# UPDATING DATA PROTECTION: PART I - IDENTIFYING THE OBJECTIVES

*A DISCUSSION DOCUMENT*

Fred H. Cate

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

## Introduction

Data protection laws face increasing stress and scrutiny in North America, Europe, Asia, and elsewhere in the face of sweeping changes in consumer behavior, technologies, markets, and data flows. This paper is intended to facilitate discussion about the objectives those laws should be designed to serve in the 21st century. The paper does not offer any conclusions, but rather sets out a statement of problems raised by current data protection systems, and identifies possible directions that modern data protection laws might take.

While part of a broader project the Centre for Information Policy Leadership at Hunton & Williams LLP is undertaking to identify the core objectives of data protection in both public and private sectors around the world, this paper responds to the U.S. Federal Trade Commission's announcement of its December 7, 2009, Roundtable entitled "Exploring Privacy". It is therefore primarily focused on data protection in the United States applicable to the private sector.

## The Problem

Data protection law is increasingly challenged to protect personal information adequately, without imposing unnecessary costs on individuals, data users, and regulators. In the face of significant changes in consumer behavior, technologies, markets, and data flows, data protection laws and their application on both sides of the Atlantic and in Asia appear increasingly challenged.

- Individuals are inundated with privacy policies and breach notices that they have neither the time nor the resources to act on. Often those notices create confusion and pose questions that create only the illusion, but not the reality, of informed consumer choice.

- Data protection laws and enforcement are often unrelated to substantive privacy protection. Many of today's most intrusive data practices, for example, by law enforcement and national security authorities, go effectively unregulated, while other activities that pose few privacy risks are subject to more extensive legal requirements.

- Similarly, expanded access by law enforcement and national security authorities to personal data collected by the private sector creates new risks for both individuals and private sector data stewards that the data may be lost or otherwise compromised or used for purposes far beyond those for which they were collected.

- Moreover, because protections for personal data are often in tension with beneficial uses of those data, existing data protection laws often result in privacy being sacrificed—often unnecessarily—to those competing uses. For example, privacy regulations can restrict

research in healthcare and other fields because of the cost or practical difficulty of complying with applicable laws, even though the research may present few, if any, risks to personal privacy and offer significant benefits to society.

- Data protection laws and practices often impose real costs on institutional operations, innovation, and efficiency that are unrelated to their ineffectiveness in protecting privacy, taking resources away from more effective privacy protection processes. This is especially likely where enforcement focuses on procedural requirements, such as providing comprehensive notices, rather than substantive protections, such as regulating harmful uses of data.

- Regulators face the daunting challenge of trying to oversee a flood of disparate data processing activities, many of which occur outside of their jurisdiction, with limited resources and often inadequate legal authority. Local, provincial, and national data protection authorities are increasingly challenged by global, widely dispersed data flows via the internet, handheld devices, and other technological innovations.

- Yet those same innovations and new applications, such as Facebook, MySpace, Twitter, and other "social" networking sites, expand the range and scope of harms that individuals can unknowingly inflict on themselves or others.

- Despite efforts at multinational frameworks, data protection law and enforcement continue to be the responsibility of national or subnational authorities, while data flows have grown increasingly global. Inconsistent and ineffective data protection regimes do not properly serve anyone.

In response to these and other challenges, policy makers and regulators in Washington, Brussels, and elsewhere are beginning the process of reexamining current data protection laws, and have invited participation from industry, advocacy groups, and academics. The Centre for Information Policy Leadership at Hunton & Williams LLP applauds these efforts and welcomes the invitation to participate.

The first step in determining how effective data protection laws are today or how they could be improved in the future is to identify the goals that they are intended to serve. While there has been considerable discussion about the definition of privacy and the role of government in protecting it, there has not been enough systematic thought given to the fundamental question of the goals that data protection law should accomplish. The failure to address this core question has been especially acute in recent years and in light of significant changes in the broad context in which data protection occurs.

Where such discussions have occurred over the past four decades, two objectives seem to dominate: to enhance individual control over personal information and to protect individuals from harmful uses of

their information. While undoubtedly important, these two goals today appear inadequate. Individual control seems both impossible in many instances in the face of the proliferation of information technologies, and potentially undesirable in some situations. In reality, data protection laws in many countries act to limit individual control by permitting extensive use of personal data without consent or, in some cases, even notice. Prevention of harm appears even more inadequate. While this is clearly an important objective, it entirely omits the concept of privacy as a human right that is recognized today in many countries, and it ignores the extent to which public opinion has overwhelmingly condemned certain practices (for example, telemarketing) that arguably threaten no specific privacy harm.

## The Centre's Project

The task that the Centre is undertaking is to identify for broader discussion the core objectives of data protection that will work in a world of modern technologies, markets, and data flows. Those objectives are critical to the on-going evaluation of existing laws and the creation of effective new ones. Those objectives should also be the basis for institutional accountability for their use of personal data: they should set forth the objectives of data protection and provide the basis for evaluating the extent to which those goals are achieved. The Centre is hopeful that this paper will spark a robust debate and welcomes the comments of others.

The collection and use of personal data often raise different issues and are subject to different constraints in the private sector than in the public sector. For example, the collection and use of personal data by governments are more likely to serve important public objectives, be subject to legal compulsion, and be insulated from market forces than by commercial or not-for-profit entities. Similarly, there may be different constraints on transparency and different tools available for protecting privacy in the public sector than in the private sector. And the jurisdiction of data protection authorities often differs significantly between public and private sectors.

The Centre believes that it is important to address the objectives of data protection in both the public and the private sector, especially as there is increasing interaction between the two as governments increasingly look to the private sector as a source of personal information. However, because of the important differences between the two contexts, the Centre intends to consider the objectives for data protection in each sector separately. Those objectives may well overlap, but it is important that they not be intermingled indiscriminately.

As the first phase of its project to assess the effectiveness of data protection laws, the Centre proposes identifying core objectives of data protection in the public sector and, separately, in the private sector, in light of consumer behavior, modern technologies, markets, and data flows.

## Initial Possible Directions

The process of identifying the objectives of data protection will be neither easy nor quick, but in anticipation of the U.S. Federal Trade Commission's December 7, 2009, Roundtable "Exploring Privacy," the Centre thought it would be useful to identify some initial thoughts about defining privacy objectives for the private sector. These do not reflect any final views of the Centre or the opinions of its members, but we hope that they will help prompt and inform the on-going discussion.

- Prevent Harm. Although it is clear that prevention of harm to individuals and society is not a complete definition of the objectives of data protection, it is likely to be an essential component. Surprisingly, prevention of harm has played comparatively little role in many data protection laws, which have focused instead on objectives unrelated to harm or have been concerned primarily with remedies for harm after it has occurred. One critical role for privacy law, however, could well be to create appropriate incentives so that private-sector collectors and users of personal data take those reasonable steps within their means to prevent harmful uses of those data. "Harm" would presumably not include appropriate uses of accurate information that result in disadvantages to an individual—for example, a determination not to lend to a consumer based on that individual's past failure to repay loans—but instead would include injuries resulting from data being inaccurate, incomplete, out-of-date, or lost or stolen. The concept of harm is therefore broader than physical or economic injury, but it does not include all negative effects resulting from the use of personal data. One important corollary of prevention of harm as an objective is that laws and regulations that do not act to prevent harm would require some other, explicit justification.

- Secure Data. A key component of preventing harm is ensuring that personal data are secured against loss, theft or other compromise. Perfect protection should not be the goal, but rather appropriate protection taking into account factors such as the sensitivity of the data, the potential for being used to cause harm, and the severity of any likely harm. Data protection laws should likely create reasonable incentives to ensure that personal data are secured appropriately.

- Rethink the Role of Consent. Individual consent has played a significant role in data protection, beginning with Alan Westin's path-breaking 1967 study, *Privacy and Freedom*, in which he defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[1] Obtaining consent and providing "privacy notices" to individuals for the purpose of obtaining consent have become a proxy for individual control, and have evolved into the central focus of many data protection regimes in the United States and elsewhere.[2] Irrespective of whether consent was ever an appropriate basis for data

[1] Alan F. Westin, *Privacy and Freedom* 7 (1967).

[2] See, e.g., Fred H. Cate, "The Failure of Fair Information Practice Principles," in *Consumer Protection in the Age of the Information Economy* 343, 356-360 (2006); Paul M. Schwartz, "Privacy and Democracy in Cyberspace," 52 *Vanderbilt Law Review* 1607, 1659 (1999); Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* 11 (2000); OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. (C 58 final) (Oct. 1, 1980), at ¶ 7; *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with*

protection, it is well documented that consent does not work in many settings today and often results in weakening the protection for personal privacy. More importantly, however, one might reasonably wonder whether consent was ever an appropriate *objective* for data protection. A more appropriate role for consent may well be as one *tool* for protecting privacy, rather than as the *goal* of privacy protection. Viewed as an important tool, but only one of many, for protecting privacy, consent might be employed where experience and research have shown it can be effective (for example, in settings where consent is not required and therefore can be truly voluntary), but not relied on in other settings.

- Ensure Accountability. To date, data protection systems have tended to be more focused on compliance with procedural requirements, rather than ensuring that an organization is accountable for its acquisition and use of personal data. This is understandable, given how complex the conditions for accountability can be—often including, for example, clear principles, training, oversight, redress, etc.—and how hard they can be to demonstrate. But the difficulty of the task should not undermine the importance of the goal—namely, that data protection systems ensure appropriate accountability for the stewardship of personal data.

- Provide Redress. While providing redress to individuals affected by uses of personal data may not seem an appropriate objective of data protection, it is certainly an essential component. Redress not only attempts to repair injuries done to individuals, but also to provide feedback to users of personal data and regulators that can be used to improve data protection systems and avoid future harms. Without appropriate mechanisms for redress, it is difficult to imagine a data protection system achieving its other objectives. Appropriate redress must be swift, accessible to individuals who believe they have been injured, and efficient. Where redress becomes unnecessarily burdensome, it discourages individuals to seek help and can inappropriately impede valuable data flows. One particular challenge in providing redress is that individuals often do not know the source of the data that they believe has been used inappropriately. This thorny issue will have to be addressed whether through coding data to indicate source, greater transparency of data processing operations, or other measures.

- Guarantee Effective Enforcement. In addition to providing redress for individual data subjects, any system of data protection will require effective enforcement mechanisms. "Effective", in this context, requires not only that the mechanisms achieve a high degree of compliance, but also that they are well targeted to do so, and so do not squander scarce resources of either government or industry officials. To date, enforcement of data protection systems has often proved both inadequate to achieve broad compliance, but also overly broad and expensive (for example, when state attorneys general in the United States bring duplicative enforcement actions, often in the wake of federal enforcement). This disserves privacy and wastes resources. As with redress, enforcement may seem an odd objective of data protection, but it is an essential component without which other objectives are unlikely to be achieved.

---

*Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281), Preamble, ¶ 25; Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, 2004/AMM/014rev1 (Nov. 2004), at 12.

- Remember Global Data Flows. Few uses of personal data today occur entirely within one nation or jurisdiction. Personal data are increasingly transferred across national boundaries for processing, storage, or other use. Many private-sector enterprises manage their data in multinational repositories or outsource data processing activities to multinational organizations. It is increasingly difficult to think of any transaction involving personal data—whether using a credit card, visiting a doctor, making an airplane reservation, or browsing the internet—where the data stays within one country. Yet most data processing laws are still adopted within a single country (or state or province). This mismatch between law and daily reality is burdensome to all concerned. While multinational data processing standards are one important approach to this conundrum, there is growing reason to think that the more immediate and practical solution is through cooperation and even collaboration in enforcement actions, and better systems for each nation or jurisdiction to recognize the enforcement activities of others. At the same time, it is important that national enforcement actions respect the sovereignty of other nations and their laws, and the difficult position of multinational companies in complying with conflicting legal requirements. Clearly, reconciling these competing interests is not easy, but the failure to explicitly take into account the multinational nature of most information flows threatens to undermine the ability of any system of data protection to achieve its objectives and therefore diminish the protection accorded privacy.

- Treat Privacy in Context. In addition to taking into account the increasingly global nature of information flows, it is important that any system of data protection be cognizant of a wider range of contextual issues, for example, that many uses of data have great value to individuals and society; that privacy is a critical value but only one of many that policy makers must attend to; that resources for crafting, complying with, and enforcing data protection laws are limited and constantly needed for other activities; and that while individuals are often very concerned about privacy (or at least their own privacy), they face many competing demands for their time and so often are not willing to expend great efforts to protect privacy. None of these or similar considerations weakens the importance of providing appropriate data protection, but ignoring them is likely to only weaken that protection.

- Treat Law in Context. Finally, it seems essential that policymakers also be clear as to the intended role of law and the context in which it operates. While law is an essential part of sound data protection, it seems unlikely (as well as undesirable) to attempt to use law to compel all behavior regarding personal data. Instead, law is likely to be more effective if employed as one of many incentives for desired types of behavior concerning data collection and use. In some settings, it may actually be a weaker incentive than economic and reputational interests. In the context of a variety of incentives, law might best be thought of as setting basic standards or principles for data processing, a floor of legal requirements, and gap-filling measures where other incentives do not appear to operate effectively. Developing a clearer understanding of the proper role of data protection law can help improve efficiency,

reduce costs, and heighten the effectiveness of privacy laws by focusing them where needed most. Similarly, a clearer understanding of the law's role might help reduce situations in which the law operates as a disincentive for good data protection, for example, as is the case when law operates a strict liability trigger to punish innocent errors with the same speed and force as reckless or deliberate conduct.

## Conclusion

It is far too early in this process to speak of a "conclusion." The list of future possible directions for privacy objectives is neither exhaustive nor necessarily correct. Rather, as noted, it is one of numerous efforts to help inform the on-going debate. The Centre believes that the discussion about the objectives of data protection is both critical and timely, and we forward to participating.

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP