Developing a Privacy Compliance Program

JUSTINE GOTTSHALL, INFORMATION LAW GROUP, AND ADAM C. NELSON, IBM SECURITY SERVICES, WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

Search the Resource ID numbers in blue on Practical Law for more.

A Practice Note addressing key considerations in developing a privacy compliance program. This Note discusses the key drivers for developing a privacy compliance program, options for structuring the privacy office, and developing a privacy compliance framework. It also discusses privacy by design and key resources that businesses may consult in developing their privacy compliance programs, such as the fair information practices principles and privacy guidance issued by the Federal Trade Commission (FTC).

Complying with global privacy regulations that govern the use, collection, and treatment of individuals' personal information is a significant and growing challenge. Until recently, global privacy compliance has been mostly an issue for large multi-national firms, but with the continued expansion of internet technology, like cloud storage services, global privacy compliance is fast becoming a concern for companies large and small. International privacy compliance has historically focused on complying with the requirements of laws implementing the European Union Directive on Data Protection of 1995 (95/46/EC) (EU directive). This EU focus will likely continue as companies consider how their programs must evolve to comply with new legislation replacing the EU directive by May 25, 2018 (General Data Protection Regulation ((EU) 2016/679)). However, privacy laws and regulations exist throughout the world, including relatively new laws and regulations in Asia, Latin America, and Africa. In addition, while the US has not enacted a comprehensive data protection law like the EU member states, despite some popular misconceptions, it does have an enhanced privacy regulatory environment that continues to grow.

In this compliance environment, companies must develop a data privacy governance process or compliance program. Companies must attain skilled professionals to lead their data governance activities, and these professionals must create a defined vision for data governance. Privacy and data governance in turn must become a fundamental component of the corporate risk management strategy.

The specific configuration of any privacy compliance program depends on the company's unique needs and requirements considering business needs, internal structure, and organizational culture. The company must first determine its primary business risks, then craft a plan to minimize those risks and address compliance in a systematic way.

This Note discusses:

- The importance of having a privacy compliance program and team.
- Structuring a privacy office.
- The privacy team's roles and responsibilities.
- Key considerations in developing a privacy compliance program.

PRELIMINARY CONSIDERATIONS

In considering the goals, requirements, and structure of a privacy program, the party responsible for designing and implementing the program should first understand and assess:

- The key drivers behind creating a privacy program (see Key Drivers).
- Basic information about the business's operations that informs the business's specific needs for developing the program (see Operational Considerations).

KEY DRIVERS

Developing a formal privacy program should address five key issues that drive program creation:

- **Overall data governance.** Because of the increased collection, use, and storage of data, particularly personal information, businesses must set up formal programs to manage that information.
- **Globalization.** Technology has allowed businesses to rapidly increase their global reaches and interface with international customers, often without a physical presence in the jurisdictions where they serve customers.

- **Increased regulation.** As the collection, use, and storage of personal information has grown, countries throughout the world have turned their attention to regulating those activities.
- **Growth of vendor networks.** The growth in the use of vendors has increased the need to manage an extended network of suppliers, contractors, consultants, and other third parties with access to corporate data.
- **Increased sensitivity.** With the increase in data collection, the threats to that data have grown. The proliferation of data breach incidents and social profiling has made employees, consumers, and customers sensitive to the risks associated with unauthorized disclosure of personal information.

OPERATIONAL CONSIDERATIONS

No one-size-fits-all template exists for privacy programs. For example, the privacy considerations differ for a manufacturing company operating in 30 countries and a small US-based business developing a mobile application that targets US children. When a company begins the process of developing a privacy program, it should develop a basic understanding of certain key considerations that drive the program's nature, structure, and focus. Privacy requirements typically differ depending on the nature of the company's:

- Industry and business.
- Data and the types of projects or tasks the company conducts.
- Geographic footprint.

To guide the process at the outset, a company should gather basic information regarding:

- The personal information the company collects, including whether it collects:
  - sensitive information, such as Social Security numbers or health information; and
  - information on employees or consumers, or both.
- How the company collects personal information.
- The purposes for which it collects personal information.
- Who has access to the personal information.
- How the company stores and disposes of data that includes personal information.
- The greatest risks the company faces to its data.
- Geographic issues related to its business operations and data, such as:
  - the location of physical facilities, employees, servers, or other assets;
  - whether the company uses cloud storage for data; and
  - the enforcement history of jurisdictions where it operates or has assets.
- Cross-border marketing issues, such as:
  - whether the company directly markets products or services to residents of other countries; and
  - the language used on its website, any mobile application, or any other marketing materials.
- Issues related to marketing and use of data, including the:
  - types of marketing activities in which the company engages;
  - overall collection, use, and sharing of information in connection with marketing activities; and
  - third parties involved in the marketing activities that collect, share, or access data.

STRUCTURING THE PRIVACY OFFICE

The first step in developing a privacy compliance program is to consider how the company should structure its privacy function. Factors that go into determining the correct structure for a particular company include:

- Culture.
- Corporate structure and size.
- Geographic locations.
- Data risks.
- Internal and external resources.
- Operational and business needs.

Regardless of the specific structure a company chooses, an effective privacy function requires that:

- The company view privacy as a key aspect of corporate risk management.
- The privacy team has the power to implement policy and influence decision making.
- Someone within the company own privacy and take the lead on installing compliance initiatives.

A successful privacy program depends on privacy being considered a top-down proposition supported by corporate leaders and ingrained in business operations. The most common senior-level sponsors of the privacy function are the:

- General counsel.
- Chief compliance officer (COO).
- Head of audit.

However, in some companies the chief executive officer directs the privacy function.

PRIVACY OFFICE MODELS

While there are many possibilities for structuring a privacy office, the two most common models are the:

- Chief privacy officer (CPO) (or core team) model (see CPO Model).
- Privacy working group (or privacy council) model (working group model) (see Working Group Model).

For a quick comparison of the two models, see Box: Comparing Privacy Office Models.

CPO Model

The CPO model is the traditional approach to structuring a privacy office and can be scaled to the company's needs. Under this model, one operating unit leads privacy. Depending on the company's size and the jurisdictions in which it operates, in addition to the CPO, the CPO model may also include:

- Country leads.
- Divisional leads.
- An executive steering committee.

For most companies, the CPO model is the best structure as it provides a single person with authority to make decisions and accountability for the program's results.

Working Group Model

Other entities choose to operate on a working group model, where a privacy committee council either:

- Makes all the compliance decisions.
- Shares resources and information to coordinate on privacy issues across the company, though decisions are ultimately made by the various business units.

The working group model may be a successful approach for some companies and tends to work best in companies with different divisions that operate separately. However, over time, it is not as effective as the CPO model for most companies, often because of the members' lack of direct responsibility for privacy. Because privacy is not the core capability of the working group members, they often are not as invested in the success of privacy programs as would be a core privacy team.

KEY PERSONNEL

While there is a great variety in possible titles for persons responsible for privacy within a company, a privacy office or team typically involves one or more of the following staff members:

- Chief privacy officer or data protection officer.
- Privacy director.
- Privacy program manager.
- Privacy analyst.
- Privacy attorneys.
- Regional data protection leads or officers in each jurisdiction in which the company collects data.
- Line of business privacy representatives.

CORE PRIVACY PROGRAM FUNCTIONS

Privacy compliance responsibilities can generally be organized into the following major functions:

- Providing strategic and thought leadership (see Providing Thought Leadership and Corporate Strategy).
- Assembling cross-functional support (see Assembling Cross-Functional Support).
- Developing a privacy framework (see Developing a Privacy Compliance Framework).
- Analyzing legal requirements and developing a compliance plan (see Analyzing Legal Requirements and Developing a Compliance Roadmap).
- Developing privacy policies, processes, and internal controls (see Developing Policies and Internal Controls).
- Dealing with day-to-day operational issues that implicate privacy (see Supporting Business Operations).

PROVIDING THOUGHT LEADERSHIP AND CORPORATE STRATEGY

Because privacy compliance is an ongoing concern, companies benefit from implementing a strategic approach to privacy that considers privacy along with corporate growth and objectives rather than from a responsive posture. To embed privacy in the strategic objectives, the company should develop mechanisms by which the privacy team provides information regarding current and future risks and obligations to:

- Senior executives.
- Security and information technology teams.
- Business unit leaders.

Planning is crucial, but both the privacy team and other senior leaders must understand the need for flexibility given how rapidly corporate objectives, technology, and privacy laws change.

ASSEMBLING CROSS-FUNCTIONAL SUPPORT

Successful privacy compliance programs are built on a culture of compliance, creating an overall awareness within the company of key privacy issues and the importance of addressing them throughout the business as they arise. Privacy is cross-functional and must be coordinated with other stakeholders across the company. Depending on the business's structure, key stakeholders may include:

- **General counsel.** Regardless of whether privacy sits within the compliance or legal function, privacy compliance implicates significant legal obligations. The privacy team should ensure that the general counsel, as the corporate officer ultimately responsible for the company's legal compliance, is engaged and responsive on privacy matters. In addition, some companies have the legal department handle certain legal issues in coordination with the privacy function, such as addressing privacy and security issues concerning vendor contracts.
- **Chief compliance officer.** The CCO works with the privacy team to identify and address the company's privacy compliance obligations. The CCO typically works with the CPO to develop the privacy compliance framework as well as all privacy practices and processes. Because the CPO sits within the CCO's office in many of the types of companies, the CCO's involvement is often most common for:
  - companies in regulated industries;
  - multi-nationals; or
  - companies that otherwise have a strong, internal compliance department (for information on developing a corporate compliance program, see Practice Note, Developing a Legal Compliance Program (4-606-5696)).
- **Chief information officer (CIO).** The CIO works with the privacy team to address the technical issues around privacy compliance and must keep the privacy team informed regarding projects that implicate protected data and may therefore require privacy oversight.
- **Information security or chief information security officer (CISO).** Privacy and security are complementary functions. Privacy compliance cannot be achieved without security and a privacy violation is a key security risk. Therefore, the privacy team should form a close partnership with the security team.

- **Marketing, business development, and sales.** Privacy issues are deeply intertwined with the collection of consumer and customer data and the use of that data for marketing and related purposes. The privacy team must work closely with marketing and sales to ensure compliance with law and corporate policy.
- **Human resources (HR).** Companies collect employees' sensitive data, for example, identification numbers or health information. Laws across the globe apply to the sensitive data an HR department collects, processes and retains. The privacy team must coordinate with HR to identify compliance risks and obligations and to agree on processes and procedures to implement compliance.
- **Records and information management.** The privacy team should work with the records management team to:
  - evaluate the entire information lifecycle; and
  - develop processes and procedures that address privacy risks.
- **Audit.** The privacy team must work with the audit team to ensure the company's policies, procedures and processes are adequate and operating properly and that the company is in practice complying with global privacy laws and regulations (see Monitoring and Auditing).
- **Business unit representation.** The privacy team should have representatives or liaisons in the various lines of business. Business unit representatives help ensure that privacy practices are being implemented and followed across the business and that the privacy team is aware of any privacy issues that arise within the business.

DEVELOPING A PRIVACY COMPLIANCE FRAMEWORK

Privacy compliance depends on developing and maintaining an appropriate framework on which the company collects, stores, processes, and transfers personal data. Not every company needs a finely detailed privacy framework, but every company does need a focus and direction on how it manages and governs data use. Having this focus helps define privacy activities for the privacy team and senior leadership.

While no two privacy programs look alike, as a business's specific nature and its risks drive program development, there are several universal considerations. Specifically, any privacy compliance framework must reflect:

- The company's operations and internal resources.
- The nature of the company's data (see Understanding the Data).
- Legal, regulatory and contractual obligations (see Determining Legal and Program Requirements).
- Key risks to company data (see Performing a Risk Assessment).
- The company's privacy principles.

While gathering basic information about many of these issues is a preliminary matter (see Preliminary Considerations), developing the privacy framework requires a deep dive.

Understanding the Data

To properly approach compliance, a business must thoroughly understand the types of personal data it collects and stores. For a new privacy program, an initial project should be to locate the data or create a data map. As a starting point, the privacy team should understand the following about the data the business collects:

- The types of protected information that the company collects, for example, health or financial information.
- Whether protected data is kept electronically or on paper, or both.
- The location of data, both within the company and as it resides with third parties.
- Countries to or between which the company's data is transferred.
- Data security measures that protect data, including for example whether any data is encrypted, either at rest or in transfer.
- The business unit or individual data owner within the company responsible for any data.

If the resources are available, the business should create a full data map of the data it collects, processes, and stores. A data map can take many forms, but typically consists of a database, list, or graphic representation of information specific to particular subsets of data. In addition to the elements noted above, a full data map should include as much detailed information as possible regarding:

- Data use.
- Data sharing.
- Data storage.
- Data retention process and policy.
- Countries to or between which data is transferred.
- Where the data is collected.
- Third-party access to any data.

A comprehensive data map is extremely useful for legal, compliance, security, and business reasons. However, preparing a complete data map is time and resource intensive and, therefore, many companies do not prepare one. At a minimum, to develop a compliance plan, the privacy office should understand the types of data the business collects and generally where that data is collected and stored.

Performing a Risk Assessment

A risk assessment is a key tool for determining where systems may be vulnerable to a data privacy incident. The risk assessment process identifies the company's unique risk profile, which in turn forms the essential foundation for the company's privacy program. Companies frequently engage third-party vendors for their risk assessments, though some companies may perform risk assessments using qualified internal personnel.

A risk assessment generally examines:

- Threats to the business and its data.
- Vulnerabilities of the business that may be exploited.
- The likelihood of any given threat occurring.
- The harm that may result if any given threat occurred.

Some risk assessments solely examine information technology (IT) systems. Others look at the fuller picture and take into account:

- Access controls.
- Internal policies and practices.
- Other compliance measurements.

The scope of any specific risk assessment varies widely from company to company, depending on:

- The sensitivity of the data the company collects and stores.
- The company's size.
- The company's industry, for instance whether it is in a highly regulated industry, such as healthcare or financial services.
- The extent to which the IT function is outsourced to vendors.
- The IT function's sophistication.

ANALYZING LEGAL REQUIREMENTS AND DEVELOPING A COMPLIANCE ROADMAP

Once the company understands its data, data flows, and primary risks, it can:

- Determine and analyze its legal obligations (see Determining Legal Requirements).
- Create a roadmap for moving toward compliance (see Building the Compliance Roadmap).

Determining Legal and Program Requirements

While the specific resources and references most applicable to a given business vary depending on its risks and compliance needs, many sources of information may be useful in crafting a privacy compliance framework. As an initial matter, companies should develop their privacy framework by reference to their specific legal compliance obligations. This is particularly important for companies in regulated industries.

The US, however, does not have a comprehensive privacy or data protection law. A patchwork of state and federal laws instead apply to the collection and use of individuals' personal information. Many foreign countries do have comprehensive laws governing the treatment of personal information, notably EU countries that have adopted the EU directive and must comply with its replacement, the General Data Protection Regulation (EU GDPR) by May 15, 2018 . For more information on US and EU privacy and data protection laws, see Practice Notes, US Privacy & Data Security Law: Overview (6-501-4555) and Overview of EU data protection regime (8-505-1453).

Determining applicable law and the corresponding legal requirements is a fact-specific analysis, but typically depends on:

- The type of information the company collects.
- The jurisdictions:
  - in which the company operates;
  - stores data; or
  - where the persons whose personal information is collected reside.
- The use or other treatment of the personal information.

However, the company should not limit its scope of reference to only applicable law. Whether or not the company is regulated, federal regulatory agency guidance provides a useful reference point for developing a privacy compliance framework. The Federal Trade Commission (FTC) in particular, which has broad regulatory authority over privacy and data security, has released guidance across many privacy topics, including:

- Fair information practices and protecting consumer privacy generally (see Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers).
- Privacy of children's information (see for example, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business and Complying with COPPA: Frequently Asked Questions).
- The internet of things (see Internet of Things: Privacy & Security in a Connected World).
- Mobile applications (see Marketing your Mobile App: Get it Right from the Start).
- Data security (see Start with Security: A Guide for Business).

For more information, see the FTC's Protecting Consumer Privacy and Business Center: Privacy and Security pages.

The EU directive and related Article 29 Working Party guidance is also helpful in understanding best privacy practices even if the company is not technically required to comply with any EU laws (for more information, see Practice Note, Overview of EU data protection regime (8-505-1453)).

In addition to laws and regulatory guidance, other useful resources a company may consult in developing its privacy compliance framework include:

- Other federal guidance, such as:
  - the US Department of Commerce's privacy green paper, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework; and
  - White House Executive Orders, guidance, policy statements, and proposed regulation, such as Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.
- Guidance from state attorneys general, notably, the California Attorney General (for more information, see Practice Note, California Privacy and Data Security: Overview: Enforcement and Regulatory Guidance (6-597-4106)).
- The Organisation for Economic Cooperation and Development's (OECD) fair information practice principles (FIPPS), a set of privacy norms developed in the 1970's that form the basis for many US and foreign privacy laws, including the EU directive and EU GDPR, and Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
- International company for standardization (ISO) standards such as:
  - ISO 29100 - privacy data protection standards; and
  - ISO 22307 - privacy impact assessments for financial services.
- The American Institute of Certified Public Accountants' generally applicable privacy principles.

Building the Compliance Roadmap

Once the company has identified the applicable legal requirements and analyzed them against its current practices, it can develop a roadmap that lays out the privacy compliance tasks to undertake in the next six to 12 months. The roadmap helps the business keep its privacy compliance efforts on track and provides direction to the team and key stakeholders regarding future activities. The company should reevaluate the roadmap every six months.

In developing the roadmap and prioritizing compliance tasks, the business should consider:

- The risks to be mitigated, particularly those identified as high risk.
- The cost of implementing programs.
- How easily and quickly a given goal can be achieved.

Businesses should typically prioritize addressing high-risk areas and easily addressable tasks.

DEVELOPING POLICIES AND INTERNAL CONTROLS

The privacy team must create and maintain the policies and internal controls that ensure the company is complying with key laws and regulations on an ongoing basis. Key policies and internal controls include:

- External privacy statements provided to consumers and others regarding the company's collection and use of data, including:
  - website privacy policies;
  - mobile app privacy policies; and
  - policies that apply to offline collection and use of data (see Practice Note, Drafting Privacy Notices (w-000-9621)).
- Internal privacy policies and procedures, such as those that govern how the company collects, uses, protects, retains, and shares consumer and employee personal information (for example, see Standard Document, Personal Information Protection Policy (Internal) (8-596-0085)).
- Policies and procedures related to privacy and security breaches, such as incident:
  - response plans and procedures; and
  - reporting and tracking tools.
- Internal reporting mechanisms for:
  - communicating privacy concerns; and
  - reporting to the board of directors or senior management.
- External reporting mechanisms for reporting privacy:
  - issues to law enforcement or regulators; and
  - risks to the Securities and Exchange Commission.
- Policies and procedures that address communicating with persons whose personal information the company has collected, such as:
  - personal information access and correction policies; and
  - procedures for handling privacy complaints.
- Policies that address the use of company IT and communications resources, such as:
  - acceptable use of company IT systems (for a sample, see Standard Document, IT Resources and Communications Systems Policy (8-500-5003)).
  - social media policies (see Standard Document, Social Media Policy (US) (5-501-1524)); and
  - bring your own device policies (see Standard Document, Bring Your Own Device to Work (BYOD) Policy (1-521-3920)).
- Tools that address managing privacy risk and assessing program success, including:
  - privacy by design policies and practices (see Box: Privacy by Design);
  - risk assessment tools (see Practice Note, Data Security Risk Assessments and Reporting (w-002-2323));
  - privacy impact assessments; and
  - privacy measures.
- Data governance practices and policies that guide compliance and address data privacy regulations, such as:
  - records retention schedules;
  - records disposal policies and procedures; and
  - records storage policies and procedures (see Records Management Toolkit (2-520-1257)).
- Internal policies that address the governance of corporate crown jewel (intellectual capital) data.
- Supplier, vendor, and other third-party privacy requirements.
- Controls directed to tracking and complying with any jurisdiction-specific requirements, such as registering with foreign data protection authorities.

SUPPORTING BUSINESS OPERATIONS

The privacy team is responsible for providing guidance to the business on complying with the privacy program and its day-to-day business objectives. The privacy team supports the business by:

- Providing business-focused solutions that protect personal data while supporting business development and growth. For example:
  - addressing the issues that arise constantly as a company markets and sells its products and services, particularly concerning the collection, use, storage, and sharing of personal information about consumers and customers;
  - working with product developers as they develop products that may affect privacy, including implementing privacy by design, which involves getting involved at the beginning of a project and ensuring that privacy concerns and protections are addressed during a product or service's build, implantation and launch (for more information on privacy by design, see Box: Privacy by Design);
  - working with HR on issues that affect employee privacy, such as cross-border transfers of employee data, the use of background checks, and employee monitoring (for more information on employee privacy considerations, see Practice Note, Privacy in the Employment Relationship (6-517-3422));
  - reviewing contracts for privacy compliance considerations; and
  - integrating a new company or database into the existing corporate structure after a merger or acquisition.
- Managing privacy complaints and incidents, including investigating and responding to data breach incidents.
- Vendor management (see Vendor Management).

Vendor Management

A key component of privacy compliance is managing relationships with vendors and other third parties that have access to the company's data. Effective vendor management requires evaluating risk around third parties and:

- Identifying the third parties that access the company's data or with whom the company shares its data.

- Developing a due diligence process for vetting vendors.
- Ensuring that vendor agreements include provisions that address and mitigate privacy risk.
- Developing a process for auditing vendor compliance with contractual requirements.
- Addressing the issues that arise when the relationship ends, including migration and return or destruction of data.

For more on managing vendor privacy compliance, see Practice Note, Managing Privacy and Data Security Risks in Vendor Relationships (w-001-8814). For sample vendor data security clauses, see Standard Clauses, Data Security Contract Clauses for Service Provider Arrangements (2-505-9027).

ADDRESSING ONGOING COMPLIANCE

A successful privacy compliance program requires ongoing assessment and efforts. Key components of ensuring ongoing compliance include:

- Providing privacy training and awareness programs (see Training and Awareness).
- Monitoring and auditing compliance efforts and benchmarking against the privacy compliance plan (see Monitoring and Auditing).
- Evaluating and revising program controls, policies, and protocols (see Evaluating and Revising Program Controls).

TRAINING AND AWARENESS

Training is a key administrative safeguard and is specifically required by some laws, such as the Health Insurance Portability and Accountability Act of 1996. The privacy compliance program should include a formal program that provides for annual training on privacy compliance issues. All company agents should receive training, including directors, officers, employees and vendors. The training program should cover:

- Applicable privacy laws and policies.
- Recognizing potential violations.
- Addressing privacy complaints and misconduct, including proper reporting procedures.
- The consequences for violating privacy laws and policies.

Companies should obtain written acknowledgements from trainees requiring them to both acknowledge receiving the training and agree to abide by company policies and applicable law. The privacy team should monitor training participation and enforce training requirements.

In addition to training, successful privacy programs often also include practices that reinforce privacy compliance awareness in multiple communication channels, such as in periodic e-mails, newsletters or by providing materials on a dedicated intranet page.

For a sample HIPAA compliance training program, see Standard Document, HIPAA Training: Presentation Materials (w-000-7162).

MONITORING AND AUDITING

The privacy team should monitor compliance with the program by monitoring the company's operations on an ongoing basis to:

- Verify that internal controls, policies, and procedures are in place and being followed.
- Identify any compliance gaps.

The privacy team should also work with internal audit or a third-party contractor, at least on an annual basis, to perform a formal audit of the effectiveness of the program, including the effectiveness of the privacy team's monitoring efforts.

EVALUATING AND REVISING PROGRAM CONTROLS

Program updates should take into account:

- Monitoring and audit results.
- Relevant changes to:
  - applicable law;
  - changes to the business;
  - evolving industry standards; and
  - benchmarking against the practices of comparable companies.

In particular, companies should assess on a regular basis whether there are:

- New threats or risks to the business and whether existing controls are adequate to address them.
- Changes to the business, such as new business areas or geographies that may affect the program controls.
- Changes to the law that affect compliance or risk levels.
- Areas for improvement based on audit results, industry or peer benchmarking, complaints or other feedback.

COMPARING PRIVACY OFFICE MODELS

Core Team Model	Privacy Working Group
Agile.	Longer decision making process.
Stronger ability to make policy.	Business units decisions may need to be a coordinated effort.
Focused forum to discuss and evaluate corporate privacy needs.	No forum to discuss all privacy issues that affect organization.
Full-time privacy team.	Generally not full-time privacy professionals.
Central decision making authority.	Corporation may not perceive privacy council as a central decision making authority.

PRIVACY BY DESIGN

Privacy by design (PbD) is an approach to operationalizing privacy within systems, products and business processes. Since it was introduced in the 1990's by former Privacy Commissioner of Canada, Ann Cavoukian, it has been widely endorsed by regulatory authorities, including the FTC, and privacy professionals. At its core, privacy by design calls promoting consumer privacy in every stage of product and program development.

PbD consists of seven foundational principles:

- Taking a proactive, not reactive, approach to privacy issues.
- Making protecting privacy the default setting in developing systems and business practices.
- Embedding privacy into the design of systems and practices.
- Making privacy a positive-sum, rather than zero-sum, game.
- Incorporating end-to-end security that protects data throughout the lifecycle.
- Visibility and transparency.
- Respecting user privacy by incorporating strong privacy defaults, appropriate notice, and user-friendly options.

(See Privacy by Design, The 7 Foundational Principles and Privacy and Security by Design: An Enterprise Architecture Approach.)

Implementing a PbD approach involves working with leadership to emphasize to business teams that privacy is a business requirement and that the privacy team should be consulted at the beginning of any project so that it can conduct a privacy impact assessment and identify any privacy issues the project may present.

As endorsed by the FTC, PbD calls for:

- Maintaining comprehensive data management procedures throughout the product lifecycle.
- Incorporating the following substantive privacy principles into product design and development:
  - data security;
  - reasonable collection limits;
  - sound retention practices; and
  - data accuracy.

(See Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers).

At a high-level, implementing PbD involves:

- Identifying the flows of individuals' personal information within a project.
- Developing specific privacy requirements for a project.
- Incorporating privacy requirements into a project's design.
- Testing to confirm that privacy protections are operating as intended.

The Office of the Information and Privacy Commissioner of Ontario maintains a website with helpful information on PbD.

10-16