust of users and demonstrating respect for their personal data, as well as for demonstrating compliance with global privacy regulations.

Lea Kissner

CISO

Lacework

Lea Kissner is the CISO of Lacework and on the board of USENIX. Kissner works to build respect for users into products and systems through deeply-integrated security and privacy. Kissner was previously the CISO and head of privacy engineering at Twitter, global lead of privacy technology at Google, came in to fix security and privacy at Zoom, and CPO of Humu. Kissner earned a Ph.D. in computer science (with a focus on cryptography) at Carnegie Mellon University and a BS in electrical engineering and computer science from UC Berkeley

Alan Mulvaney

Senior Manager, Legal

Lacework

Alan Mulvaney specializes in the negotiation of commercial contracts at Lacework and has more than 20 years IT industry experience, having previously worked for Pure Storage and IBM. Mulvaney has in-depth knowledge and experience in the privacy-sensitive markets of Germany and France and also holds key insights into the concerns of other highly privacy sensitive customers, especially in highly regulated industries. Mulvaney has a BBS degree from Dublin City University, in addition to a qualification in Data Protection.