Applying Privacy Principles in a Rapidly Changing World

As new technology and data uses challenge traditional privacy guidance, Intel recognizes the enduring value of this guidance and seeks ways to implement recognized privacy principles flexibly and effectively.

Executive Summary

Dramatic, fast-paced developments in digital technology present unprecedented challenges for companies applying privacy law, regulation, and commonly accepted principles. As a result, traditional notions of fair information practice principles (FIPPs) that form the basis of privacy guidance are under scrutiny. Intel believes businesses and policymakers should not discard these enduring principles, but instead consider new implementations that effectively protect privacy and encourage innovation.

The fair information practice principles that govern the protection of individual privacy were first defined in the 1970s—a time when computer systems, processes, and programs that enabled the accumulation, storage, and use of personal data proliferated. Over time, these principles have been adapted to accommodate the growing complexity and sophistication of new technologies and business models and the ease with which data moves across national boundaries.

The pace of technological change, advances in analytic processing, developments in business models, and proliferation of data collected and generated from different sources all drive the need to reexamine these principles. If businesses and consumers are to continue deriving the benefits of privacy guidance, it will be necessary to rethink how the principles can be applied effectively and with sufficient flexibility to serve the dynamic digital marketplace.

Creative approaches to transparency and notice, enhanced security, and accountability can help adapt fair information practice principles to meet the requirements of the marketplace and consumers. We believe transparency can be accomplished through comprehensive notices that support oversight by regulators and civil society, coupled with contextual notices that help individuals make appropriate decisions about the collection and use of their data. The massive collection and storage of data demand heightened security measures. And flexible application of the FIPPs should be balanced with accountability and organizations’ internal policies, practices, and programs that foster responsible data use and protection.
Business Challenge
Rapid advances in technology significantly strain the application of established privacy protections. The challenge is how to apply accepted privacy principles to new technologies and business practices in a way that provides effective protection and encourages innovation.

The growing volume, speed, and complexity of data collection, transfer, and use all challenge existing models of data protection. Massive stores of data from diverse sources provide a rich and potent resource for education, commerce, research, and government. Powerful analytics yield insightful, real-time inferences about individual consumers. Organizations employ service suppliers located worldwide to perform business processes. Using technologies ranging from surveillance cameras to radio frequency identification, organizations gather and store data inexpensively, often in the cloud, where servers may be located anywhere in the world.

Not only do companies collect data—individuals generate information about themselves and others through social networks and mobile devices. And given the rapid pace of development, the impulse to retain information for as-yet-unanticipated uses is perhaps understandable and often makes good business sense.

Policymakers seek ways to improve data governance to better serve consumers and businesses. While traditional principles of fair information practice still serve as the foundation of responsible data management, new technologies and business models raise questions about how these principles can continue to provide the best possible privacy protection and still encourage innovation.

The fair information practice principles (FIPPs) of notice and choice are under particular scrutiny. In a notice-and-choice model, companies provide individuals with information about how data will be collected and used. Based on this notification, individuals choose whether to share their data. This model is challenged by an environment in which organizations can analyze and process information instantaneously at the collection point. In this environment, data collection has become ubiquitous. Individuals are easily overwhelmed by the number of privacy notices they receive as they shop online, use a mobile device, engage in social networking, or visit a building that has surveillance cameras.

In many cases, it may not be possible to provide notice to consumers. Even in cases when it is, the notice may be lengthy and complex and not designed to support the individual’s ability to decide. Only in limited circumstances might the choice itself provide real guidance for organizations about user preferences.

Moreover, as the amount of online data relating to consumers has continued to grow, the percentage of that data that comes directly from individuals has decreased. In many instances, individuals do not have an opportunity to consent to collection or use of their data. Questions about notice and choice are further complicated when data is used subsequently for a different or unanticipated purpose, is aggregated with other data, or is anonymized.

Intel’s challenge is to apply established privacy principles in ways that work in this complex environment. While implementation may of necessity look different, the goals remain the same: to provide effective protection for individuals, enable innovation, improve the user experience, and meet the requirements of regulators worldwide.

Evolving Principles of Fair Information Practice
Since the 1970s, FIPPs have served as the foundation for the responsible collection, use, and protection of information about consumers. These principles have stood the test of time and remained sufficiently flexible to respond to the demands of changing technology, complex business models, and a global digital marketplace.
FIPPs

The United States Department of Health, Education, and Welfare in 1972 established the Advisory Committee on Automated Personal Data Systems to explore the impact of computerized recordkeeping on individuals. In its report, published a year later, the committee proposed a Code of Fair Information Practices. These principles form the basis of subsequent codes and laws related to information collection, including the United States Privacy Act of 1974.

The FIPPs include the following:

- There must be no personal data recordkeeping system whose existence is secret.
- There must be a way for individuals to find out what information about them is recorded and how it is used.
- There must be a way for individuals to prevent information that was obtained for one purpose from being used or made available for other purposes without their consent.
- There must be a way for individuals to correct or amend records of identifiable information about themselves.
- Any organization creating, maintaining, using, or disseminating identifiable personal data must assure the reliability of the data for the intended use and must take precautions to prevent its misuse.

These principles now form the foundation of law and regulation across the United States, Europe, and around the globe. They also serve as the basis for industry best practices and international agreements addressing data protection and transfer.

OECD Privacy Guidelines

The Organization for Economic Cooperation and Development (OECD) in 1980 adopted guidelines based on the FIPPs, designed to harmonize national privacy legislation without interrupting the free flow of information across borders. The OECD guidelines comprise eight principles addressing the collection, security, and primary and secondary uses of data.

These guidelines and their core principles have become an internationally acknowledged framework for privacy and responsible international data flows (see the “Protecting Personal Privacy: The OECD Guidelines” sidebar). The OECD guidelines are recognized for their continued utility over 30 years in the face of rapid changes in information technology and data-driven business.

Recently the OECD recognized that new technologies and data uses create new requirements for data protection and management, and in 2013 released revisions to the guidelines. The revisions encourage the growth of an information-fueled economy and recognize the need to reduce barriers to movement of data across borders. The OECD did not change the core privacy principles but reconsidered the guidelines, focusing on the requirements of accountability; the importance of robust, streamlined cross-border flow of data; harmonized breach notification requirements; and the need for enhanced interoperability across national and regional privacy regimes.

APEC Privacy Framework

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework comprises nine principles and implementation guidance designed to assist APEC economies in developing consistent domestic approaches to personal information and privacy protections. This framework forms the basis of a regional approach to the accountable and responsible transfers of personal data between APEC economies.

The APEC Privacy Framework is founded on the principles contained in the OECD guidelines. It differs, however, in its focus on preventing misuse of personal information and the harm that results. The framework also places more emphasis on the data controller’s accountability for the appropriate protection of information as it is transferred. The APEC framework addresses

Intel Privacy Rules Meet the Requirements for Global Transfer of Data

The Irish Data Protection Commissioner in 2013 approved Intel’s Binding Corporate Rules, specifically the Intel Corporate Privacy Rules (ICPR) governing the company’s movement of data across international borders. Binding Corporate Rules are legally enforceable rules for the processing of personal data. These rules are developed by the company and recognized by the appropriate European data authority. They ensure that adequate safeguards are in place to protect the rights of individuals when personal data is transferred between members of a corporate group to countries outside Europe that do not have legally required levels of protection.

Approval of the ICPR by the Irish authority enables us to move data not only into and out of Ireland but also across the European Union and globally between Intel sites. Recognition of the ICPR highlights Intel’s ongoing effort to implement effective privacy protections.
Privacy by Design’s Foundational Principles

Privacy by Design (PbD) is an approach that takes privacy into account and builds in protections at each phase of the product or service development process. It promotes the dual goals of enhancing privacy and personal control over individuals’ information and enabling organizations to sustain a competitive advantage through innovation and robust data use. PbD incorporates seven privacy principles:

• Privacy should be built in at the beginning of product or service development. It should be proactive and not reactive, preventive and not remedial.
• Privacy should be implemented as the default setting.
• Privacy should be embedded into the product or service design.
• PbD encourages both privacy and robust innovation, with privacy as a positive-sum—not a zero-sum—game.
• PbD involves implementation of end-to-end security that provides full lifecycle protection.
• PbD promotes openness, visibility, and transparency.
• PbD is about respect for user privacy and must be user-centric in its orientation.

several areas of privacy concern, including preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability.

The APEC Ministerial Meeting endorsed the framework in 2004. Since then, APEC participants have made significant progress in designing an infrastructure based on the principles that would facilitate protected cross-border data transfers.

Intel Privacy Principles

Intel’s longstanding commitment to protecting privacy is at the core of the company’s values. Our company-wide privacy program is based on traditional principles of fair information practice. While these principles remain as relevant as they were when established 40 years ago, we recognize the challenges of effectively applying them to our products, services, and processes.

Intel continues to support the OECD privacy guidelines and uses them as the basis of our corporate privacy program. This program is based on the following beliefs:

• Individuals have the right to keep aspects of their personal lives confidential and to expect appropriate collection, use, and disclosure of personal information.
• Organizations are responsible for respecting an individual’s rights and for managing personal information appropriately.

The requirements of international privacy law and regulation directly affect Intel. As a global organization, we transfer personal information about our employees related to payroll, benefits, and personnel matters. We make devices that are used by individuals around the world to enrich their lives, and we handle customer data for product and technical support services. Online, in the cloud, and when transferring data between countries, we manage data responsibly, and we build privacy into everything we do.

To integrate privacy across its business, Intel applies the principles of Privacy by Design—an internationally recognized approach to protecting individual information that requires companies to consider and address privacy at each phase of a product or service’s development. In 2010 the International Conference of Data Protection and Privacy Commissioners adopted a resolution recognizing PbD as an essential component of fundamental privacy protection. The conference encouraged organizations to adopt PbD’s foundational principles as their default mode of operation for guidance in establishing privacy standards.

Rethinking the Implementation of FIPPs

In considering ways to apply FIPPs in the emerging data environment, we believe new approaches to transparency and notice, security safeguards, and accountability are the key to establishing effective, workable protections.

Transparency and Notice

Transparency and notice remain fundamental to good privacy and data practices. They encourage companies to engage in important data hygiene—understanding what data they collect and hold, how and why they use it, whether and for how long they maintain it, and how they secure and protect it. They enable individuals, advocates, and experts to access information about an organization’s data collection practices, use of technologies, and privacy protection measures. Transparency and notice are also necessary for regulatory oversight and enforcement.

Transparency and notice may best be realized through the implementation of two kinds of communications:

• Comprehensive notices, which provide an in-depth explanation of how an organization collects, processes, and protects data. Civil society experts may review these notices to develop a detailed view of a company’s practices or an understanding of developments across the digital marketplace. Regulators may compare these statements with the company’s activities to determine
whether their representations are valid and whether their practices fall within the bounds of law and commonly accepted guidance.

- **Context-specific notices**, which provide concise, targeted information about data collection, use, storage, and protection so individuals can determine whether to make a purchase, engage in some activity, or interact with an online vendor. Focused, tailored, context-specific notices support individuals' real-time decision making about the collection and use of their data.

**Security Safeguards**

Complex data environments heighten the importance of security. Technology's increased capacity to collect, correlate, and store data about individuals raises the risk of its exposure and misuse. These risks, and the threats to the individual that result, drive Intel's focus on security technologies and tools.

Security—along with power-efficient performance and connectivity—are the pillars upon which Intel builds its innovation efforts. Because we develop, manufacture, and sell technology around the globe, we are keenly aware that trust—in our products, services, and business practices—is fundamental to the success of the company's vision.

**Accountability**

Increasingly complex technologies, business models, and supplier relationships demand innovative approaches to the implementation of FIPPs. As businesses seek flexible approaches to applying these principles, accountability can provide the rigor necessary to ensure they are implemented effectively and in a manner that promotes trust.

A traditional notice-and-choice model provides a ready example. Protection regimes that rely primarily on this model have been identified as not adequately serving individuals, whose data is often generated by third parties through social networks, often without the person's knowledge. Because data collection has become ubiquitous, reading notices and exercising choice in every instance may prove unduly burdensome and ineffective. Even when individuals do access notices, they are often lengthy and complex and do not support well-informed privacy decisions.

In an accountability model, companies are required to act on meaningful consent when individuals can provide it. But even when choice is not available or appropriate, accountability demands responsible, disciplined collection, use, and protection of consumer data.

Accountability also addresses concerns about the global nature of data flows, requiring that companies remain responsible and answerable for the protection and management of data, regardless of who processes it or where the processing occurs.

Accountability requires that organizations establish policies that foster the protection of individual privacy and put in place programs and practices to further the effective implementation of these policies. Accountability focuses on setting privacy-protection goals for companies based on established public policy and allowing them discretion to determine how those goals are met.

Accountable businesses adopt methods and practices to reach those goals in a way that best serves their business models, the requirements of technology, and the demands of their customers. In exchange, accountability requires organizations to demonstrate responsible policies and systems that effectively protect individuals and their data.

**Conclusion**

Intel believes that the FIPPs continue to provide useful guidance, and we are rethinking how to adapt them to best serve the emerging data environment. We encourage businesses, experts, and policymakers to consider how these recognized protections can be implemented to promote responsible data practice and to foster the trust necessary for innovation and economic growth.

The FIPPs that form the basis for the OECD guidelines, the APEC privacy framework, and Intel's own privacy program have endured and accommodated dramatic advances in information technology. Intel looks forward to working with businesses, regulators, and civil society to develop workable approaches to applying fair information practices in ways that protect individuals and encourage innovation. We are “Rethinking Privacy” by applying the enduring guidance of FIPPS to innovative products and services that will further our goal: to connect and enrich the lives of every person on earth.
Protecting Personal Privacy: The OECD Guidelines

The Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data is the world’s most influential framework addressing international privacy concerns. Based on the principles of fair information practice, the OECD guidelines are designed to protect the privacy of individuals and the flow of data across national borders. They include the following:

- **Collection Limitation Principle.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data Quality Principle.** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

- **Purpose Specification Principle.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Use Limitation Principle.** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle with the following exceptions:
  - With the consent of the data subject
  - By the authority of law

- **Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

- **Openness Principle.** There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use as well as the identity and usual residence of the data controller.

- **Individual Participation Principle.** Individuals should have the right to do the following:
  a. Obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to them
  b. Have communicated to them the data relating to them
    - Within a reasonable time
    - At a charge, if any, that is not excessive
    - In a reasonable manner
    - In a form that is readily intelligible to them
  c. Be given reasons if a request made under subparagraphs (a) and (b) is denied, and be able to challenge such denial
  d. Challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed, or amended

- **Accountability Principle.** A data controller should be accountable for complying with measures that give effect to the principles stated above.