ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Future-Proofing Your Privacy Program

Technology, Privacy, and eCommerce


FUTURE-
PROOFING
YOUR
PRIVACY
PROGRAM

CHEAT SHEET

- ***FIPPs.*** While there is no global standard for privacy laws, many of them share key requirements based on Fair Information Practice Principles (FIPPs).
- ***Obligations.*** A company that collects and uses information about people is obligated to know what, where, and why personal information is collected and used; identify with whom it is shared; secure it from breach or misuse; service requests from individuals about their information; produce personal information for legal obligations; and selectively delete it.
- ***Approach.*** When designing a privacy program to withstand evolving regulations, first decide if you will tackle everything at once or start small and incorporate more areas as your

organization becomes more agile.

- ***Capabilities.*** You will need to explore the following privacy capabilities: dynamic personal information identification and mapping, security controls and information classification, privacy-enabled incident response, scalable and efficient processes for Subject Access Requests, and a compliant process for selectively deleting personal information.

Companies have faced Europe's General Data Protection Regulation (GDPR), then the California Consumer Privacy Act (CCPA), and now a seemingly endless patchwork of new and proposed privacy laws. Instead of perpetually redesigning the privacy wheel to accommodate each new or potential requirement, companies should consider "future-proofing" their privacy programs by developing a core set of flexible personal information management capabilities that can be applied to both current and upcoming requirements.

Privacy rules are getting more complex

Privacy did not start with the EU's GDPR. Since its passage in 2016, though, governments worldwide have been passing laws regarding privacy and data protection that span the spectrum: some mirroring GDPR (such as Brazil's General Data Protection Law) and some creating wholly different areas of responsibility (such as China's Cybersecurity Law). The CCPA, passed in 2018, sits somewhere in the middle. Additionally, data security laws, mostly in the form of data breach notification requirements, have been around for almost 20 years.

And it is not stopping. The District of Columbia just passed an amendment to its security breach notification law, which among other changes added biometric, genetic, and medical information to the list of data elements that would trigger a notification. States throughout the United States are adding privacy and data protection requirements to their insurance and financial codes, and we are still seeing laws proposed globally — for example, the Indian Personal Data Protection Bill 2019 is under consideration in the Indian Parliament.

To summarize: Companies face a patchwork of laws, there are more requirements seemingly every day, and there are no global standards yet on the horizon.

So, what do you do?

All privacy laws share key requirements. Privacy laws worldwide are generally based to a greater or lesser extent around the same set of principles, generally referred to as the Fair Information Practice Principles (FIPPs). The FIPPs are written as individual rights and are generally summarized as Transparency (sometimes called Access), Individual Participation (sometimes called Consent or Choice), Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. You can see these principles in most of the data protection laws.

A company that collects and uses information about people (whether or not it is individually attributable) has a set of obligations related to those rights:

- Know what personal information you have, and where, and for what purpose it is being

collected and used.
- Be able to identify with whom you have shared personal information.
- Secure personal information and protect it from breach or misuse.
- Be able to service requests from the individual about their personal information.
- Be able to produce personal information as necessary for other legal obligations.
- Be able to selectively delete personal information.

An entity will need to have some minimal privacy functions to meet these obligations.

Future-proofing your privacy program

To enable your company to honor an individual's data rights, and to meet your company's obligations with respect to those rights, you will need to explore the following privacy capabilities.

Dynamic personal information identification and mapping

To meet your first obligation (know what you have) and honor the data rights of the individual, you must identify the personal information in your organization's possession, custody, or control. You must also identify the purpose for collecting the information and how it is used, and with whom you have shared the information, including the purpose for that sharing.

> **By knowing what information you have, and the ways it flows through your organization, you can then determine the sensitivity of various data stores and set expectations for each sensitivity class.**

The best way to collect and maintain this information is through a personal data inventory and a data mapping exercise. Generally, this is an interview-based process, which collects information from various business units that use personal information, since they are in the best position to know what information they use on a regular basis. You should supplement this with interviews with the IT organization, as they will have the database administrators who will know what is in the databases. You'll also want to talk to IT about the repository capabilities for processes like access control, targeted deletion, data encryption or masking, and the like. These interviews will help you develop your data flow to demonstrate how personal information enters, moves throughout, and leaves your organization. System owners should also maintain documentation of upstream and downstream processes and repositories.

Security controls and information classification

Once you understand what you have, you must then determine how to secure the information, and protect it from misuse. Information security as a general matter is usually not the purview of an organization's privacy team, nor should it be. However, the privacy function must work hand-in-glove with the security function. It is not entirely accurate to say that "you can't have privacy without security," but it is absolutely accurate to say that the two functions are deeply intertwined. The privacy organization must work with the security function to understand the security controls available within the organization, and the security function must work with the privacy organization to understand what controls should be applied and where.

Additionally, with the information security organization, review the laws that apply to your company.

Many states (if you do business in the United States), such as New York, Massachusetts, Delaware, and California, have information security requirements throughout the statutes, as well as state-specific privacy protection laws; reviewing those with the information security organization to assure a mutual understanding of the requirements and how your organization can meet those requirements will be helpful.

It is not possible for security and privacy to be embedded in every project throughout an organization, irrespective of its size; therefore, it is important to provide tools for the company to use. Information classification is one such useful tool. By knowing what information you have, and the ways it flows through your organization, you can then determine the sensitivity of various data stores and set expectations for each sensitivity class. One simple example is as follows:

You can see how and why information classification is helpful — it creates an understanding throughout the organization of the information that must be protected and creates an understanding of the agreed-upon ways to protect it. When personal information is specifically detailed in and among the classifications, it helps to create an understanding that not all personal information is protected the same way. It may be useful to create a classification chart specifically for the personal information collected and used by your company, identifying each element and its classification. Your personal data inventory and data map will be a great resource here.

Privacy-enabled incident response

Creating and managing a privacy incident response plan will also require significant partnership between legal and information security. Incident response can no longer be managed exclusively by the information security organization; because of the potential for meaningful fines and regulatory scrutiny, incident response is now very much a legal issue.

A privacy incident response plan can be fairly simple or extremely detailed. Create an appropriate incident response plan for your response team that addresses, at a minimum, the following:

- The members of the incident response team, and contact information for them (this should be readily available to the entire organization)
- How and when members of the organization should contact the incident response team (this also should be available to the entire organization)
- How the incident response team categorizes incidents and responds to them (“triage”; not every incident is created equal)
- A discussion of which group performs what function during an incident (note that a RACI (“Responsible / Accountable / Consulted / Informed”) matrix works well here)
- Contact information for any third-party incident response service providers (outside counsel; insurance brokers, incident management provided by insurance, forensic investigators, etc.)
- Decision process for when to escalate from the day-to-day operations team to include more senior/executive leadership or the board of directors
- Contact information for any regulators which may need to be notified, and the process and timelines for that
- Any jurisdictional or industry requirements that create specific considerations (example: a US healthcare organization regulated by HIPAA has two different notification timelines, depending on the number of persons impacted)
- Other information that can be useful, such as cybersecurity coverage limits, critical third-party partner notification protocols, sample notification templates, etc.

No matter what kind of plan your organization creates and maintains, it is also critical to review the plan periodically with the entire organization, and to test the plan regularly with involved employees, including executive leadership and the board of directors. Having everyone understand how and when they will be notified in the event of an incident, and who is responsible, will go a long way to making sure that any incident is handled appropriately and meets the deadlines set out in the various laws.

> **Now that you have created the protections for the information you collect and use, it is time to consider how to support the individual's exercise of their data rights.**

Creating a scalable and efficient process for meeting Subject Access Requests

Now that you have created the protections for the information you collect and use, it is time to consider how to support the individual's exercise of their data rights. An individual has a right under many existing and proposed laws to request a company to provide them with certain specific information about the individual. These rights vary from law to law, so a detailed discussion of each right is not appropriate here. However, one thing all the laws have in common is an expectation that the company will know the information they have about the individual, and will be able to access and produce it upon request of the individual.

Additionally, none of the laws giving individuals these rights specify any difference in the exercise of those rights between information in databases ("structured data") and information in things like email or word documents ("unstructured data"). For example, GDPR does provide that the requirements only apply to information which is "part of a filing system," but that does not rule out paper; and CCPA does not mention it at all. Further, GDPR lays out the process for rejecting a request for access if the information contains information about other data subjects, which likely would not happen in a structured system. Therefore, it seems likely that each of these laws contemplates some form of unstructured data search and production in the event of an appliable request.

Information classification

SENSITIVITY	EXAMPLE	TREATMENT
PUBLIC	Approved, issued press releases; information published on our website	None
INTERNAL Information not approved for external publication	Outlook calendars, company policies, project documentation	Control access to the information; note as “internal” on any documents
CONFIDENTIAL Business information that could negatively impact the company	Pre-release product information, contact lists, sales targets	Control access to the information; note as “confidential” on any documents; non-disclosure agreements in place if exchanged with third parties
SENSITIVE Information that could create regulatory or enforcement action if released	Pre-release financial information; personal information that triggers notification in the event of a breach, like Social Security numbers or driver’s license numbers	Control access to the information; note as “sensitive” on any documents; non-disclosure agreements in place if exchanged with third parties; encrypted in transit and at rest

Searching each individual data store every time your company receives a request is absolutely unscalable and inefficient. To avoid having to do this, you must develop a standardized process to receive and track these requests, and make sure that they are being handled in a timely manner. A ticketing system (such as ServiceNow) can work very well for this process and can also be set up to provide special processes like escalation notifications as the deadline gets closer. Once the process

is developed, you must train your employees how to recognize these requests and how to submit a ticket for them. You cannot make it too laborious or time-consuming — or your employees will not do it.

Design a scalable process for producing personal information

Similar to the need for a scalable, efficient process for responding to access requests, your company will also need a process for producing specific requested personal information, whether in litigation or as a response to a request for a copy of their information from a data subject. It will be important to reference the specific laws in your jurisdictions when creating this process, as each law provides for a different set of exceptions to this requirement.

Create and maintain a compliant process for selectively deleting personal information

Most companies have records retention schedules. There are a fair number of schedules that only cover personal information of employees; those that cover other personal information, such as retention of customer information, are frequently not actively enforced.

Because many personal information laws provide that an individual can request that a company delete their specific personal information, if your company does not already have a process to delete specific information, rather than retiring entire tables, databases, or servers, it is time to create one. There are exceptions to the deletion request in each of these laws, but there will be data subjects who are able to make this request and for which exceptions do not apply. (Note that CCPA, particularly, requires an entity to delete information upon request unless the information meets one of nine exceptions.)

There are other good reasons to begin enforcing not just specific, targeted deletion, but a records retention schedule as a whole:

- If a company does not have personal information in its possession/custody/control, the information cannot be breached.
- Having a records retention schedule that is not properly enforced can create significant liability in litigation and discovery.

There are likely some legacy technologies still in use at your company that cannot delete specific information; it is important to know what those systems are, and what information they maintain or have access to, in order to both properly protect the information and to be able to appropriately respond to a data subject’s request to delete the information. As your company looks to replace those technologies, however, it is important that the legal team, in concert with information security and procurement, work to acquire new platforms that can handle these kinds of targeted requests.

Balancing your risk and maturity across all privacy laws

Once you have accomplished these tasks, it is time to look at your organization’s ability to balance risk across all the privacy laws that apply to your company, and to determine both your entity’s current maturity as well as its target maturity. This is not a “check the box” exercise; this is ongoing program management and will help your organization stay ahead of the changing laws.

Searching each individual data store every time your company receives a request is absolutely unscalable and inefficient. To avoid having to do this, you must develop a standardized process to receive and track these requests, and make sure that they are being handled in a timely manner.

First, determine what should be in or out of the assessment's scope. Are you going to tackle everything at once, or will you start small and work other areas in as your organization changes and becomes more privacy-agile? One example would be the requirement under GDPR to perform a Data Protection Impact Assessment if an action could pose a high risk to subject rights and freedoms. Will your organization only perform a DPIA for those activities that will specifically impact EU persons, or will you institute the DPIA requirement enterprise-wide? There are good arguments for either decision, so the answer will be based on your entity's risk tolerance and its other processes.

You will also need to consider how to handle personal information you receive from or send to third parties. Most (although not all) of the privacy laws currently in place have a concept of "data controller" or something similar, and "data processor" or something similar — that is, an entity responsible for making decisions about the information, and another entity that carries out the instructions of the first entity. While this makes sense in theory, in practice, it tends to be much more complicated, and not all entities fall into neat boxes. Therefore, your company will need to determine how it will handle requests to share information with third parties which may not fall neatly into "data processor" (or "service provider," to use the CCPA term). You will want to develop a review process that incorporates not just an assessment of the security of the third party, which of course you already look at, but also the data use and protection practices of the third party. Do their contract terms seem to suggest that once the data is sent to them, they consider it to be their own to do with as they will? Do they have a process for responding to your request for information they may hold about your customer? Or alternatively, if your entity is the service provider, how do you manage the information you receive from your clients?

Also consider records management. In addition to the records retention schedule work, you will need to do to specifically respond to a request to delete, consider the broader management issue and address your onsite and offsite paper records. For many entities, sending their boxes of paper offsite is the mental equivalent of dropping them into a black hole, never to be thought of or seen again. With the new data protection laws, that may result in regulatory action against the company that could have been managed.

Review whether eDiscovery processes trigger new privacy burdens. Is your company based in the United States, but with information about EU persons? If so, make sure you have a process for addressing production under litigation while keeping the GDPR requirements in mind.

Conclusion

Building core capabilities will prevent you from having to redesign your privacy program with every new law. There will still be local exceptions that need to be addressed, but if you start with these basic, common requirements, you will be able to manage those differences without creating a brand-new effort every year.

"Cyberthreats in the Age of COVID-19" on *ACC*

Throughout this article, terms like "data subject," "personal information," etc., are used without reference to their specific legal meaning, unless so stated. For example, a "data subject" is not specifically an EU person; it is simply the subject of the information.

ACC EXTRAS ON… Preparing for privacy regulations

ACC Docket

Privacy Now: A Dedicated Data Discussion (Jan. 2020)

Are You Really Ready for the New Privacy Laws? (Sept. 2019)

5 Questions Corporate Counsel Should Ask About Privacy Assessments (May 2019)

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT WWW.ACC.COM, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

Gail Eagan

Senior Vice President and General Counsel

Arbella Insurance Group

Gail Eagan is senior vice president and general counsel of Arbella Insurance Group, a customer-focused regional property and casualty insurance company headquartered in Quincy, MA.

Kerry Childe

Senior Consultant

Contoural, Inc.

Kerry Childe is a senior consultant with Contoural, Inc. She has almost 20 years of information counsel experience, leading the development and implementation of enterprise-wide privacy and

information protection programs to protect company information. She has previously worked as senior corporate counsel for a Fortune 100 company and senior privacy and regulatory counsel for a nonprofit student lending organization.