There is growing recognition that conventional privacy rights and protective measures are inadequate for dealing effectively with the civil liberties challenges posed by the ongoing explosion in personal information trafficking. To address some of the major shortcomings of current privacy frameworks, this chapter explores the prospects for an allied but distinct identity rights framework for dealing with personal information handling by large organizations. In particular, we introduce the notion of “identity impairment,” not subsumed by “privacy violation.” We further propose a view of citizen-centric identity rights relevant to interactions between individuals and organizations that make categorical judgments about individuals based on information, regardless of whether this information should enjoy privacy protection. Drawing from the Canadian Charter of Rights and Freedoms and borrowing heavily from fair information practices more generally, we articulate a set of fundamental identity integrity rights and associated “fair identity practice” principles. Such a citizen-centric-identity-based approach to personal information handling, by focusing on the decisions that directly affect individuals in transactional situations, promises to be more easily understood and actively supported by members of the public than privacy-based arguments.

“ID, please.” In one form or another, whether in person or online, individuals increasingly hear this request when initiating a service transaction with an organization. Typically the expected response of handing over a document with a name, number, and picture, or entering an account name...
and password, produces the desired result, and the individual can proceed with the transaction smoothly. Occasionally however, providing identification has the opposite result, and the transaction is denied. Sometimes the person is then treated with suspicion, especially if she questions the decision, and may even be apprehended. Too often the reasons for this denial of service or access are not clear, and no adequate justification is provided. When someone is not permitted to enter a building, pick up a parcel, buy liquor, or the like, the person may be inconvenienced or embarrassed. In the case of making an important application, such as for a loan, welfare benefit, housing, job, or student admission, a refusal can diminish one’s life chances. Often no clues are given about the grounds on which the “data subject” has been sorted into a disadvantaged category or even that this categorizing has occurred. At borders or when boarding an airplane, the consequences can be more serious yet. The recurring, well-publicized trouble that Ted Kennedy faced in U.S. airports because a variant of his name appeared on a no-fly watch list offers insight into the difficulties facing thousands of other innocent travellers similarly listed, few of whom have the resources that the late senator could muster in repairing his situation. An extreme example of such challenges involves Canadian engineer Maher Arar, who was detained by U.S. officials while in transit at JFK airport and underwent “extraordinary rendition,” including torture and solitary confinement in his native Syria. After he was released an extensive public inquiry cleared his name, and the Canadian government awarded him $10.5 million in compensation. However, the United States still does not allow him to cross its borders.

While there are important differences across all the various cases of unwarranted access or service denial sketched above, which we may refer to as “identity impairments,” there are also some key similarities promising of a unified corrective approach. Whether it is a mail recipient trying to collect a package with a former address still on her driver’s license, an innocent victim of extraordinary rendition intercepted because his records appear to fit some terrorist profile, or someone in the myriad of other life situations where one’s legitimate business is thwarted after trying to comply with an ID request, each case is characterized by an adverse organizational judgement based on information previously recorded about the individual. The conventional approach to dealing with harms related to the misuse of personal information, i.e., about an identifiable individual, is to treat it as a form of privacy violation. Privacy protection usually involves withholding one’s information in anticipation of potential violation or once collected ensuring it is neither used nor disclosed in ways inconsistent with the original purpose. However, in the ID cases mentioned here, this approach is not likely to be effective. Another
way of thinking about promoting the rights of information subjects that address these identity impairments needs to be explored.

This chapter takes up the challenge of articulating a new information right that is applicable to ID-demanding situations, one that addresses the limitations of privacy as the overarching framework. It proposes a distinctive “identity right,” allied with the right to privacy but going beyond it in terms of the problematic situations that it can help resolve. We begin the exploration of identity rights by examining some of the shortcomings of privacy and how a focus on identity can shift the focus of attention from the point of personal information collection onto the categorical judgments organizations make about individuals. This leads into looking at constitutional sources, notably the Canadian Charter of Rights and Freedoms, for the legal foundations for a right to identity integrity. Extending the widely adopted principles of fair information practice and incorporating the seven laws of identity, we then articulate eighteen fair identity/information practice principles. The chapter closes by discussing some of the expected challenges in establishing identity integrity as a well-recognized and supported information right.

LIMITATIONS OF A PRIVACY FRAMEWORK

*Privacy* is the broad term commonly used in referring to incidents when information about a person is used by others in ways considered harmful, risky, or socially inappropriate. Public opinion surveys have long indicated that privacy violations are a widespread concern. Privacy advocates, however, lament that, in spite of high public awareness of privacy conflicts, conventional measures are inadequate for dealing with the problems associated with the burgeoning collection and use of personal information. Furthermore, privacy concerns do not translate readily into practical action by individuals, who often relinquish control of their information for immediate, but relatively modest, benefits.

Semantically Complex

Various reasons are given for the current privacy crisis (note other chapters in this volume). Drawing on conceptual and situational perspectives, we examine three limitations that are especially relevant to this discussion of problematic ID-based transactions. Many authors have pointed out confusion and lack of clarity about what is meant by “privacy” in informational contexts. It appears to mean very different things to different people in different situations. Part of the confusion arises from the origins of the modern treatment of privacy
rights in the classic Warren and Brandeis (1890) formulation as “the right to be let alone,” which is not directly appropriate to transactional settings when, far from wanting seclusion, people seek to be active in the public realm, by traveling, conducting business, and the like. The more recent informational self-determination interpretation partly overcomes this difficulty but brings others related to the still-growing variety and subtlety of situations in which individuals act with their personal information. While there are some important advantages to having a broad umbrella term such as *privacy* widely used for referring to a variety of forms of personal information abuse, it brings serious shortcomings when probing problematic situations more deeply. Solove (2002) provides a survey of the various conceptualizations of privacy, which while helpful in better appreciating the complexity of the term, does little to clarify things from an individual person’s perspective. If scholars have trouble articulating a coherent common ground for understanding privacy, it is not surprising that the lay public adopts varied and inconsistent meanings.

**Situationally Impractical**

A second major area of difficulty that the prevailing privacy framework presents is the burden of vigilance and restraint it places on anyone trying to exercise effective control over her personal information. In situations where one is explicitly requested to provide information, such as filling in an application form during an enrollment process, there is a strong bias against the data subject taking the steps necessary to make good judgments about whether the risk of loss of control over personal information is worth the payoff. The benefit for providing the requested information is usually immediate and tangible—the application is accepted, the desired service is provided, the transaction proceeds smoothly. Even the attempt to assess the privacy risks and tradeoffs involved in providing or withholding information brings an immediate cost in terms of delay. Simply reading and understanding the privacy policy related to an online transaction is beyond the patience and expertise of even the most dedicated privacy advocate (Akalu 2005). Assessing the likely risks of providing information requires additional experience and anticipation of future events that are inherently impossible to evaluate confidently. The situation is exacerbated by the realization that, if one’s information was handled improperly, it would be extremely difficult to determine whether such mishandling had happened and then would be expensive and time-consuming to correct. Acting on privacy concerns during in-person transactions further involves an awkward and time-consuming exchange with the service agent, who is typically not used to answering detailed questions about what is done with the information collected and may hold up other clients waiting.
in line. Any possible benefits from this kind of privacy diligence are typically remote in time and place. And these are the data collection situations that are best covered by privacy protection measures. The challenge is exacerbated in situations where the personal data capture is implicit, embedded within the transaction as is normal when using ID in the form of a credit/debit, library, membership, or other type of digitally enabled card linked with an organizational database. The organization in effect “holds all the cards” in the implicit negotiating process, with the cognitive burden placed squarely on the shoulders of largely isolated individuals. From this situational perspective, who can be surprised then that even those most concerned about their privacy will generally comply, without delay or voicing misgivings, with the data collection regimes they encounter in everyday life?

Focus on Data Collection

A third limitation of privacy is its strong emphasis on the early data collection stage of the information life cycle within organizational information systems while having relatively little to say about the organizational actions based on the collected information. This limitation relates directly to the previous point about the difficulty that an individual data subject faces in anticipating how his information may be used. Much more important to an individual than whether the collecting organization strictly follows fair information practices is whether the outcome will be detrimental to the individual’s interest. If an individual is adversely affected, it matters little to her that her data were collected and processed lawfully. Conversely, if information handling was sloppy but the results benign, the individual is not likely to be as concerned, even though this sloppy handling might constitute a technical violation of privacy principles and perhaps even the law. This point was driven home during fieldwork on a study of attitudes and everyday practices of domestic Internet use. We were struck by the contrast between the widespread awareness of privacy issues among our informants and the almost complete ignorance or indifference to the fair information practice principles that provide the foundation for privacy protection. While everyone in the relatively small sample was aware of privacy risks, they had little expectation that once they released personal information that it would be handled accountably. They appeared to make an assessment of the trustworthiness of the site and likelihood that any harm would come to them, and based on this assessment decided whether to provide personal information (Viseu, Clement, and Aspinall 2004). Once a data subject has consented to data collection, the only opportunity provided by fair information practices for dealing with the substantive outcomes of personal information process is through the Access/Participation principle,
which provides individuals with the ability to view the data collected and to verify and contest its accuracy. It gives no right to contest the validity of the results that are based on the collected data, such as whether a benefit is denied. By focusing only on the procedural aspects of information handling and providing the data subject with decisional authority only at the point of data collection rather than when the organization acts on the information, a privacy approach offers very little in the way of remedial tools for addressing problematic personal information situations.

**Informational Scope**

The fourth and final major limitation of a privacy framework for addressing ID-based transactions is that privacy regulations are confined to handling only what is considered personal information and hence do not include information about an individual that is publicly available. Information about an individual that has been obtained from a published source, such as the home address and phone number that appear in a telephone directory or date and city of birth posted to a social networking site, does not enjoy privacy protection, yet it is commonly used as the basis for distinguishing individuals and making decisions about them.

Table 3.1 summarizes the various limitations of the conventional privacy framework related to failure in organizational systems to properly use per-

<table>
<thead>
<tr>
<th>Table 3.1. Summary of Privacy Framework Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Semantic Complexity</strong></td>
</tr>
<tr>
<td><strong>Semantic Complexity</strong></td>
</tr>
<tr>
<td>Privacy, in organizational transactional situations, has a wide range of sometimes conflicting meanings (e.g., withholding information versus expecting organizational accountability for information provided).</td>
</tr>
<tr>
<td><strong>Semantic Complexity</strong></td>
</tr>
<tr>
<td>Requires an anticipatory assessment of the risks at a time when the data subject is at a negotiating disadvantage. Benefits of complying with organizational requirements are immediate and tangible. Benefits of personal data protection are distant and uncertain.</td>
</tr>
<tr>
<td><strong>Focus of Attention</strong></td>
</tr>
<tr>
<td>Focuses mainly on the procedural aspects of data collection, before the data subject is aware of how she will be treated based on the information provided.</td>
</tr>
<tr>
<td><strong>Informational Scope</strong></td>
</tr>
<tr>
<td>Excludes attention to data from public sources or that which is generated by the organization.</td>
</tr>
</tbody>
</table>
sonal information in making service or other transactional decisions. These limitations help account in part for why it is hard for individuals to act in pursuit of their own immediate privacy concerns. This failure further undermines any willingness to join others similarly positioned in building a social movement around privacy rights that could develop sustained pressure for reform of prevailing personal-information-handling practices (Clement and Hurrell 2008). These limitations also provide a strong incentive for exploring other more promising frameworks for addressing such situations. In particular, the key shortcomings of the privacy framework that an alternative needs to overcome are the adverse judgments made about individuals and the heavy onus it places on them to make prudent decisions about the release of information about themselves. It is the central claim of this chapter that an identity rights framework offers such a promising alternative approach. It is to articulating such an identity framework that we now turn.

**AN IDENTITY FRAMEWORK ALTERNATIVE TO PRIVACY**

A first step in developing an alternative identity rights framework for addressing unwarranted denial of a service or access request is to recognize that identity is a common and central feature. We introduced earlier the term *identity impairment* to characterize such situations because it draws attention to the fact that a person’s standing or reputation, his “identity” in short, at least in the eyes of the organization, is compromised and/or unjustified. Identity here refers not to a singular, all-encompassing ideal of the entire person, but more simply to who the person *is* in relation to a particular organization, and possibly even to a specific time, place, and transactional context.

Earlier we observed that a shortcoming of a privacy framework was the imprecision of the term *privacy* because it is subject to multiple and even contradictory readings. *Identity* potentially faces a similar, or even more severe, limitation, given its very wide use and disparate interpretations across a broad range of disciplines and settings. Often identity refers to a form of collective affiliation, such as through gender, race, nationality, ethnicity, or linguistic competence, that unitea potentially large number of people with a common, shared “identity.” These factors, and many others, are no doubt important from the point of view of an individual in her own sense of who she is and perhaps also for the organizations she encounters. This chapter, however, takes a much narrower interpretation of “identity” in the context of interacting with organizations and their information systems. In this setting, identity is typically about individuating persons from one another to address a person according to the specificities of her situation, as reflected in the
organizational database records associated with that particular person. This individuation is often a precondition for assigning individuals to predefined categories for subsequent treatment in a process Gandy (1993) has termed more generally the panoptic sort.

These situations of social sorting are increasingly common as governments and private sector enterprises respond to growing pressures to provide service in online environments and as authenticating individual identities is viewed as one of the principal security tools at a time of heightened insecurity associated with the “war on terror.” Establishing the identity of individuals in transactional settings, or simply identification, is thus becoming a major preoccupation of service-providing organizations. From their point of view, the essential first step in a transaction is to determine whether the person presenting herself is already in their database and then to look up her records to assess eligibility and otherwise determine how to respond to the particular request. A good indication of this organization-centered view of identity comes from the authoritative definition used by the Government of Canada. The Senior Director, Identity Management and Security, Chief Information Office Branch, Treasury Board Secretariat,5 gave this standard interpretation of identity at an annual joint meeting of U.S. and Canadian government officials: Identity: a reference or designation used to distinguish a unique and particular individual (Boucher 2007, slide 8).

Typically the “reference or designation” is in the form of a unique identifier, such as a driver’s license number, social security or insurance number,6 passport number, student number or bank account number, that directly links the person to the records about that individual in the organization’s database. Often this number, together with the person’s name, facial image, and other information about the data subject stored in the organizational database is printed on an ID card issued to the individual for presentation on the occasions of subsequent service or access requests (Lyon 2009). The main function of the ID card in this case is to expedite the location of correct database records to use in determining the authoritative organizational handling of the transaction.

A Citizen-Centered Definition of Identity

The interpretation and practices around the concept of identity discussed so far clearly and quite understandably reflect an organization-centered identity perspective, consistent with a central objective of “making sure we are dealing with the right person” (Boucher 2007, slide 7). However, from the point of view of individuals encountering a service transaction, who overwhelmingly are legitimate and law-abiding, this form of unique individuation is not
their primary concern. They already know they are the persons they claim to be, so the key identity question for them is whether they will be recognized by the organization as entitled subjects or more generally enabled to proceed with the requested transactions (Clement et al. 2008).

In shifting away from an exclusively organization/system-centered view of identity to incorporate what also matters to the identity subject—being recognized as a legitimate and entitled person in relation to the specific organization and transaction—we can refine the definition of a person’s “identity” given previously to the following: Identity: a reference or designation associated with an individual, consisting of information about that person enduringly linked with categorical judgments assigned by an organization to confirm a status or conduct a transaction.

There are three key points to note here about this more “citizen-centric” interpretation of identity. First, that the essence of identity for citizens or clients is not just their personal information (e.g., name, date of birth, etc.) but also their standing vis-à-vis the organization with which they are dealing. In short, it is mainly about the person’s “reputation” with respect to the organization in question.

Secondly, and flowing from this first point, is that identity records are more than the “personal information” normally considered in privacy discourse and specifically include the categorical assignments made by (identity assigning and data holding) organizations. This wider view shifts attention from the data collection, storage, and management practices that are central to privacy protection and helps focus on the key judgments organizations make about individuals based on the information so collected. Arguably, from the point of view of the individual “identity-subject,” the organizational actions taken that affect the outcome of everyday transactions as well as cumulatively a person’s life chances are more consequential than those related to privacy concerns.

Thirdly, this definition of identity does not presuppose a singular, essential identity that is applicable across all transactions and which opens the door to all appropriate service and access entitlements. Rather, analogous to the multiple cards carried in one’s wallet, a person will possess multiple, partial identities that are each specific to purpose, organization, and other contextual features. Indeed, according to this view identity is not simply a static “fact” about a person but is closely akin to the possible roles that a person can present or perform in the various facets of her life.

This refined, more citizen-centric, contextually sensitive understanding of identity also helps show better how much is at stake for individuals as well as organizations in the decision-making process, and hence why identity is a sensitive concern and so politically charged for many people.
Comparing Identity and Privacy Interests

With this understanding of identity in mind, we are now in a position to begin comparing identity and privacy frameworks in dealing with identity impairments. In particular we will review how an identity integrity perspective addresses the limitations of privacy frameworks discussed earlier.

The service transactions discussed so far present several aspects of interest from a privacy and fair information practice point of view. Briefly, the focus is mainly on the points of data collection and whether the information is “minimal” for the stated purposes and is obtained with appropriate authority and/or consent. And once collected from the data subject, as long as the organization maintains the security, confidentiality, and accuracy of the personal information, uses it only in keeping with the stated purpose, and ensures that any third parties who have access to the personal data comply with the same terms, the privacy interest is satisfied. Nor is there a privacy interest in any information about the person that is not considered “personal” such as that obtained from public sources. This situation is represented schematically in figure 3.1.

The organization has no privacy responsibility to account for the decisions it makes based on the data, regardless of how unfair the decision making may be or how detrimental the consequences. There may be other forms of accountability and responsibility that the organization may be subject to, but these will be specific to the particular context of the decision.

An identity perspective on personal information attempts, as a privacy one does as well, to apply to a wide range of situations where information about

Figure 3.1. Privacy interests in an organizational database of personal information.
a person is directly involved. When we adopt such an identity perspective, the interest shifts to the points where the organization makes judgments about the status or entitlements of the individual. It is helpful here to distinguish between two different processes—initial enrollment in the organization’s information system (represented schematically in figure 3.2), and subsequent authentication and authorization for transactions (represented schematically in figure 3.3). In particular, in the enrollment process, the identity interest centers on decision making about whether the subject is eligible to be enrolled (the “OK?” decision diamond in figure 2), issuing an ID token or card, and assigning the subject a particular status or category of “member.” These are all matters beyond the scope of privacy interest because this is how an organization produces new data about the person, not how it collects it from the person. This point is made clearer in the case where the organization collects data from public sources. The organization is exempt from any privacy claim from the individual, regardless of what it does with the data about that person. However, an identity interest can be invoked once the organization makes a judgment about that person.

An identity interest is principally invoked in the authentication/authorization stage because this is when any decisions the organization makes become
directly consequential for the individual. If either the person is not recognized as a “member” of the organization, or if is so recognized but deemed ineligible, the transaction request will be denied. This point is represented by the “OK?” decision diamond in figure 3; this time, however, it refers to denying or granting the requested service, rather than whether to enroll an applicant. This authentication/authorization situation is devoid of any new privacy interest, while an identity interest can focus on whether the denial is justified. This is the point at which an identity subject experiences the consequences of an organizational decision and is likely well motivated to complain, request explanations, enroll allies, and generally attempt to hold the organization to account. Such holding to account will likely not be easy, particularly because the aggrieved person has to start from the position of an isolated individual. But he will be in a much stronger bargaining position than if he has to rely on privacy arguments, which would involve reconstructing the data trails and then challenging consent procedures at the earlier point of collection.

We can now return to consider in turn each of the four limitations a privacy framework faces in dealing with identity impairments. These are summarized in table 3.2. We can see from this analysis that by focusing mainly on organizational judgments about individuals, an identity ap-
proach enjoys a relative conceptual tightness that has so far been hard to achieve with an exclusively privacy focus. While it may be difficult for an individual to challenge an adverse decision, she will nevertheless be in a much better position motivationally to assert rights and seek redress. An identity framework places the attention on the proximate phenomenon (the adverse decision), whereas tracing back the personal data trails to

<table>
<thead>
<tr>
<th>Table 3.2. Summary Comparison of Privacy and Identity Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy Framework Limitations</strong></td>
</tr>
<tr>
<td><strong>Identity Framework Relative Advantages</strong></td>
</tr>
<tr>
<td><strong>Semantic Complexity</strong></td>
</tr>
<tr>
<td>Broad, ambiguous Privacy, in organizational transactional situations, has a wide range of sometimes conflicting meanings (e.g., withholding information versus expecting organizational accountability for information provided).</td>
</tr>
<tr>
<td><strong>Situational Practicality</strong></td>
</tr>
<tr>
<td>Difficult Requires an anticipatory assessment of the risks at a time when the data subject is at a negotiating disadvantage. Benefits of complying with organizational requirements are immediate and tangible. Benefits of personal data protection are distant and uncertain.</td>
</tr>
<tr>
<td><strong>Focus of Attention</strong></td>
</tr>
<tr>
<td>Collection Procedure Focuses mainly on the procedural aspects of data collection, before the data subject is aware of how she will be treated based on the information provided.</td>
</tr>
<tr>
<td><strong>Informational Scope</strong></td>
</tr>
<tr>
<td>Limited to “Personal” Information Excludes attention to data from public sources or that which is generated by the organization.</td>
</tr>
</tbody>
</table>
determine whether there was any improper handling, as a privacy orientation would call for, would be very much more difficult and discouraging. This difference is due in large part because the privacy interest is mainly invoked during data collection, which may have been scattered across time and space. And finally, the identity approach would not be diverted by having to consider whether the information upon which a particular decision was based was “personal” in legal terms. Regardless of the source of its information, an organization should still be accountable for its judgment about the individuals it deals with.

TOWARD IDENTITY RIGHTS

A clear conception of identity is only one ingredient of an identity framework. It is common for organizations when developing identity rules and procedures, as with other complex policy areas, also to formulate concise sets of overarching principles. These are intended to focus discussion on central identity questions and guide subsequent action. The Government of Canada’s efforts in this regard provide useful insight into how a large organization approaches the complex challenges of creating a consistent and workable identity management regime. The Treasury Board Secretariat, the central coordinating body for the Canadian Government, articulated a set of eleven Identity Principles “intended to apply throughout the entire government in contexts where identity is an issue or consideration.”

These government principles provide a useful basis for developing organizational identity management policies and practices. They address some of the central concerns of identity management, such as the need for lawfulness, transparency, and public trust. Each principle is distinctively valuable, and all are necessary. However, this list, as well as the conceptual framework and the assumptions that underlie them, are limited in several important respects and so are not a sufficient foundation for proper identity management. In addition to the reconceptualization of basic identity definitions as discussed above, such limitations call for additional principles derived more broadly. Reflecting a drafting process conducted exclusively within the Government of Canada, this formulation understandably adopts a organization-centered view of identity. Appropriately, the various principles repeatedly begin with the phrase, “The Government of Canada will . . . ” However, several important dimensions of identity policy are missing—most notably a client-centered focus incorporating the perspectives of individual “identity subjects” as well as a grounding in constitutional human/civil rights rather than just organizational/bureaucratic mandates.
Chapter 3

Guiding Identity Precept

One of the greatest risks run by a government or other organization in establishing rules and procedures related to identity is political (Boa et al. 2007). That is, identity rules and procedures, like any others involving personal data collection and processing (especially ones that decisively define status in society or in relation to powerful organizations as identity schemes of broad scope do), hinge on public trust. If the identity authority does not earn public trust in its identity scheme, it risks rejection of the scheme and its own legitimacy. The recent UK elections provide a vivid example of the political consequences that can befall a government that attempts to impose an identity scheme without garnering popular support. The first legislative act of the Conservative–Liberal Democrat coalition was the introduction of the Identity Documents Bill 2010, which repeals the previous Labour Government’s Identity Cards Act 2006, cancels the National ID card program, and requires the destruction of the information held on the National Identity Register.11 Posed positively, this change suggests the following broad precept for guiding identity policy development:

For any jurisdictional or organizational identity system to be legitimate and effective in achieving its intended purposes, it must earn wide acceptance and trust among the relevant public or client group based on transparency and accountability.

To give this precept practical value, more specific principles are needed. There are various ways for developing such principles, depending on the perspective one adopts. Rather than combining these principles into a single integrated list from the start, we will here explore several approaches to identity, each from a different perspective, bringing along their associated conceptual presumptions and interests. At this point we are aiming for a relatively comprehensive treatment, which will mean some overlap and duplication, which provides the basis for a subsequent consolidation into a tighter framework with less redundancy.

Some Fundamental Rights in Relation to Identity

Identity documentation is the *sine qua non* of “citizenship,” in any of its forms, such as for voting, traveling abroad, claiming an entitlement, or receiving a benefit. Hence it needs ultimately to rest on, as well as reinforce, the fundamental rights of formal citizenship. In Canada, these citizenship rights are most definitively spelled out in the Canadian Charter of Rights and Freedoms.12 This Charter, passed in 1982 as part of the Constitution Act,
is relatively young in comparison with constitutions internationally, and it draws extensively on them for core principles. There have so far been few cases in the personal information area on which the Canadian Supreme Court has rendered authoritative rulings, giving more precise interpretation of the Charter’s sweeping ideals. Nevertheless, the Charter represents a clear and succinct statement of societal norms, specifying the rights that everyone, including those charged with serious crimes, can enjoy. It therefore offers a good starting point for thinking about the rights individuals should enjoy in their dealings with any organization in society. Sections 7, 8, 9, 10, 11, 15, and 27 of the Charter are the most pertinent to identity rights:13

Sec. 7. Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.

Sec. 8. Everyone has the right to be secure against unreasonable search or seizure.

Sec. 9. Everyone has the right not to be arbitrarily detained or imprisoned.

Sec. 10. Everyone has the right on arrest or detention
a) to be informed promptly of the reasons therefore;

b) to retain and instruct counsel without delay and to be informed of that right; and

c) to have the validity of the detention determined by way of habeas corpus and to be released if the detention is not lawful.

Sec. 11. Any person charged with an offence has the right . . .

d) to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal;

Sec. 15. (1) Every individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability. (2) Subsection (1) does not preclude any law, program or activity that has as its object the amelioration of conditions of disadvantaged individuals or groups including those that are disadvantaged because of race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.

Sec. 27. This Charter shall be interpreted in a manner consistent with the preservation and enhancement of the multicultural heritage of Canadians.

Based on a lay reading of these particular sections, here are four proposed rights pertaining to identity:

1. Integrity of (Personal) Identity. Everyone has the right to the integrity of her personal identity. This is the most fundamental of the distinctive iden-
Chapter 3

101
tity rights. Like the closely related right to privacy, it can be based directly on the constitutional right of “security of the person” (sec. 7) and “to be secure against unreasonable search and seizure” (sec. 8). In keeping with the definition of identity mentioned above, this right includes the right to reliable identity documentation and goes beyond personal information protection to include the judgments about the person made by an authority based on these data, such as profiling, categorical treatment, and the like.

2. Presumption of Anonymous Entitlement. When an individual asserts a claim for entitlement or to conduct a transaction, the initial presumption is that he is so entitled by virtue of his existence. Where there is a requirement to deviate from this presumption, the responsibility is on the authority to justify the need to go beyond anonymity and establish some form of pseudonymity or collective or individual identity. This right is founded on sec. 11d: presumption of innocence. The presumption of innocence is designed to protect the relatively weak individual in the face of a more powerful organization by placing the burden of proof of “suspicion” or “guilt” on that organization. Similarly, it should be possible for individuals to conduct many of their everyday affairs anonymously, without having to reveal who they are. There are, of course, also many instances where it is necessary for an organization to know some specific details about the person it is transacting business with, such as when making a delivery to a particular address or determining whether an age requirement is met. Strict anonymity is therefore not an absolute right. In such cases, starting with an initial presumption of anonymity, an organization that needs more personal information should demonstrably justify the specific additional information it needs.

3. Judgmental Transparency and Accountability. Where an agency has made an (enduring categorical) adverse judgment about an individual, this judgment shall not be made arbitrarily. That person has the right a) to be informed promptly of the reasons therefore; b) to retain and instruct expert advice without delay and to be informed of that right; and c) to have the validity of the judgment determined by way of habeas corpus and to be reversed if the judgment is not justifiable. This right is based in sec. 9 and 10: Arrest or detention. Being denied access or service that one is normally entitled to is a form of arrest, albeit typically much milder than arrest and detention by law enforcement authorities. Similarly, requiring personal information of an individual is akin to search and seizure, again milder than when performed by police backed by arms. Nevertheless, no organization should deny access or demand personal information in an arbitrary, opaque, or unaccountable fashion. Everyone whose identity is impaired in some way by an organization should be informed of the reasons and given the opportunity to challenge the judgment in a timely fashion, assisted as needed by competent experts.
4. Equality, Diversity, and Cultural Inclusion. Every individual will be treated equally in terms of identity documentation and practices, recognizing our multicultural heritage. This right is based in sec. 15: Equality, and sec. 27: Multicultural heritage. Many of the principal elements for determining identities, such as names, their number, ordering, spelling, and length; and facial images have differing meanings and sensitivities across various cultures. Dominant Anglo American norms about names and facial images do not translate easily to other linguistic, cultural, and religious traditions. ID schemes need to be sufficiently flexible to adapt to the preferences of significant minority communities.

Fair Identity/Information Practice Principles?

It is evident that the policy issues around identity management are closely related to those around privacy protection. Indeed, in some cases they are indistinguishable. However, with the making of enduring categorical judgments about individuals by organizations recorded as part of the person’s “identity package,” there are some important distinctive and novel elements about identity that warrant reformulating the familiar privacy principles of fair information practice to take account of these organizational judgments about individuals. The U.S. Department of Health, Education, and Welfare provided the first comprehensive articulation of fair information practice principles (FIP) in 1973. The other jurisdictions that have developed privacy or data protection legislation have drawn on and extended these principles. The most widely applied Canadian version of fair information practices is articulated in the Canadian Standards Association (CSA) Model Code, subsequently incorporated into the Personal Information Protection and Electronic Documents Act (PIPEDA), which largely governs private sector personal information in Canada. In light of our identity concerns, we have modified each of the ten CSA FIP principles to highlight the corresponding identity issue. This Code and the principles it enumerates reflect the perspective and responsibilities of an organization that is a custodian of personal information and that makes and records judgments about individuals on the basis of this information. In what follows, the phrase identity judgments refers to the categorical assignments made by the organization about the individual that become part of the stored records about that individual. Changes to the original privacy/data protection text are shown italicized.

1. Accountability. An organization is responsible for personal information and identity judgments under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.
2. Identifying Purposes. The purposes for which personal information is collected and identity judgments made shall be identified by the organization at or before the time the information is collected.

3. Consent. The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, as well as in making identity judgments, except where inappropriate.

4. Limiting Collection. The collection of personal information and making of identity judgments shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected and identity judgments made by fair and lawful means.

5. Limiting Use, Disclosure, and Retention. Personal information, including identity judgments, shall not be used or disclosed for purposes other than those for which it was collected or made, except with the consent of the individual or as required by law. Personal information, including identity judgments, shall be retained only as long as necessary for the fulfillment of those purposes.

6. Accuracy. Personal information, including identity judgments, shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards. Personal information, including identity judgments, shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness. An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information and the making of identity judgments.

9. Individual Access. Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, as well as the making of identity judgments, and shall be given access to that information and identity judgment-making process. An individual shall be able to challenge the accuracy and completeness of the information as well as the identity judgment-making process and have them amended as appropriate.

10. Challenging Compliance. An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.

These ten principles can be supplemented by eight more, which can also serve usefully to regulate organizational practices around identity.

11. Identity minimization. An organization shall minimize the degree of identification required of an individual, preferably conducting transactions anonymously or pseudonymously.

12. Identity Repair and Mitigation. Where a person’s identity has been impaired unjustifiably, the organization shall repair and mitigate the harm
done, compensate the individual appropriately, and take reasonable steps to avoid recurrence.

13. **Identity Breach Publicity.** When an organization breaches its identity management responsibilities, it shall publicize appropriately any such breach, proportionate to its severity and taking due account of the privacy rights of any individuals affected.

14. **Universal Accessibility.** An organization shall ensure that its identity documentation and practices are accessible for all, regardless of age, disability, language preference, education, and income. In particular, communications must be clear and understandable via interfaces that are humanly comprehensible and controllable.

15. **Proportionality.** An organization shall ensure that the means, criteria, and costs of assuring identity are proportionate to the intended purposes, benefits expected, risks incurred, and control that can be exercised by each party.

16. **Reciprocity.** An organization shall ensure that to the greatest extent feasible, identity transactions will be based on reciprocal rights and responsibilities by minimizing the effect of power differentials between it and its clients.

17. **Pluralism of Operators and Technologies.** The interoperability of different identity technologies and their providers must be enabled by the identity scheme (“universal identity metasystem”). Both the interoperability and segregations of identity technologies may offer users more choices and control over the means of identification across different contexts.

18. **Consistent Experience across Contexts: Enhanced User Empowerment and Control.** The identity scheme (“unifying identity metasystem”) must guarantee its users a simple consistent experience while enabling the separation of contexts through multiple operators and technologies.

**Identity System Desiderata**

Flowing from and assuming compliance with these foundational identity rights and fair practice principles, the following are intended to serve as criteria for assessing jurisdictional identity systems from the perspective of various outsiders, e.g., identity subjects, citizens, consumers, clients, civil society organizations, legislators, and technical experts. In some cases these desiderata repeat themes mentioned above as part of the Fair Identity Practice principles, but here the emphasis shifts from individual usage to the scheme as a whole identity package of organization, technical system, practices, regulation, and governance.

These desiderata range from those deemed important in any large-scale, organizationwide infrastructure to those that are specifically relevant to identity systems:
Transparency of objectives, standards, processes, and redress mechanisms to facilitate individual empowerment and collective accountability.

Accountability of the ID operation and its identity activities to democratic norms and institutions, achieved through independent oversight by competent technical, legal, and political authorities.

Necessity. The need for the identity system is clearly demonstrated.

Clear purpose specification. The identity system has a clear, publicly stated, and broadly accepted purpose.

Effectiveness. The identity system demonstrably achieves the stated purpose.

Cost effectiveness. The identity system demonstrably achieves the stated purpose in an efficient manner.

Client-Centeredness. The identity system is organized around the needs and rights of individuals rather than predominantly administrative priorities.

Proportionality of means to justifiable risks and desired ends.

Minimization of civil liberty risks and effective mitigation of risks where unavoidable.

Multiple, purpose-specific ID token/systems, rather than a single, all-purpose ID token/system.

Open technical standards to avoid reliance on “security though obscurity” and facilitate testing by independent experts.

Technical neutrality, to avoid vendor dependence.

Eligibility authentication rather than identity authentication where feasible (e.g., by using “electronic signature cards” rather than “ID cards”).

Two-way device and authority authentication so that individuals conducting identity transactions can as quickly and easily check the authority for the collection of personal information and subsequent judgments as the agency checks the individual for identity assurance.

Back-up ID documents readily available in case of loss or theft.

No central storage of biometrics, as this presents unacceptable risks of being compromised.

Identity System Development Desiderata

The principles or desiderata sketched so far pertain to properties of an identity management regime once established. The processes for developing the regime in the first place and keeping it “on track” need to be consistent with the desired outcome. There are many well-recognized principles for developing and maintaining complex institutional information systems. Here we list a few that are especially relevant given the particular challenges that developing a jurisdictional identity system face:
Participatory Design. Since a jurisdictional or organizational identity system so vitally affects individual clients as well as society more broadly, it is vital that all the stakeholders have an effective influence over its development. This influence requires the active, facilitated, informed, effective, and resourced civil society participation throughout the development process.

Social Impact Assessment-Driven. The development should involve from the beginning social impact assessment (SIA) and design approaches facilitated by competent experts and publicly accountable bodies that take appropriate account of the privacy, civil liberties, equity, and other relevant social/cultural issues. Such SIA’s should play a formative role in the early stages where they can help avoid problems before they emerge and become difficult to remedy.

Identity Practice Foundations. The design process needs to be grounded in a clear appreciation of the identity practices of individuals in everyday lived situations. It is conventional in the design of complex informational/institutional systems to take a top-down, deductive approach. But to achieve the good operational fit on which effective performance and public trust rely, the design of identity tokens, systems, and rules need also to be grounded in the particular ways people acquire and handle their identity documents and engage with relevant organizations.

Privacy Enhancing/Preserving Techniques. The full range of up-to-date privacy enhancing (and preserving) technologies (PETs) and methods (e.g., encryption, digital credentials, and others mentioned earlier) should be considered for appropriate incorporation into the identity system.

Ongoing Assessment and Redesign. To ensure that an identity system continues to meet its objectives even as these may shift, there needs to be ongoing mechanisms for feedback about scheme strengths and weaknesses as well as regular systematic assessments of performance, both of which are linked to revising the scheme in light of emerging difficulties, needs, and opportunities.

Prospects for an Identity Rights Framework for Personal Information

The identity framework and specific sets of principles presented above build on and contribute new ingredients to the prior work that has been done in the areas of privacy and identity. However, we are still at an early stage in formulating workable guidelines. Their very number and diversity so far illustrate the complexity of the issues involved but at the same time point to significant limitations in the usefulness of these principles and the need for further refinement.

First, these principles should be subject to usual tests of necessity, completeness, clarity, parsimony, and relevance. It is this last characteristic that
is probably the biggest challenge since so little is known about the ways that people engage in identification practices in their daily lives. This lack of knowledge calls for significant empirical research to elicit the understandings people have about identity as well as what their needs and desires are around identity. In the absence of such grounded research, any formulation of general principles is suspect.

A further step is to turn each of these principles into clear tests that can be applied in practice to identity systems, both proposed and in operation. Strong tests, such as those outlined in the final section of CAN ID? Visions for Canada’s Identity Policy (Boa et al. 2007), will be valuable in assessing clearly whether the corresponding principles have been observed properly or not. Without such operationalization, even the most refined set of principles will be useless, or even dangerous, if they are used to promote identity systems that then cannot be held to account by citizens or independent oversight bodies.

One of the most compelling forms of operationalization of information rights principles is the working implementation of a technology that exemplifies and reinforces the principles. Recent cryptographically based research and development has demonstrated the feasibility of identity schemes that are not based on the conventional full identification approach but rather are based on user-centric principles similar to those mentioned above. Of particular note in this regard is the U-Prove suite of minimal disclosure techniques developed by Stefan Brands (2000) and colleagues at Credentica and released publicly in March 2010 by Microsoft under open licenses (Cameron 2010). U-Prove, in a significant departure from conventional identification methods, relies on cryptographically verifiable certificates of specific identity assertions, such as year of birth, age greater than a given threshold, membership in a particular group, and so on, while withholding all other aspects of a subject’s identity that are not needed for the transaction. So far this minimal disclosure approach has mainly been tested experimentally in online transaction settings and has yet to be widely adopted by government or commercial enterprises.18

But refined principles, strong tests, and working prototypes taken together will not by themselves reform identification and related personal information handling practices. This transformation will likely require sustained social, economic, and political pressure on the part of the public. And it is here that an identity rights approach to personal information holds the promise of succeeding beyond where privacy measures have taken us. We are shifting the focus of attention from informed consent at the moment of data collection to the categorical judgments made by organizations at the point and moment of service, as well as shifting the burden of proof from the individual toward
the organization. By doing so, individuals may be more able to grasp the significance of the mishandling of their personal information and be willing to act on that mishandling. Of course, if individuals suffering egregious identity impairments remain uninformed and isolated from each other, then sustained pressure for reform will remain weak. But a public discourse around identity rights that allows many people to see more clearly the alignment of their personal and collective interests can help overcome these obstacles of fragmentation and inertia. A focus on organizational misjudgements leading to identity impairment could help individuals view their own experiences and potential identity injuries as part of a wider phenomenon in which they have a vital stake. More people coming to regard such routine institutional sorting processes as directly linked to who they are and can be can become a powerful impetus for reform. A robust identity framework (Clement and Hurrell 2008), in combination with privacy protections and as a prominent part of a wider information rights social movement, could help bring the democratically accountable and responsive information environment that we need and deserve.

NOTES

1. For more on no-fly watch lists, such as Secure Flight (U.S.) and Passenger Protect (Canada) and the problems these can lead to for otherwise innocent citizens, see: http://en.wikipedia.org/wiki/No-fly_list and the websites developed by the American Civil Liberties Union (ACLU) http://www.aclu.org/national-security/aclu-challenges-government-no-fly-list and the Canadian-based International Civil Liberties Monitoring Group (ICLMG) http://travelwatchlist.ca/.

2. For a good starting point for the extensive materials on Maher Arar’s case, see http://en.wikipedia.org/wiki/Maher_Arar. For the “Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Commission),” see http://www.fedpubs.com/subject/govern/arar.htm.


4. It could be argued that other vital political ideals, such as liberty or free expression, similarly lack precision without jeopardizing their value. But privacy appears to be especially fraught with internal inconsistency and competing concepts, such as “right to be left alone” versus “informational self-determination” mentioned earlier.

5. Treasury Board is the cabinet-level committee in charge of much of the operation of the Canadian government. It is equivalent to the U.S. Office of Management and Budget.
6. Social Security Number (SSN) in the U.S. or Social Insurance Number (SIN) in Canada.

7. Various terms similar to citizen-centric can be found in the discussion of identity management frameworks—including user-, consumer-, customer-, and client-centric identity. We use citizen- here in the informal sense, since the argument applies to rights that individuals should enjoy not only in their relations with governmental agencies, but more broadly in relation to other organizations to which they “belong” in some way and thereby enjoy rights with respect to.

8. This view of identity is consistent with Roger Clarke’s interpretation of identities, as distinct from entities (2010).

9. Sometimes, of course, these two processes appear to the data subject to happen simultaneously.

10. Treasury Board Secretariat Identity Principles:

Principle 1. Justify the Use of Identity: The Government of Canada will identify individuals and businesses only when it is authorized by legislation, policy, or program mandates.

Principle 2. Identify with Specific Reason: The Government of Canada will identify individuals and businesses only when there is a specific reason to do so.

Principle 3. Use Appropriate Methods: The Government of Canada will use acceptable and appropriate means to identify individuals and businesses.

Principle 4. Use a Risk-Based Approach: The Government of Canada will use a comprehensive, risk-based approach to identity management that balances all relevant considerations, including privacy and security.


Principle 8. Enable Consistency, Availability, and Interoperability: Through a governmentwide approach to identity, the Government of Canada will enable consistency, availability, and interoperability of government programs and services.


Principle 10. Be Collectively Responsible: The Government of Canada recognizes that identity is the collective responsibility of all governments and the individuals they serve.

Principle 11. Preserve Proportionality: The Government of Canada will ensure that identity management activities remain within their intended scope and jurisdiction and are proportional to the stated goals (Bouma 2006, slide 18).


13. Within the U.S. Constitution, these sections correspond most closely to the
Fourth Amendment. See: http://www.usconstitution.net/constquick.html.


15. Derived from the Canadian Standards Association (CSA) Privacy Principles
&language=english.


17. The last two principles are inspired by Microsoft’s “7 Laws of Identity,”
notably “laws” 5 and 7 (Pluralism of Operators and Technologies and Consistent
Experience across Contexts) that go beyond single organizations and require at least
governmentwide or industrywide coordination. The wording here is drawn directly
from the Ontario Information and Privacy Commissioner’s reinterpretation of these
laws (Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada,
2006. 7 laws of identity: The case for privacy-embedded laws of identity in the digital
age. http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-
Summary/?id=470). As the OPC notes, all seven laws are highly consistent with
well-established privacy principles. The other “laws” that are oriented to individual
identity handling organizations, notably 1–4 and 6, can be found in the first fifteen
principles listed here.

18. One experimental implementation of the U-Prove technology using physical
ID cards for use during in-person as well as online transactions is being conducted by
the Fraunhofer FOKUS Institute in Germany. It aims to demonstrate interoperability
with the German eID card system. The current author (Clement 2010) is also taking
a similar approach in the “Proportionate ID Digital Wallet” project, which is using
smartphones for prototyping user-centric, minimal disclosure ID tokens (see http://
iprp.ischool.utoronto.ca/Prop-ID).

REFERENCES

Akalu, Rajen et al. 2005. Implementing PIPEDA: A review of Internet privacy state-
ments and on-line practices. A report to the Office of the Privacy Commissioner
of Canada.

Boa, Krista, Andrew Clement, Simon Davies, and Gus Hosein. 2007. CAN ID?
Visions for Canada’s identity policy: Understanding identity policy and policy
archive.iprp.ischool.utoronto.ca/publications/PDFs/CAN-ID/CAN-IDreportv2ga-
Jul3.pdf

Boucher, Pierre. 2007. Identity management in the Government of Canada. Presen-
CanadaPierreBoucherIDmanagement.pdf

Bouma, Tim. 2006. Identity: Setting the larger context, achieving the right outcomes.
Presentation at CACR Privacy and Security Conference. Slides and a video of the pre-


