
THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

GLOBAL PRIVACY PROTECTION FRAMEWORK

A project of the

Hunton & Williams Center for Information Policy Leadership

February 2003

Part I—The Principles

Introduction

The past decade has witnessed a surge in concerns about protecting the privacy of personal information. This new attention is prompted by many factors. Two of the most important are the spread of the Internet and the development of new digital technologies and applications that make the collection and use of personal information easier, cheaper, less centralized, and often undetectable to individuals. The growth of personalized direct marketing around the world has added to these concerns, as have lingering memories of government surveillance and misuse of personal information by the Nazis during World War II, the secret police in communist Eastern Europe and the Soviet Union, and the FBI and other law enforcement authorities in the United States during the Cold War and the McCarthy era.

Addressing these concerns is critical for national governments, not only because of the significance of privacy to individuals as citizens and consumers, but also because data protection laws affect the affordable, reliable availability of information that is essential for democracy and market economies. The public's need for data protection is always in tension with its need for accessible information. Data protection law is the tool to help craft the delicate balance between privacy and the free flow of information. Getting that balance right is essential to maximizing individual and societal welfare.

One of the earliest and broadest efforts to identify the principles necessary to strike that balance was led by the Organization for Economic Cooperation and Development. The OECD's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* outline the basic principles for both data protection and the free flow of information.* They have been widely accepted, but they operate at a high level of generality and therefore permit broad variation in national implementation.

As a result, national governments have responded to recent fears about new technologies and past abuses of personal information in very different ways. At one extreme, the European Union in 1995 adopted a data protection directive that regards data privacy as a fundamental human right and imposes sweeping requirements on national governments to regulate virtually all aspects of data collection, use, transfer, storage, and even destruction. Under this model, centralized data protection authorities administer a complex array of requirements—applicable to public and private sectors—for national registration of data processing activities, notice and consent documents, investigative and enforcement mechanisms, and substantive limits on data processing and data transfers. The presumption of the law is that personal data may not be collected or used without specific authorization by the government, the data subject, or both.

At the other end of the spectrum, the United States has evolved a system of data protection that is highly contextual, based on industry sector, type of information, and intended use. Some uses of information—for example, the monitoring or telephone calls or the seizure of records by

* The OECD Guidelines are reproduced in Appendix A.

the government—are regarded as implicating constitutional or human rights, but many are not. Even similar types of information may be dealt with differently, depending upon the setting in which they were collected. For example, three entirely different laws regulate name and address information resulting from subscribing to cable television, obtaining telephone service, or renting video cassettes. This situation is further complicated by the existence of 51 sets of state privacy laws and the central role in U.S. data protection played by private agreements, industry self-regulatory codes, company privacy policies, and individual self-help mechanisms. Despite the contextuality of the U.S. system of data protection, it rests on the presumption that personal data usually may be processed without individual or government permission, unless it is very likely that significant harm would result.

It is increasingly clear that neither the EU nor the U.S. system of data protection offers a very useful model for how to implement the OECD Guidelines. Not only do they each reflect their own unique set of circumstances, but they—like the Guidelines themselves—were developed prior to significant changes in technologies and markets that have created new privacy challenges. It is certainly possible to learn from the experience with these two systems, but neither presents a model to be emulated, as a growing chorus of critics within each system have noted.

Moreover, the human rights rhetoric that has often appeared to divide the European Union and the United States has proved more distracting than informative. Few people would disagree that information privacy, at least in some contexts, is a human right, but that conclusion is not particularly illuminating, because of the unavoidable need to balance competing human rights. Even if regarded as a human right, data privacy will have to be balanced with others, including freedom of expression, protection against crime and other threats to person and property, and the opportunity to confront witnesses and present evidence.

The need for balancing reflected in the OECD Guidelines is thus essential in all workable systems of data protection. Many countries around the world are looking for a model for how to achieve that balance—to respond to the concerns of their citizens regarding both privacy and other human rights and interests served by information flows.

In addition, there is an increasing awareness of the importance of international information flows and therefore of the need to prevent unnecessary interruptions in those flows, whether from embargos by countries with restrictive privacy regimes or from the impediments created by inconsistent national data protection laws. This need grows more acute as international trade, commerce, and travel expand. Consumers are highly mobile and increasingly expect customized services wherever they are located, provided 24 hours a day, seven days a week. Only by sharing information across borders—to support customer service centers, Internet commerce, international clearance of checks and credit and debit card payments, and the operations of multinational entities—can these expectations be met. In an increasingly global economy, and especially in the context of an inherently global commodity like information, the need for consistent or harmonized data protection laws grows ever more urgent.

This Framework is designed to help meet the need for a practical, modern data protection model—one that facilitates a pragmatic balancing of individual privacy and individuals' need for

accessible information to provide a consistent, principles-based standard of protection in many different national settings. It is the result of an initiative undertaken by the Hunton & Williams Center for Information Policy Leadership in 2001-2003 to examine the successes and failures of the European and U.S. experiences implementing the OECD Guidelines and to understand the emerging challenges to, and opportunities for, data protection presented by new technologies that did not even exist when the Guidelines were adopted. As part of its analysis, the Center has consulted with a wide range of government officials, industry leaders, consumer advocates, and scholars to craft a new framework for data protection.

This Framework responds to the charge in the OECD Guidelines that countries work toward the “development of principles, domestic and international.” (OECD Guidelines ¶ 22) It builds on the foundation laid by the OECD in 1980, the experience of existing data protection regimes, and other multinational principles, such as the United Nations Guidelines for the Regulation of Computerized Personal Files (1990), the International Labour Organization’s Code of Practice on the Protection of Workers’ Personal Data (1996), and the Ottawa Ministerial Declaration on Privacy (1998).

This Framework focuses on data protection applicable to the private (as opposed to government) sector, but is otherwise intended to be neutral with regard to medium of communication, technology, and country. It does not advocate specific privacy protection measures, but rather seeks to provide principles to guide legislators and policymakers in crafting, implementing, and enforcing privacy laws and regulations. To the extent laws are based on common principles they are easier to harmonize. Such laws are also less likely to impose impediments to the multinational flows of information that increasingly undergird the free movement of people, products, and services across borders. Both are explicit objectives of the OECD Guidelines, which call on countries to take “all reasonable and appropriate steps to ensure that transborder flows of personal data . . . are uninterrupted and secure” and that data protection regimes are “simple and compatible.” (OECD Guidelines ¶¶ 16, 20)

While this document focuses on when and how law should be used to protect privacy, its provisions are also a useful guide for internal privacy policies, self-regulation, and decision-making by companies and other entities that collect or use personal information. This is a valuable role for these principles because such individual and self-regulatory actions often provide more effective and more sensitive protection for personal privacy than do laws or regulations.

Finally, although these principles have been the subject of intensive discussions that in many ways have spanned 30 years, they are still a work in progress. The Center’s goal in creating this document is not merely to aid in the development of effective, consistent systems of data protection today, but also to facilitate further discussion and to build consensus about how such protection might be improved for the future.

The principles are summarized below. They are described more fully, together with commentary illustrating how they might be applied in practice, in Part II.

The Principles

1. **Honesty and Accountability Principle**—Entities should collect, use, or transfer personal data only in compliance with applicable law and with any stated or knowingly implied undertakings, and with concern for data privacy, accuracy, and security. They should be accountable for their activities.
2. **Respect for Individual Action Principle**—Individuals are entitled to make choices about how personal data about them are used and protected. The government should therefore facilitate individual choices and interfere as little as possible with private or market-based arrangements.
3. **Benefits Principle**—Data protection is not an end in itself, but rather a tool for enhancing individual and societal welfare. To be effective, data protection must rest on the recognition that both information flows and privacy have value and are necessary in a democratic society and market economy. That value benefits individuals as well as society as a whole. The goal of any privacy regime must therefore be to balance the value of accessible personal information with the value of information privacy to maximize both individual and public benefits.
4. **Prevention of Harm Principle**—Data protection laws should regulate information flows when necessary to protect individuals from harmful uses of information.
 - a. Privacy protection should be proportional to the likelihood and severity of the harm threatened.
 - b. Individuals are less likely to be harmed by the mere collection, possession, or transfer of accurate information. Moreover, even information that could be used for harmful purposes may also have uses that are beneficial for the data subject, the data user, and society as well. As a result, privacy regulation should target harmful uses of information, rather than its collection, possession, or transfer.
 - c. Some personal information or uses of personal information may be especially sensitive within the context of cultural norms, and therefore more likely to cause significant emotional distress or other harm. Such sensitive information warrants special legal protection, which may include restrictions on its collection, possession, or transfer, as well as use.
5. **Security Principle**—Personal data which could reasonably be used to harm individuals should be secured against accidental or deliberate loss, misuse, alteration, or destruction. The level of security should reflect the likelihood that the information could be used to cause harm and the severity of the likely harm. Legal requirements concerning security should be technology-neutral and avoid interfering with the development and use of new measures.

6. **Effective and Efficient Enforcement Principle**—Enforcement of privacy laws should achieve effective compliance with these principles and applicable law, as efficiently as possible, while minimizing the burden on individuals or interference with the benefits they enjoy.

7. **Consistent Protection Principle**—Individuals should enjoy privacy protection that is consistent across jurisdictions. To this end, data protection laws should reflect broadly accepted principles, be adopted at the highest level feasible (e.g., national instead of local), be harmonized to the greatest extent possible, and be enforced efficiently. They should not impose special obligations on personal data that are exported from or imported to the jurisdiction.

Part II—Commentary on the Principles

Data protection and the use of information in modern societies are complex issues. While the principles are intended to stand on their own, they are more likely to prove a useful guide for specific, globally interoperable privacy protections if supplemented by additional commentary explaining how they might be applied in practice and how that application could affect current policy debates over issues such as the appropriate use of opt-in and opt-out consent systems. Because the specific application of the principles will depend upon many contextual factors, and must necessarily be flexible, this commentary is intended to be illustrative, not prescriptive. The commentary is designed to enhance the usefulness of the principles as a guide for crafting, implementing, and enforcing privacy laws and regulations (as well as for internal privacy policies, self-regulation, and decision-making concerning privacy), and as a spark for further discussion.

1. Honesty and Accountability Principle—Entities should collect, use, or transfer personal data only in compliance with applicable law and with any stated or knowingly implied undertakings, and with concern for data privacy, accuracy, and security. They should be accountable for their activities.

It is essential in any meaningful system of data protection that the entities that collect, use, or transfer personal data be honest and accountable. This is especially important because effective privacy protection is rarely provided by data protection laws alone. Rather, many of the most effective and sensitive means for protecting the privacy of personal information involve self-help measures, self-regulation, industry codes, and individual entities' privacy policies. The importance of these tools are reflected in the following two principles. The success of these tools depends on individuals being aware of when personal information is being collected and used, data collectors and users being sensitive to the privacy implications of their activities, and an assurance that the law will enforce agreements and undertakings concerning data protection. These are the objectives of this principle and the foundation of any system of data protection, as recognized in the OECD Guidelines by the Collection Limitation and Openness Principles.

2. Respect for Individual Action Principle—Individuals are entitled to make choices about how personal data about them are used and protected. The government should therefore facilitate individual choices and interfere as little as possible with private or market-based arrangements.

Data protection is inherently concerned with individuals' control over uses of personal information about them. This is often a personal matter; tastes vary widely about what information is sensitive and how much it should be protected. As a result, data protection tools should be designed to enhance individual choice. This includes choice about what personal information is collected or used and for what purposes, but it also includes choice about data protection. Because data protection often blocks beneficial information flows and therefore results in decreased opportunities, higher prices, and less convenience for consumers, individuals should also have meaningful choice about how much they are willing to pay, or what benefits they are willing to forgo, in exchange for data protection.

Even the provision of choice, however, creates costs. So the goal of data protection should therefore be to enhance choice about the collection and use of personal information and types and degrees of data protection without imposing unnecessary costs or inconvenience on individuals. In competitive markets, this may mean allowing entities that wish to collect or use personal information to compete for business by the level of privacy protection they offer. This principle reflects a preference for tools that allow for a more precise balancing of privacy benefits and costs than do most substantive legal protections. So, for example, under this principle, consumers are better served by technologies that allow for personalized privacy protections, or a wide range of individual privacy policies from which consumers may select, than a one-size-fits-all government-imposed standard of privacy protection.

This principle is reflected in the OECD Guidelines' admonition that countries should "in particular" endeavor to "encourage and support self-regulation, whether in the form of codes of conduct or otherwise" and "provide for reasonable means for individuals to exercise their rights." (OECD Guidelines ¶ 19) If individuals are empowered to make informed choices in competitive markets, this will not only enhance their ability to make privacy choices, it will also spur the development of better data protection tools from which to choose.

As suggested by the OECD Guidelines, this does not mean that governments play no role. There are many important steps that governments can take to facilitate meaningful individual choice, including:

- Educate consumers and citizens.
- Encourage the development of technologies that enhance individual choice concerning data protection.
- Create incentives for the creation and deployment of market-based data protection tools.
- Facilitate standardized and easily comparable privacy notices.
- Promote self-regulatory efforts by data users.
- Eliminate barriers to the creation and use of interoperable privacy protections.
- Prohibit and prosecute fraudulent or willful misrepresentations and other related deceptive trade practices.

In markets where competition does not exist or where special interests are at stake, the government may need to play a more direct role in guaranteeing that individuals have meaningful choices about data processing and data privacy. Those situations are discussed in greater detail below under Principle 4.

- 3. Benefits Principle—Data protection is not an end in itself, but rather a tool for enhancing individual and societal welfare. To be effective, data protection must rest on the recognition that both information flows and privacy have value and are necessary in a democratic society and market economy. That value benefits individuals as well as society as a whole. The goal of any privacy regime must therefore be to balance the value of accessible personal information with the value of information privacy to maximize both individual and public benefits.**

The Benefits Principle reflects the critical understanding that data protection does not exist in a vacuum. It is not the only value that individuals care about. Protecting the privacy of personal information is always in tension with other values, such as the benefits and convenience that individuals enjoy from the availability of personal information. Moreover, data protection almost always creates compliance costs. The existence of this tension and these costs suggests another reason why data protection is such an individual matter: Individuals don't want to pay for more privacy than they desire.

The underlying goal, therefore, of data protection law should be to maximize individual and public benefits, of which the privacy of personal information is an important one, but only one. As noted above, one way of helping to maximize benefits is to allow individuals to strike the balance between data protection and other values for themselves.

There are other general guidelines that can help maximize benefits across the society and are useful tools for implementing the Benefits Principle. For example, no data protection law should be enacted or enforced that does not in fact significantly serve the purpose for which it was enacted. Laws that are ineffective or that are enacted without a specific purpose in mind, run the risk of imposing costs without achieving benefits.

Data protection laws should also not be enacted or enforced if they are substantially more burdensome or broader than necessary to serve that purpose. There is no doubt but that personal privacy could be enhanced by prohibiting all collection and use of personal information. But to do so would greatly interfere with democratic self-government, public safety, human interaction, and free markets. If a data protection law is substantially more restrictive than necessary to serve its purpose, then no matter how valuable that purpose, the law will impose costs without achieving commensurate benefits. Similarly, some data protection laws, even if narrow and precise, may necessarily impose costs that exceed their benefits.

Overly burdensome or intrusive privacy protection poses many risks. Not only does it fail to maximize the benefits enjoyed by both individuals and society, it is likely to impose unnecessary costs and to interfere with the ability of entities to compete with each other, new entities to participate in markets, and the development and deployment of new services and products, including new forms of data protection. As a result, the Benefits Principle is concerned not only with maximizing benefits at any particular moment in time, but with the long-term sustained maximization of public benefits.

4. Prevention of Harm Principle—Data protection laws should regulate information flows when necessary to protect individuals from harmful uses of information.

There are situations where technologies, industry codes, privacy policies, and individually negotiated privacy measures do not offer effective privacy protection. For example, the absence of a competitive market for an essential product or service may mean that individuals have no meaningful choice about the collection or use of information about them. Similarly, in some settings individuals have no meaningful opportunity to be aware of, or express preferences regarding, the collection or use of personal information about him or her. In these situations, data protection law may be necessary to ensure that individuals are provided with opportunities to

control the collection or use of personal information about them. By contrast, data protection laws should not apply in settings where no meaningful harm is realistically threatened. This principle is at the heart of the OECD Guidelines, which exclude from data protection regimes “personal data which obviously do not contain any risk to privacy and personal liberties.” (OECD Guidelines ¶ 3)

a. Privacy protection should be proportional to the likelihood and severity of the harm threatened.

The most common form of data protection employed in such situations is a requirement that entities desiring to collect or use personal information provide notice and a meaningful opportunity to consent (opt in) or withhold consent (opt out) for a proposed use. The type of notice and consent mechanisms employed should reflect the likelihood and severity of the harm threatened. The principle of proportionality was recognized in the recent joint submission by Austria, Finland, Sweden, and the United Kingdom, later joined by the Netherlands, on the need for amending the EU data protection directive:

[T]he processing (in the widest sense of that term) of personal data is essential to the effective functioning of the single market. The purpose of data protection rules is not to prevent the processing of personal data. Rather, it is to ensure the proportionate regulation of such processing. The rules must give effective protection to individuals’ personal data without unnecessarily restricting the processing needed to deliver the services which our increasingly technologically sophisticated society demands. (Joint Submission ¶ 3)

Under the Prevention of Harm Principle, if there is only limited risk of harm and the degree of harm is not likely to be great (for example, if the harm is the inconvenience of receiving offers for products or services that may or may not be of interest), then it may be appropriate for the law to require only a basic or general notice and to presume consent in the absence of an individual opting out. If the risk of harm is great or the harm threatened severe, specific, individual notice and consent may be justified. Because the greater the notice and consent requirement, the greater the cost, inconvenience, and risk of missed opportunities are likely to be, data protection tools should be no more restrictive than necessitated by the likelihood and severity of the harm. Proportionality is essential, as the OECD Guidelines make clear by providing for “the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated.” (OECD Guidelines ¶ 3)

The goal of notice is to provide enough information to allow individuals to make informed decisions concerning the collection and the use of personal data. Consent requirements are designed to ensure that individuals have an appropriate opportunity to express or withhold consent for uses of information that pose a risk of harm. If there is no meaningful decision for the individual to make, a notice requirement is likely to be unwarranted. Similarly, if no significant harm is realistically likely to result from the collection or use of the information, mandatory consent will usually be unjustified. (See OECD Guidelines ¶ 10)

Even if notice and consent requirements are appropriate, subsequent uses of personal information should be permitted to the extent they are necessary to the “fulfillment of those purposes” for which the information was collected, or are otherwise “not incompatible with those purposes.” (OECD Guidelines ¶ 9)

Another data protection tool that governments may employ is a requirement that collectors or users of personal data provide individuals with access to, and an opportunity to dispute or correct the accuracy of, data concerning them. (See OECD Guidelines ¶ 13) This can be a controversial requirement, because while access may serve valuable purposes, it is often very costly and it always presents privacy and security risks. For example, requiring access may require entities to centralize information about individuals, thereby creating a storehouse of personal information that can be target for hackers and identity thieves. Similarly, providing access requires verifying identity, which in turn requires the collection of more personal information, is often costly and time-consuming, and poses the grave risk of providing one individual with access to another individual’s personal information. As a result, the requirement that the data protection tool be commensurate with the risk of harm is particularly important in the case of access.

As a practical way of reducing the costs and risks associated with access and with determining its proper scope and reasonableness, access should only be required if the information identifies a specific individual, is not lawfully publicly available, is routinely associated with other information about a specific individual (e.g., is organized according to individual, rather than by transaction or date or store), and could reasonably be used to cause a specific, identified harm to a consumer.

- b. Individuals are less likely to be harmed by the mere collection, possession, or transfer of accurate information. Moreover, even information that could be used for harmful purposes may also have uses that are beneficial for the data subject, the data user, and society as well. As a result, privacy regulation should target harmful uses of information, rather than its collection, possession, or transfer.**

One useful principle in measuring harm is to focus on uses of information. Individuals are less likely to be injured by the mere collection or transfer of information about them. For example, knowing the age or gender of an individual is not likely, by itself, to harm him or her. However, if that information is used to discriminate unlawfully, then the use of the information is clearly injurious. The harm results from the use, not the existence of the information. As Austria, Finland, the Netherlands, Sweden, and the United Kingdom recently noted: “The data themselves are neutral. It is their processing which can give rise to risk.” (Joint Submission ¶ 8)*

It is sometimes argued that regulating collection and possession of personal information is one way of ensuring that it is not available to be used in harmful ways. This is not necessarily true, because information can be collected or observed in many different ways, some of which

* For additional information on the new importance placed by Sweden, home of the world’s first comprehensive data protection law, on use—rather than collection, possession, or transfer—of personal data see <http://justitie.regeringen.se/inenglish/ issues/dataprotection/index.htm>.

are likely to be beyond the reach of law or regulation. But more importantly, even information that may be used inappropriately may also have many beneficial, desirable uses. Seeking to regulate the mere collection, possession, or transfer of such information interferes with those beneficial uses. For example, a merchant may collect a credit card number in order to process a transaction for a consumer. The merchant must transfer that number to a bank or other clearing institution to complete the consumer's transaction. This clearly serves the consumer's interest. If the number is used to commit fraud, however, this is a harmful use that the law in most countries prohibits.

Focusing on harmful uses also helps improve the effectiveness and lower the cost of data protection and the enforcement of data protection laws. Prosecuting an entity because it has observed or collected personal information, but not in any way used it to anyone's detriment, wastes public resources. It is analogous to stopping every car that enters a highway, just because some people will take advantage of that highway to speed or otherwise violate the law. Far better to focus scarce public resources on only those users that use the highway for an unlawful purpose. This is fundamental to the OECD Guidelines, which by their own terms apply only to personal data which "because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties." (OECD Guidelines ¶ 2) Personal data which "obviously do not contain any risk to privacy" are excluded from protection. (OECD Guidelines ¶ 3)

Where a type of use is always harmful (e.g., the use of personal information to commit fraud), the government is justified in prohibiting the use outright. There is no need to provide for notice and choice, since if a use is always harmful, it can reasonably be assumed that no one would consent to the use. But these uses are rare and often already made illegal under existing law.

- c. **Some personal information or uses of personal information may be especially sensitive within the context of cultural norms, and therefore more likely to cause significant emotional distress or other harm. Such sensitive information warrants special legal protection, which may include restrictions on its collection, possession, or transfer, as well as use.**

Many systems of data protection, including the OECD Guidelines, recognize that some personal information, or uses of personal information, may be particularly sensitive and therefore warrant special protection under the law because they are more likely to cause harm. That harm is measured not only in economic loss or physical injury, but also in emotional distress or significant burdens on time and convenience. Because of the sensitivity of the information, it may be necessary under this principle to regulate not only use, but also the collection, possession, or transfer of such information. It is important to remember, however, that what makes these types and uses of information sensitive is seldom defined meaningfully only by content, because what is sensitive in one setting may not be in another. As a result, this principle focuses on context and broadly accepted social and cultural norms to determine when information is sensitive.

The determination as to what constitutes sensitive information should be made consciously and thoughtfully. The fact that information is sensitive in a given context does not necessarily mean that its use should be restricted for all purposes. For example, in many countries information about a communicable medical condition, while widely regarded as sensitive, may nevertheless be required to be disclosed as a means of protecting public health or protecting sexual partners.

5. Security Principle—Personal data which could reasonably be used to harm individuals should be secured against accidental or deliberate loss, misuse, alteration, or destruction. The level of security should reflect the likelihood that the information could be used to cause harm and the severity of the likely harm. Legal requirements concerning security should be technology-neutral and avoid interfering with the development and use of new measures.

Security is a critical component of data protection because no matter how responsible an entity's own use of personal information, if that information is not adequately protected it can be accessed and misused by others. Providing appropriate security requires action at many levels. Technology can be a critical component, locking away the information so that it is not easily stolen or hacked. Employee training and monitoring are important components, because even the best security is valueless if employees who are authorized to have access abuse that authorization. Individual responsibility is also an essential element, because even the most impregnable security cannot protect individuals who fail to protect their own records, share passwords, or who volunteer information to strangers over the telephone or via e-mail. No amount of legal or corporate security can protect individuals from their own poor judgment.

As a result, good security always involves education and training, the adoption and enforcement of appropriate policies, and the development and use of technologies. Moreover, security needs are constantly changing and so all three elements of a security strategy require constant reexamination and revision. Legal requirements often evolve too slowly to meet the demands of effective security, and they often run the risk of fixing in place an outmoded technology or other approach to security. The risk is not only that security will be compromised, but that outdated or inappropriate requirements will impose costs without achieving benefits. As with all other aspects of data protection, the requirements imposed by law should be proportional to the likelihood and severity of harm. This is why the OECD Guidelines call for "reasonable security safeguards." (OECD Guidelines ¶ 11)

Both governmental and nongovernmental organizations can play an important role in helping to ensure an appropriate level of security, including:

- Working jointly with business, academic researchers, consumer advocates, and others to develop guidance as to appropriate minimum standards for security.
- Providing incentives for developing and implementing security standards and devices.
- Encouraging private-sector initiatives and removing impediments to those initiatives.
- Educating data users and the public about appropriate security techniques.
- Imposing liability for foreseeable harms resulting directly from the negligent or willful failure to provide security that was appropriate and reasonable given the type of

information being processed and the state of security-related research and applications at the time of the processing.

- Funding and otherwise facilitating the development of security technologies, best practices, audits, certification standards and programs, and codes of conduct.

6. Effective and Efficient Enforcement Principle—Enforcement of privacy laws should achieve effective compliance with these principles and applicable law, as efficiently as possible, while minimizing the burden on individuals or interference with the benefits they enjoy.

Effective enforcement is essential to meaningful, consistent data protection. The goal of enforcement should be to achieve a high degree of compliance and to compensate victims for actual harms suffered as a result of misuse of personal information, without imposing unnecessary burdens on individuals or the responsible, lawful use of personal information. It is important that enforcement not create a disincentive for attempting to comply with the law, by unfairly punishing responsible users who try and fail or by ignoring harmful uses of data that may be more difficult to prosecute.

As a result, enforcement actions should target information processors that contribute directly and materially to the harmful use of personal information. Processors should be liable only if the harm results from their negligent, willful, or intentional behavior. They should be liable if third parties obtain personal information from them and then use it for harmful purposes only if the harmful use was reasonably foreseeable and the provider of the information intended or recklessly failed to prevent it. Liability should never be determined under a strict liability standard, or when the harm was not reasonably foreseeable or could not reasonably have been prevented, because to do so is both unfair and provides a strong disincentive to the responsible use of information. (See OECD Guidelines ¶ 14)

As discussed below, data protection laws should not permit overlapping or duplicative enforcement actions. Enforcement should be as efficient as possible.

7. Consistent Protection Principle—Individuals should enjoy privacy protection that is consistent across jurisdictions. To this end, data protection laws should reflect broadly accepted principles, be adopted at the highest level feasible (e.g., national instead of local), be harmonized to the greatest extent possible, and be enforced efficiently. They should not impose special obligations on personal data that are exported from or imported to the jurisdiction.

To facilitate consistency and predictability in privacy protection, governments should seek to avoid inconsistent or overlapping local laws or regulations. Where possible, privacy laws should be adopted at the highest practical level (e.g., national instead of local or provincial), and laws should be harmonized to the greatest extent possible in an effort to achieve consistent, if not uniform, national standards. Data protection laws should avoid imposing special burdens on the transborder flow of personal data and should avoid creating special or greater obligations outside of the jurisdiction in which the law operates than apply within the jurisdiction.

Rather than seeking to impose extraterritorial legal obligations on data flows in other countries, national data protection laws and authorities should focus instead on mutual recognition of concurrent national regimes. As long as those regimes reflect the same basic principles, whether those identified in this document or the more general OECD Guidelines, compliance with the laws in the country in which personal information is used should satisfy the requirements of the national law where the data originated. In addition cooperation between federal and state or provincial authorities, cross-border agreements, and other initiatives can improve the quality, efficiency, and uniformity of data protection laws and enforcement. Alternatively, the parties to a transaction involving personal information may specify (through contract, privacy policy, or other means) the jurisdiction whose laws shall govern the use of the information. In either case, one regulatory entity should be responsible for addressing each violation of a data protection law.

The critical point—reflected in the Consistent Protection Principle and the OECD Guidelines—is to avoid overlapping data protection regimes or enforcement, or other impediments to the transborder flow of information. The OECD Guidelines emphasize this point repeatedly, requiring countries to “take all reasonable and appropriate steps to ensure that transborder flows of personal data . . . are uninterrupted and secure,” and urging countries to “refrain from restricting transborder flows of personal data” and to “avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.” (OECD Guidelines ¶¶ 16-17)

The Guidelines lay particular stress on “International Cooperation,” to ensure that data flows are not unnecessarily restricted by overlapping or inconsistent data protection laws, that national laws and the procedures for implementing and enforcing them are “simple and compatible,” and that nations provide “mutual assistance” in enforcing data protection laws and investigating alleged violations. (OECD Guidelines ¶¶ 20-21)

The Global Data Protection Framework, by building on the OECD Guidelines, other multinational data protection principles, and the experience of nations implementing them, lays the foundation for data protection systems that protect individuals’ interest in privacy, as well as their interest in choice, convenience, service, and lower prices that accessible information make possible. It seeks to maximize both individual and public benefit by focusing on four key elements.

First, the Framework explicitly addresses the inherent tension between restrictions on information flows necessary to protect privacy and the impact of those restrictions on the availability of the information necessary to serve other vital interests, ranging from self-governance and public safety to convenient and affordable access to desired products and services.

Second, the Framework recognizes that while law is an important element in data protection, it is not the only one and often not the most important one. The wide range of tools—including, but not limited to, law—for helping individuals achieve the most sensitive and least costly balance between restrictions on information flows necessary to protect privacy and protections for information flows necessary to serve other vital interests. Technologies, self-help, codes of conduct, privacy policies, and other measures can provide greater precision and flexibility than laws or regulations.

Third, the Framework is built on the principle of proportionality in data protection, especially concerning the adoption and enforcement of data protection laws and regulations. Precisely because of the individual nature of personal privacy and the variety of competing interests at stake, it is essential that data protection be commensurate with the likelihood that personal could be used to cause harm and the severity of harm likely to result.

Finally, the Framework is designed to facilitate consistent, globally compatible data protection, without ignoring important differences among nations. In an increasingly global society, and when dealing with a subject as inherently global as information flows, individuals are best served by data protections systems that are as consistent and compatible as possible. Laws that impose special obligations outside of their jurisdiction, data protection systems that impose a burden on transborder data flows, and overlapping or over-zealous enforcement disserve the public and the society by imposing costs far in excess of their benefits.

The Hunton & Williams Center for Information Policy Leadership believes that this Framework, by building on the OECD Guidelines and diverse national experiences and multinational agreements concerning data protection, provides a workable model to help countries develop effective, consistent systems of data protection today and well into the future.

Appendix A

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL DEFINITIONS.

1. For the purposes of these Guidelines:

- a) “data controller” means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
- b) “personal data” means any information relating to an identified or identifiable individual (data subject);
- c) “transborder flows of personal data” means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

- a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
- b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
- c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy (“ordre public”), should be:

- a) as few as possible, and
- b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.

Collection Limitation Principle

7. 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

8. 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

9. 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

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. 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

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

- a) adopt appropriate domestic legislation;
- b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
- c) provide for reasonable means for individuals to exercise their rights;
- d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

information exchange related to these Guidelines, and

mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.