PrivacyStudio.com
The Art of Information Management

THE PRIVACY CASE BOOK:

A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks

CHAPTER 9
Strategies for Managing Enforcement Risks

Margaret P. Eisenhauer, Esq., CIPP
Privacy and Information Management Services – Margaret P. Eisenhauer, P.C.

Chapter Nine
STRATEGIES FOR MANAGING ENFORCEMENT RISKS

Understanding and Balancing Risks

Companies invest significant time and effort in complying with laws and minimizing enforcement risks. The investments allow companies both to avoid costly and disruptive claims and also to protect their reputations and brands. However, companies must also consider the costs of compliance. These costs may manifest themselves as bottom line expenses (such as fees paid for legal advice, compliance tools and employee training) as well as top line costs associated with the loss of flexibility that results from strict information management controls.

In order to find the "sweet spot" where legal risks around privacy laws are managed without excessive cost or constraint on the business, companies must approach compliance program development thoughtfully. The goal is to manage the legal risks appropriately, without spending too much on compliance or foreclosing necessary or desirable opportunities to leverage personal information.

The same balance is required exist on the security side. For example, a company can require multiple authentication steps to help ensure that it knows its customers. If these added steps increase the transaction times, however, the customer may reject the transaction in favor of a more efficient provider. Similarly, consumers may be comfortable being asked to show a photo ID to complete a credit transaction, but they may balk at a request for biometric identity confirmation, such as fingerprint. They may believe that the added security is too invasive of their privacy. Companies must consider all the trade-offs.

The Role of the Privacy Professional

The task of finding the right balance for an organization is typically given to a privacy professional, such as a chief privacy office or privacy lawyer. The International Association of Privacy Professionals (IAPP) defines a **privacy professional** as:

> *A leader who understands the technical, legal and operational aspects of gathering, handling and securing personal data, and who can establish and maintain a comprehensive strategic vision for handling all personal data of employees, customers and suppliers of an organization in a manner that is legal, secure and ethical, from the point of acquisition through the point of disposition, thereby gaining public trust in the organization's role as custodian of such data.*[158]

Effective privacy professionals rely on a combination of good instincts and sound processes to achieve the right risk balance. For example, successful privacy professionals will rely on processes to ensure that proposed data uses are consistent with legal requirements and expectations. They weigh investment plans against the probability of future changed expectations. They then build consensus around the results of the processes, offering solutions that meet corporate goals in a manner consistent with the corporate culture.

Privacy professionals must work collaboratively with corporate leaders, security professionals and legal counsel to develop formal, balanced information management programs that manage the legal compliance risks. The information management program should do more than manage enforcement risks, however, it should provide a framework that enables the company to achieve a variety of information policy and business goals by helping the company build trust with its employees, customers, business partners and regulators. The privacy program can help guiding marketing initiatives, business planning and advocacy. It should also enable the company to anticipate business threats, such as the requirements of new laws, and consumer and policy-maker concerns.

To find the right balance, privacy professionals start by developing a list of specific information policy objectives, then they create a holistic, enterprise-wide set of business standards and tools that enable the company to realize the defined objectives. This approach allows the company to meet compliance objectives while maintaining as much flexibility within the organization for the legitimate use of personal information as needed for the company to achieve both short and long term business goals. This approach also allows the company to make informed decisions about the potential risks and returns on its investments in information technologies, outsourcing and customer relationship management programs. By imposing a formal process approach on procedure development, privacy professionals also help their companies anticipate future changes both in the regulatory environment and in their business needs.

Most importantly, this approach also allows the company to articulate its information policy values, which are the cornerstones of trusted relationships. Many companies have discovered that they can gain real top and bottom-line revenue advantages by being good, privacy-sensitive corporate citizens. By considering all of the issues related to the data collected and used by the company, the company is well-positioned to leverage its program to build consumer and business partner trust.

Creating an Information Management Program

Privacy professionals must assist their organizations in thinking about privacy policy development in a formal, objective way, meeting defined policy goals as well as preserving business flexibility. Privacy

professionals must also understand and anticipate future changes both in the regulatory environment and in their companies' business needs. To achieve these objectives, companies should consider **four distinct phases of privacy program development: (1) discovery, (2) construction, (3) communication and (4) evolution**.

PHASE 1: DISCOVERY

The first step in developing a privacy compliance program is to gather the necessary information. In particular, as a privacy professional, you must:

- Recognize the specific regulatory requirements, industry guidelines and contractual requirements that apply to your business operations (and, if you are a service provider, those of your customers);
- Analyze your existing information management policies and procedures and privacy governance framework;
- Consider the corporate culture and management level of risk tolerance;
- Consider peer company practices and related-industry best practices, if applicable;
- Identify existing and planned business relationships that involve significant transfers of personal information;
- Understand precisely how your use of information furthers your current and future business goals, considering not only obvious goals (such as planned product marketing) but other goals, such plans to consolidate data centers or outsource corporate functions; and
- Prioritize the compliance risks based on the intersection of laws and enforcement trends within the scope of your operations, taking into account your clients' sensitivities.

PHASE 2: CONSTRUCTION

Once you understand your company's current practices and goals, you can help your company find the best way to achieve compliance goals, address employee, customer and regulator expectations, and meet business goals. The compliance program construction phase consists of:

- Formal articulation of company privacy and information management principles or values;
- Privacy and security policy development;
- Development of process requirements, such as standard operating procedures, and associated controls and metrics;
- Development of auditability criteria, so the company's compliance with its procedures can be evaluated periodically;
- Creation of guidance materials, such as recommendations; and
- Incident response planning.

Depending on the organization's business and the regulatory regime it faces, the policies and procedures prepared may be comprehensive, covering (for instance) all employee data handling, or specialized. Specialized policies might cover processes such as maintaining opt out lists for direct marketing, developing appropriate security for customer financial or medical records, executing proper contracts to authorize international data flows, or publishing an online privacy notice if data is collected over the Internet.

During the construction phase, the privacy program should be socialized at all levels of the company. The privacy professional should take steps to confirm that planned procedures will not unduly burden the business; where possible, existing processes should be respected and leveraged. Additionally, the privacy professional must have broad executive –level support for the program. This is necessary to ensure that appropriate resources will be available to support a successful program launch.

PHASE 3: COMMUNICATION

Once your company has developed and implemented an information management program, it is essential that you communicate the elements of the program to internal and external audiences.

Privacy professional should never underestimate the important of training. Internal audiences must be trained on the procedures and processes that are established, and individuals must be accountable for

complying with the company's program. More importantly, the company's information policy values need to be shared with all company decision-makers and consumer-facing employees, so that they are able to use these values to shape the messages given to the company's customers and other stakeholders.

Consumer and/or business partner education may also be critical. The primary goal of a written privacy notice is to educate external audiences about the actual practices of the company. As we know from the cases presented in Chapter 2, privacy statements must accurately reflect the company's practices, and it must not mislead readers, even by omission. The privacy statement also provides a basis for accountability of the organization with respect to its practices.

With regard to all privacy statements, there is a good deal of consensus as to what types of organizational practices the privacy statement should address. At minimum, the privacy statement should include a clear notice as to what personal information is being collected, how the information will be used, and what types of entities to which the information may be disclosed. Additionally, the privacy statement should inform readers about their legal rights, such as rights of access, as well the choices (if any) that the individual has with respect to the intended uses and disclosures of the personal information. For example, as discussed in Chapter 5, if the personal information is to be used for direct marketing purposes, companies are generally expected to offer individuals the ability to opt out of the communications. Finally, the privacy statement should include contact information for the company.

PHASE 4: EVOLUTION

Finally, privacy professionals must understand that a compliance program is not something that can be built and then put on a shelf. Privacy laws are changes, and the enforcement risks are growing. In order for the program to effectively manage risks over time, the company's policies and procedures must evolve. Accordingly, privacy professionals should formalize periodic reviews of the privacy policies and procedures. Employees should be periodically retrained as well.

Privacy professionals must monitor legislative developments and regulatory trends, as well as shifts in consumer or regulatory expectations, new industry standards, or other similar developments. The Evolution Phase is designed both to verify ongoing compliance with your company's published procedures and also to position the company to proactively respond to changes that affect your information handling processes in the future.

Conclusion

Both risk management and good corporate citizenship require that organizations develop policies for the appropriate collection and use of personal information.

Privacy professionals must assist their organizations in thinking about privacy and security policy development in a formal, objective way, striving to help the company meet risk management and legal compliance goals as well as to preserve business flexibility. Successful privacy professionals must also understand and anticipate future changes both in the regulatory environment and in their companies' business needs. In order to do this, privacy professionals must be conversant in all of the business, legal, economic, social and political factors that may be relevant to the company's situation.

By imposing a formal process approach on procedure development, companies can maximize the success of the information management program because the structure of the program will permit the companies to anticipate future changes both in the regulatory environment and in their business needs. Additionally, a company can use a well-designed information policy program to develop consumer and business partner trust, and to make better investment decisions about technology infrastructure investments, resulting in top and bottom-line revenue advantages for the organization.