A Macdonald-Laurier Institute Publication

# Finding the Balance on Digital Privacy

## Toward a New Canadian Model for Data Protection in the 21st Century

Solveig Singleton

June 2014

MLI
Macdonald-Laurier Institute

MACDONALD-LAURIER INSTITUTE

*True North in Canadian Public Policy*



## Board of Directors

**CHAIR**
**Rob Wildeboer**
Executive Chairman, Martinrea International Inc., Vaughan

**VICE CHAIR**
**Jacquelyn Thayer Scott**
Past President and Professor, Cape Breton University, Sydney

**MANAGING DIRECTOR**
**Brian Lee Crowley**
Former Clifford Clark Visiting Economist at Finance Canada

**SECRETARY**
**Lincoln Caylor**
Partner, Bennett Jones LLP, Toronto

**TREASURER**
**Martin MacKinnon**
Co-Founder & Chief Financial Officer, b4checkin, Halifax

**DIRECTORS**

**John Beck**
Chairman, Aecon Construction Ltd., Toronto

**Pierre Casgrain**
Director and Corporate Secretary of Casgrain & Company Limited, Montreal

**Erin Chutter**
President and CEO of Global Cobalt Corp., Vancouver

**Navjeet (Bob) Dhillon**
President and CEO, Mainstreet Equity Corp., Calgary

**Wayne Gudbranson**
CEO, Branham Group Inc., Ottawa

**Stanley Hartt**
Counsel, Norton Rose Fulbright, Toronto

**Peter John Nicholson**
Former President, Canadian Council of Academies, Ottawa

## Advisory Council

**Purdy Crawford**
Former CEO, Imasco, Counsel at Osler Hoskins

**Jim Dinning**
Former Treasurer of Alberta

**Don Drummond**
Economics Advisor to the TD Bank, Matthews Fellow in Global Policy and Distinguished Visiting Scholar at the School of Policy Studies at Queen's University

**Brian Flemming**
International lawyer, writer and policy advisor

**Robert Fulford**
Former editor of *Saturday Night* magazine, columnist with the *National Post*, Toronto

**Calvin Helin**
Aboriginal author and entrepreneur, Vancouver

**Hon. Jim Peterson**
Former federal cabinet minister, Counsel at Fasken Martineau, Toronto

**Maurice B. Tobin**
The Tobin Foundation, Washington DC

## Research Advisory Board

**Janet Ajzenstat**
Professor Emeritus of Politics, McMaster University

**Brian Ferguson**
Professor, health care economics, University of Guelph

**Jack Granatstein**
Historian and former head of the Canadian War Museum

**Patrick James**
Professor, University of Southern California

**Rainer Knopff**
Professor of Politics, University of Calgary

**Larry Martin**
George Morris Centre, University of Guelph

**Christopher Sands**
Senior Fellow, Hudson Institute, Washington DC

**William Watson**
Associate Professor of Economics, McGill University


# Table of Contents



*The author of this document has worked independently and is solely responsible for the views presented here. The opinions are not necessarily those of the Macdonald-Laurier Institute, its Directors or Supporters.*

# Executive Summary

With the federal government's recently unveiled digital strategy and new legislation, and the appointment of a new Canadian privacy commissioner, digital privacy issues are at the forefront of the policy debate. Canada's approach to protecting personal data is still evolving, and care must be taken to strike the right balance on digital privacy regulation.

Few people are against having their privacy protected, to the extent that in this digital age, privacy has come to be seen as a new human right. But privacy is not an absolute good. It can conflict with more established rights, principles, and goals such as free expression, competition, and even security from fraud. Furthermore, protecting privacy from the public sector should be treated as a fundamentally different problem than regulating data in the private sector.

This paper examines the European and US approaches to privacy protection and finds that Canada lies somewhere in between Europe, with its heavy regulatory approach, and the US, which has been more liberal.

The current European approach to protecting private information online was adopted in haste, without the refinement that comes about by considering real-world cases or considering alternative rules across different jurisdictions. The result is an abstract regime that may not mesh well with the complexities of real life or with open markets.

United States privacy law has come under fire for being inadequate compared to that of countries with more strict data protection regimes. But these observers are using extensive data protection law as a benchmark, with any departure from it being sufficient to prove inadequacy, a rather circular bit of reasoning. We should choose a more neutral benchmark, such as consumer welfare.

This paper goes on to compare data protection in Canada to more established legal regimes for information, such as copyright and trademark law, and then to consider the negative consequences for business and consumers of overbroad privacy regulation.

A more liberal regime for Canada, designed to accommodate competing principles such as free expression, competition, and economic growth, would best serve the public interest – a system more focused on describing necessary rules that target concrete harm.

## Recommendations for Data Protection Policy in Canada

- **Maintain the distinction in Canadian law between privacy rules for the public sector and rules for the private sector.** Be aware that the European model of privacy does not make a clear distinction between these spheres. This may lead that model to include rules for the public sector that are too lenient, and rules for the private sector that are too strict.
- Recognize that **data protection law is not sufficiently mature for conventional enforcement methods,** especially given the truncated nature of the process by which it has been developed.
- In trade negotiations, insist that differences between national regimes be tolerated, just as they are tolerated in areas such as judicial process, patent law, and in other areas. **Harmonization is a goal for the very long run** and has drawbacks as well as benefits.
- **Ensure that common-law concepts from contract law and tort law inform data protection decisions,** as they developed over the course of many generations in real-world conflicts and

cases, and are familiar in the commercial sector. In contract law, for example, implied consent, not explicit consent, is ordinarily perfectly acceptable. Those acting in good faith ought to be protected from extensive liability. Emotional or symbolic damage are rarely compensable, except under extreme circumstances. Penalties ought to be in proportion to the harm.

- Recognize **that the problem of rapid technological change and the complexity of the information landscape are in themselves a compelling argument for minimal data protection regulation.** Broad abstract rules are unlikely to provide enough clarity to economic actors, and will result in a regulatory regime that is a poor fit in many contexts. More specific rules are likely to become outdated rather quickly. The best way to avoid this dilemma is to adopt only minimal regulation. The second best way is to adopt responsive rules governing specific sectors (children, health care) after real problems have arisen and have been studied for some time.

- Fraud is a real problem for both consumers and merchants. **Addressing fear of financial loss, not abstract concerns about privacy, is most likely to support an atmosphere of trust online.** Enforcement resources should be narrowly focused on bad actors.

- Amend exemptions to data protection rules to **ensure that potentially conflicting principles and goals such as free expression, competition, and security are liberally accommodated.** These fundamental principles ought not to be narrowly confined by poorly articulated, narrow exemptions.

- **Maintain the Office of the Privacy Commissioner in its role as an ombudsman.** As an advocate for privacy, the office is unsuited to design neutral rules for the private sector or to decide disputes.

- **Ensure that quality controls on studies or surveys relating to privacy and funded by the public sector are in place.** Require cost-benefit analysis of rules, including anti-spam laws and data breach notification provisions.

Attention to these ideas will move Canada towards a model of privacy regulation for Canada that will support innovation and competition while protecting consumers from fraud and other real hazards.

# Sommaire

La récente stratégie numérique du gouvernement fédéral, qui a été inaugurée dans la foulée de la nouvelle loi et s'est conjuguée à la désignation d'un nouveau commissaire à la protection de la vie privée du Canada, a propulsé les questions liées à la stratégie numérique à l'avant-scène du débat politique. Alors que l'approche utilisée par le Canada pour protéger les renseignements personnels évolue encore, il importe de trouver un juste équilibre pour réglementer la protection de la vie privée numérique.

Peu nombreuses sont les personnes qui s'opposent à la protection de leur vie privée dans la mesure où cette protection est considérée, en cette ère numérique, comme un nouveau droit humain. Mais la protection de la vie privée n'est pas un bien absolu. Elle peut entrer en contradiction avec des droits, des principes et des objectifs déjà bien enracinés comme, par exemple, la liberté d'expression, la concurrence et même la protection contre la fraude. En outre, la protection de la vie privée dans le secteur public et la réglementation des données dans le secteur privé soulèvent des enjeux qui sont fondamentalement différents et qui doivent être considérés comme tels.

Dans cette étude, on examine les voies suivies en Europe et aux États-Unis en matière de protection de la vie privée et on conclut que le Canada se situe quelque part entre la lourde réglementation européenne et l'approche plus libérale adoptée aux États-Unis.

L'approche utilisée actuellement en Europe pour protéger les renseignements personnels en ligne a été adoptée dans la précipitation et ne possède donc pas la profondeur qui aurait pu émaner d'une étude de cas concrets ou des divers règlements relevant d'autres compétences. Il en a résulté un régime abstrait, qui risque d'être incapable de tenir compte des complexités de la vie actuelle ou de l'ouverture des marchés.

La loi sur la protection de la vie privée aux États-Unis a été fortement critiquée, car elle est considérée comme inadéquate par rapport aux régimes de protection des données plus contraignants mis en œuvre dans divers pays. Les observateurs érigent cependant en modèle les régimes de grande envergure et considèrent que toute disposition en rupture avec ceux-ci constitue une raison suffisante pour juger une loi inapte, un raisonnement bien tautologique. On devra choisir un modèle plus neutre, en accord par exemple avec le bien-être des consommateurs.

Dans cette étude, on compare ensuite la protection des données au Canada aux régimes légaux bien établis dans le domaine de l'information, tels que le droit d'auteur et le droit des marques de commerce, puis on examine les conséquences néfastes d'une réglementation de la vie privée excessive sur les entreprises et les consommateurs.

Un régime plus libéral au Canada, guidé par les principes en concurrence que sont, par exemple, la liberté d'expression, la concurrence et la croissance économique, servirait le mieux l'intérêt public –, soit un système visant davantage à décrire des règles protégeant contre des dommages concrets.

## Recommandations pour une politique sur la protection des données :

- **Maintenir dans la loi canadienne la distinction entre les secteurs public et privé en ce qui concerne les règles sur la protection de la vie privée.** Il faut être conscient du fait que le modèle européen n'établit pas de distinction claire entre ces deux sphères. Cela pourrait expliquer pourquoi ce modèle est assorti de règles qui sont trop tolérantes pour le secteur public, mais trop strictes pour le secteur privé.

- Reconnaître que la **loi sur la protection des données n'est pas suffisamment développée au regard des méthodes traditionnelles utilisées pour assurer qu'elle soit respectée**, en particulier compte tenu de la nature tronquée du processus par lequel elle a été conçue.

- Au cours des négociations commerciales, faire accepter les différences entre les régimes nationaux, tout comme c'est le cas déjà pour les processus judiciaires, les lois sur les brevets et bien d'autres domaines encore. L'**harmonisation est un objectif à long terme,** mais elle comporte aussi bien des avantages que des inconvénients.

- **Veiller à ce que les décisions en matière de protection des données se fondent sur les notions de la *common law* tirées du droit des contrats et de la responsabilité délictuelle**, tel qu'elles se sont développées au fil des nombreuses générations de conflits et de cas survenus dans le monde réel, et qu'elles sont connues du secteur commercial. Dans le droit des contrats, par exemple, le consentement implicite plutôt qu'explicite est habituellement parfaitement acceptable. Les personnes qui agissent de bonne foi doivent bénéficier d'une protection étendue en matière de responsabilité. Les souffrances émotionnelles ou symboliques peuvent rarement être compensées, sauf dans des circonstances extrêmes. Les peines doivent être proportionnelles aux dommages subis.

- Reconnaître **que les** développements rapides de la technologie et la **complexité du monde de l'information sont en eux-mêmes des arguments irréfutables justifiant une** réglementation minimale **en matière de protection des données**. Des règles abstraites générales seraient peu susceptibles de révéler suffisamment les acteurs économiques en jeu et rendraient le système réglementaire inapproprié à de nombreux contextes. En revanche, des règles très ciblées deviendraient rapidement obsolètes. Le meilleur moyen de résoudre cette impasse serait d'adopter une réglementation minimale. Un second choix serait d'adopter les règles permettant de régir des secteurs en particulier (enfance, services de santé) après avoir étudié un certain temps les problèmes survenus.

- La fraude représente un problème réel tant pour les consommateurs que pour les commerçants. **La confiance en ligne a davantage de chance de s'établir si on se préoccupe des craintes de pertes financières plutôt que des inquiétudes théoriques sur la protection de la vie privée.** Les ressources consacrées à l'application de la loi devraient se concentrer étroitement sur les acteurs mal intentionnés.

- Modifier les exemptions aux règles de protection des données pour **reconnaître ouvertement les principes et les objectifs potentiellement contradictoires que sont, par exemple, la liberté d'expression, la concurrence et la sécurité**. Ces principes fondamentaux ne doivent pas être limités par des exemptions étroites ou mal formulées.

- **Conserver le rôle d'ombudsman au Bureau du commissaire à la vie privée**. En tant que défenseur de la protection de la vie privée, le bureau n'est pas préparé pour concevoir des règles neutres à l'intention du secteur privé ou pour régler lui-même les différends.

- **Veiller à ce que soient mises en place des pratiques de contrôle de la qualité pour les** études ou **les enquêtes relatives à la protection de la vie privée financées par le secteur public**. Exiger une analyse coût-bénéfice des règles, y compris les lois antipourriels et les dispositions en matière de signalement des atteintes à la sécurité des renseignements.

La mise en valeur de ces idées permettra au Canada de s'orienter vers un modèle de réglementation de la protection de la vie privée qui soutiendra l'innovation et la concurrence au pays, tout en protégeant les consommateurs contre la fraude et d'autres dangers réels.

# Introduction

Data protection, the idea of broad privacy regulation of the private sector, grew up alongside computer databases in the 1970s. Data protection principles are comparatively new to the world and to Canada. Information is fluid, and the technologies and techniques used to store and transmit it are complex and changing. Privacy rules have an unfinished feel to them, and the debate about data protection is ongoing. In April of 2014, *The Act to Amend PIPEDA* (Bill S-4) was introduced, again raising the question of the best direction for the evolution of data protection laws in Canada.

The Office of the Privacy Commissioner of Canada proposed in 2013 that its authority be enhanced and expanded to give it more regulatory authority and the power to impose greater damages. Bill S-4 generally makes only very modest enhancements to the authority of the Privacy Commissioner and to the substantive rules of privacy, except for the addition of security breach disclosure rules. Following tendencies in some European Union nations, however, the idea of expansion is likely to be put forward again. Opponents of expansion note that expanding data protection would be expensive, amounting to a considerable economic burden (Descôteaux and Szoka 2013; Burt and Grant 2012). This invites the counterargument, that monetary cost ought not to be an obstacle to expanding a regime important to human rights or for consumer protection.

*We need a system more focused on rules that target concrete harm.*

This paper takes a different perspective. We analyse the coherence of conventional data protection principles as functioning parts of systems of human rights, commercial law, and consumer protection. We find that the current approach to data protection is flawed, and ought to be revisited. The dominant European model of data protection was adopted in haste, without the refinement that comes about by considering many cases over time, or considering how alternative rules across different jurisdictions worked in practice. The result is an abstract regime that often conflicts with other important legal principles and policy goals, such as free expression, competition, or even security from fraud. A more liberal regime, designed to accommodate competing principles would better serve the public interest – a system more focused on describing necessary rules that target concrete harm.

In conclusion, we draw on this analysis to offer new ideas for data protection in Canada. Policy-makers should maintain the role of the Privacy Commissioner as an advocate and recognize the value of general privacy principles (such as the idea of notice and choice) as aspirational principles or voluntary guidelines. Second, policy-makers should maintain consistency between data protection law and traditional legal concepts, including the traditional law of consent and damages. Legally enforceable rules should be minimal and be imposed only as necessary to prevent concrete harm. Enforcement resources should likewise be focused on taking direct action against the perpetrators of fraud and others acting in bad faith to do concrete harm. Many of the exceptions to data protection, such as those recognizing rights of free expression, should be expanded and strengthened, and Parliamentary mechanisms to recognize the need for this could be improved.

# I Where Are We, and How Did We Get Here? The Evolution of Data Protection in Canada and Abroad

Critiques of data protection tend to be rare. We have all become aware that technology enables a significant amount of data to leave local communities and be handled by remote strangers. The most familiar uses of data in the late twentieth century included abuse of census data during the Second World War and fictional accounts of information-processing technologies in George Orwell's *1984*. Fear and pessimism about these technology trends came to dominate the debate. Data protection has been heralded as a new human right[1] and became rapidly ensconced in the legal system in many countries.

*We have reason to be skeptical of the expansion of data protection.*

In this atmosphere, discussions of privacy regulation tend to be rather one-sided. Understandable though this may be, it is likely to lead to policies of low quality. Information is complex. Rapidly changing technology and business arrangements add another layer of complexity. Under these circumstances, insulating data protection regimes from criticism will not get good results. There is no particular reason to be pessimistic about new data-intensive technologies. Orwell's dire predictions concerning 1984 did not come to pass; computers have empowered individuals around the world in both the political and economic sphere.

In the spirit of encouraging reflection, we begin with an overview of the history of data protection. We draw attention throughout to reasons to be skeptical of the expansion of data protection.

## History in a Nutshell, and Law in a Hurry

For centuries, the ordinary rule of human interactions was that people are free to make observations about other people, communicate those observations to others, and use them in making their own plans. Informational privacy law consisted of exceptions to that general rule. The most important of these involved restraints on the public sector such as those reflected in Section 7 and 8 of the *Canadian Charter of Rights and Freedoms* (the rights to life, liberty, and security of the person, and the right to be secure against unreasonable searches). Information-gathering by the private sector had to respect property rights (you could not break into someone's house to count their spoons or read their letters, or creep up under their windows to eavesdrop) but beyond that received little legal attention outside of confidential relationships (doctor and patient, attorney and client, and so on). In some jurisdictions, the common law evolved variations on this theme such as the invasion of privacy torts, but not many.[2]

This began to change in the 1970s. Motivated powerfully by the history of the Second World War and concern about the expansion of computer databases, especially those linked to the growing

welfare state, data protection ideas began to be discussed. The first binding legal rules affecting the private sector were enacted in Europe. Early national constitutional decisions and laws concerning data threatened to create trade barriers between countries in the European Union, and Europeans moved to harmonize data protection regimes. Key developments include the Committee of Ministers of the Organization for Economic Cooperation and Development's (OECD) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980, followed by the European Union's Data Protection Directive in 1995. Generally, European data protection laws incorporate the "fair information principles," which require organizations to provide notice and ask for consent before collecting, using, or disclosing personal information, and provide rights of access and correction.

*The Second World War sparked serious policy discussions about data protection.*

Canadian developments paralleled those of Europe, particularly as the EU looked to trading partners that were not EU members to adopt similar rules. In 1983, the *Privacy Act* was enacted, setting out the ground rules for federal governmental institutions relating to the collection, use, disclosure, retention and disposal of personal information and creating the Office of the Privacy Commissioner.[3] Canada signed the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1984. The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) was enacted in 2000 and became fully effective in 2004, setting out ground rules based on fair information principles for private organizations engaged in commercial activities. The Privacy Commissioner was empowered to hear and investigate complaints under *PIPEDA*. Some provinces have similar laws administered by provincial privacy commissioners, including British Columbia, Alberta, and Quebec;[4] in these provinces the federal law is not applied. In 1996, the Canadian Standard Association's Model Code for the Protection of Personal Information (Q830) was recognized by the Standards Council of Canada as a basis for private sector self-regulation. This code was then incorporated into *PIPEDA*.

The data protection rules in Canada and elsewhere were enacted to protect privacy, a familiar term with many meanings. But they are perhaps most remarkable not in building on existing privacy cases and principles, but in the degree to which they departed from them.

Furthermore these legal developments came at a rapid pace, and without an extended period of inter-jurisdictional trial and error. Differences in the substantive rules of different countries give policy-makers in each jurisdiction opportunities to learn from other jurisdictions, ultimately improving the quality of legal rules. This has been one key factor in the development of competition law, for example,[5] and also been helpful in education policy, family law, and so on. Modern governance regimes are complex, and it is difficult to know the best system *a priori*. There has been little time to consider the comparative advantages, disadvantages, costs, and benefits of different types of data protection and privacy regimes.

## A Comparison with the United States: An Alternative Path?

In the 1970s, in the wake of the McCarthy era and Watergate, committees and legislators in the United States (US) began to consider ramifications of the growth of computer databases of personal information, as in Europe. A 1973 privacy committee report by the US set out ideas that later came to be referred to as the fair information principles. The *Privacy Act of 1974*, detailing the privacy rights of citizens and federal employees as against the federal government, was passed. The 1976 Privacy Commission report again cited the fair information principles, and set out its own nuanced proposals, which in many contexts emphasized access (United States 1977). (Both the 1973 and

the 1976 Commissions are credited with playing a leading role in developing the fair information principles in Europe. But the degree to which the 1976 Commission's sectoral rules departed from the aspirational fair informational principles set out in 1973 often seems to be overlooked.) The fair information principles were taken up again much later by the Federal Trade Commission, which formulated its own version in interpreting its statutory mandate to regulate unfair trade practices in addressing issues with electronic commerce (United States 1998; 2000).

In many respects privacy law in the US has evolved differently from data protection elsewhere. The US has not passed comprehensive, general federal data protection legislation, and there is no specialized "data protection" ombudsman. Since the 1976 Commission, no one has articulated a general plan of privacy regulation for the private sector in the US; it is all rather ad hoc.

Privacy law governing the private sector in the US tends to be more bottom-up than top-down. Privacy legislation is passed to deal with particular problems arising in a particular sector or with a particular technology. There is, for example, plenty of statute law (federal or state) concerning children, credit reporting context, banking and finance, medical information, unsolicited commercial email (commonly called "spam"), and fraud. Most states have a data breach notification statute. By comparison, Canada has its own sectoral statutes, federal and provincial, for the public sector, and for health care, unsolicited commercial email, and so on, but it also has general data protection law applicable to the commercial sector. Canada is thus seen as falling somewhere between the EU and the US in the extent to which it prefers an omnibus to a sectoral approach.

Overall, regulation of data in the US tends to be liberal. From the start, the benefits were recognized as well as risks from the free flow of information, as were potential conflicts between privacy and freedom of speech, freedom of information, law enforcement, and concerns about cost to government and private organizations (United States 1977, 21–28). Many commercial transactions are governed by rules under guidelines set by self-regulatory bodies. Some states have passed their own laws governing data, but the effect of these is limited by the flow of data traffic interstate. In terms of liberality, Canada lies somewhere in between Europe and the US. Canadian consumer credit reports, for example, can include much the same information that credit reports in the US do; by comparison, some credit regimes in Europe (and elsewhere) do not allow positive information, or allow information only with consent (Rothemund and Gerhardt 2011).

*Consumer welfare is a useful benchmark of data protection law.*

US privacy law has come under fire for being inadequate compared to that of countries with data protection regimes. But these observers are using data protection law as a benchmark, with any departure from it being sufficient to prove inadequacy, a rather circular bit of reasoning. Suppose one were to choose a more neutral benchmark, such as consumer welfare. Are consumers in the US worse off than consumers elsewhere? No one has produced evidence that they are, and by some measures they are doing very well indeed.[6]

The need to support consumer trust in electronic commerce is often cited as a reason for expanding data protection. But there is no evidence that the growth of electronic commerce is lagging in the US because of a lack of general data protection rules. Early predictions to this effect have proved wrong.[7] Canadians, too, are willing to buy from sites in the US, as reported by emarketer.com on February 23, 2011, in an article titled "US Retailers Help Boost Canadian Ecommerce." Under self-regulation, web sites in the US have followed privacy policies comparable to those in the United Kingdom.[8] In general, when it comes to e-commerce, the US has been ahead, not behind.

No one has ever sat down to articulate exactly what vision drives privacy legislation in the US. It seems that a country with an advanced economy where value is placed on privacy and other human rights can, in fact, do without broad data protection law.

## More Comparisons: How is Data Protection Not Like Other Information Law?

Here we compare data protection to other legal regimes for information. Information is particularly hard to keep within boundaries because anyone can easily make a copy without the awareness of others. Regimes for regulating information include defamation law, patent law, trademark law, trade secret law, and copyright; today one would add data protection to the list. How does data protection compare to these older regimes? For the sake of brevity, we choose just two points of comparison. First, trademark law, perhaps the most straightforward because trademark law is comparatively simple and stable. For good measure, we'll also make some comparisons between copyright and data protection.

First, consider trademark law. Trademark law in some form has been around for centuries.[9] Basic trademark principles were hammered out in the course of resolving many real-world disputes and cases. Many nations passed their first trademark statutes late in the nineteenth century. These were not uniform. Progress towards uniformity was gradual; treaty provisions accommodating the goal of uniformity were mostly a product of the late twentieth century. For example, in the United Kingdom, the first recorded common law trademark case thus far identified dates from 1584 (Stolte 2006, 509); the first recognizably modern statute was passed in 1862 in England and 1857 in France. Proposals to move towards more uniform rules internationally were made as early as 1899 (Beier and Reimer 1955, 1266) but only limited progress towards this goal was made until the 1990s, and many differences between the laws of different nations remain.

As compared to trademark law, the history of data protection is truncated. Within one generation, in a commercial context, the general rule that actors in the private sector are free to learn about each other was reversed. Progress towards uniform rules was sought within only a decade or so of the first national rules. This is important when one considers the scope of the data protection enterprise compared with the scope of the trademark enterprise. Trademark law is a modest business, concerning itself with the names and/or identifying "marks" of products and organizations. Data protection regimes are more ambitious, covering personal information generally, including names, images, and facts or opinions. The rules apply to almost any economic use and user of information, even when no attempt is made, as in Europe, to apply the rules to the public sector as well as the private sector. All in all, the process of developing broad data protection has been not only brief, but more top-down, trying to do much more with less. Law can provide a powerful foundation for social order. But it is not magic. It is certainly possible for legal and regulatory institutions to fail; data protection, by comparison with trademark law, seems almost as if it were designed to do so.

*Copyright also represents an effort to regulate a new technology: the printing press.*

Perhaps this comparison between data protection and trademark law is unfair; trademark law is, after all, rather simpler, more stable, and less controversial than several types of information law (patent law, defamation law). Thus we come to copyright law. Copyright also began with a marked statutory departure from previous legal ideas, (in England, the *Licensing Act of 1662,* followed by the *Statute of Anne* in 1710). Copyright also represents an effort to regulate a new technology: the printing press. And both copyright and data protection potentially cover a large body of information

(though, significantly, copyright law does not cover facts and certainly is not involved in every economic transaction).

Having noted these similarities, however, perhaps the differences between data protection and copyright will appear more striking. For copyright to provide a foundation for content markets, it developed over the course of centuries, not in one generation. Ultimately many ideas in copyright were worked out slowly, case by case. These cases, and developments across many jurisdictions, informed the next generation of statute law, driving the law over time to include consideration of context. The development of the fair dealing defence, first explored in an eighteenth-century English case and codified in the UK in 1911 and in Canada in 1921, is a good example. Little effort was put into harmonizing copyright principles internationally until the twentieth century, and even now it proceeds slowly. Copyright law began top-down, but it could only become workable by a more bottom-up process, and often by making refinements tailored to specific technologies.

*There is a risk a data protection regime will be unworkable from the start due to unrefined rules.*

The question of how and whether legal principles should be designed or redesigned around a specific technology is important with data protection as well. In Canada and elsewhere, part of the reason that data protection rules started with broad, abstract principles is because this degree of abstraction was thought desirable and necessary to make the law technology-neutral. With copyright, we see why this was an attractive idea; technological change can throw the balance struck by a legal regime quite out of line. Mature copyright rules evolved so as to be closely tied to particular technological contexts – even the jukebox. The photocopy machine, the VCR, and then the Internet vastly complicated matters, especially at the enforcement end, necessitating reforms to Canadian copyright statutes in 1997 and again in 2012, some controversial and others less so. Data protection principles under the current dominant model are certainly broad and abstract enough to avoid some of these problems. However, as we discuss further in the section below titled "Constitutional Conflicts: Data Protection as Human Rights", the opposite problem of over-abstraction might turn out to be worse. It is one thing for a legal regime to become hard to enforce as a result of technological change. But with data protection there is a risk that the regime will be too costly or unworkable from the start in many contexts because the rules are not sufficiently refined.

Now, one might argue that data protection law is so important for human rights that it is unreasonable to expect that the process of developing it would look much like the process of developing copyright or trademark law. Lawmakers embarked on the enterprise of data protection to avoid having the new information networks become a free-for-all in which all ordinary expectations and accountability mechanisms for handling personal information were set aside. Both the ambitious scope and the haste of the data protection enterprise are thus understandable.

But the need to make data protection work within a system of human rights means that more, not less, attention to detail is needed, if not at first, then further down the road. If we compare data protection to more traditional human rights, again, the process by which data protection has been developed again looks truncated. The traditional law of privacy, free expression rights, or rights of habeas corpus may appear boiled down, simplified, and highly abstract in the text of a constitution. But the interpretation of key words in the text can be informed by a long history of cases and real-world conflicts, from the Magna Carta forward. The rapid transformation of aspirational principles of privacy into data protection represents an attempt to fabricate new legal principles informed by little more than raw fear of new technology. Given the complexity of the task, this is unlikely to have good results. In Parts II, III, and IV, we examine some of these results.

# II Fair Information Principles Revisited: Conflicting Principles and Goals

Here we consider the application of fair information principles in practice. The history in Part I shows that the process by which general data protection laws were adopted was lacking in characteristics that serve as quality controls. This part assesses the consequences of these lapses. First, we look at current issues with data protection as a part of a constitutional system. Next, we review current issues with data protection as a part of a system for commercial law. Then, we look at data protection as a policy that affects economic growth and competition. In general, we find that data protection rules are overbroad, and likely to present ongoing conflicts with other principles and goals. Furthermore, there is no effective process to mediate these conflicts.

*Data protection rules are overbroad, and likely to present ongoing conflicts with other principles and goals.*

Note that the issues we raise in this Part implicate *general* prophylactic data protection ideas derived from the fair information principles, especially the emphasis on notice and choice in *PIPEDA*. Some other data-protection-related rules are much less general and evolved differently. These more specific rules include anti-fraud regimes, security breach disclosure laws, and anti-spam legislation. Problems of fraud, unsolicited commercial email, and security breaches will be considered in Part III.

## Constitutional Conflicts: Data Protection as Human Rights

The idea that data protection is intended to protect human rights is a familiar one. Since no one is opposed to human rights, the institutional details of this venture are rarely subjected to systemic dissection. The result of this neglect is a conceptual muddle. In the end, data protection is a less effective regime for protecting human rights than one might hope. In some cases, it will squarely conflict with human rights, such as free expression, which is explicitly protected in Section 2(b) of the *Charter*. In May of 2014, a European court recognized a new "right to be forgotten," under which Google must erase links to web pages describing a forced auction of a Spanish lawyer's property to address his debts, as reported by David Stretfield for the *New York Times* on May 13, 2004, in "European Court Lets Users Erase Records on Web". This example of the "right to be forgotten" presents not only a conflict with free expression, but also carelessness about the importance of maintaining the openness of the legal process, as well as the scrutiny of professionals sometimes given responsibility for controlling others' financial affairs.

In Canada, the conflict between privacy and other rights is seen in the case of *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401.* In this case, workers on strike at a casino filmed their picket lines, posting a notice to the effect that images of those crossing the lines might be posted online. Several of those who crossed the line complained that this violated their statutory privacy rights, and an adjudicator agreed. The Supreme Court concluded that Alberta's privacy statute did not strike an acceptable balance between the union's rights of free expression and privacy. The Court called upon legislators to revise the Alberta law.

What does this suggest about the functioning of data protection ideas within a coherent framework of rights? From a classical human rights standpoint the case is worrisome. Human rights ought not to clash with other human rights. The conflict in the Alberta case involved traditional and fairly ordinary political expression, not an obscure or novel practice. A generation ago the idea that this activity ought to be illegal would have been considered quite strange. For this case to arise at all, something has gone awry.

Taking a step back and looking at data protection in wider historical perspective suggests systemic problems likely to lead to more conflicts. In the US, private-sector privacy issues were distinguished from public-sector issues. As a restraint on the public sector alongside other limits on the public sector (including free expression rights), more privacy protection will buttress, not conflict with, free expression rights or any other classic human rights.

But, in Europe, where the fair information principles evolved into data protection, policy-makers have tried to apply data protection rules to the public and private sectors alike. This effort has proved problematic. Literal application of fair information principles to government would bring it to a grinding halt. Many people would be delighted if tax authorities were required to ask their consent before obtaining information about their finances. But this is not going to happen. In Europe, therefore, data protection rules are replete with exemptions to allow government to function as usual. Indeed, some exemptions have grown so that they seem about to swallow the rules. This swallowing process is ongoing. From 2012 to 2013 some EU institutions sought to be entirely exempt from then newly proposed rules, as reported by John Higgins on June 19, 2013, in "One Law Should Cover EU, Governments, and Private Sector," for Euractiv.com, and local governments have also requested exemptions (Council of European Municipalities and Regions, 2012). Ironically, the data protection model thus has come to weigh more heavily on the private sector than on the public sector. A broad framework inspired in part by events such as the misuse of census data by governments during the Second World War is now applied with vigour to photographers, department stores, lawyers, and myriad other private actors. The result is regulatory overkill that will repeatedly conflict with principles of free expression or freedom of association (not to mention long-standing principles of commercial law, discussed in the next section, Data Protection and Commerce: Privacy Policy Problems).

*The Canadian constitutional charter relies on the classical liberal idea that private power and public power are different.*

The question of whether the power exercised by a department store is more or less to be feared than that exercised by the RCMP or Parliament is beyond the scope of this paper. Uneasiness about private power is a familiar idea in Europe, where affairs in many nations were long dominated by landed aristocracy and other privileged groups. But the tremendous importance of social class was not maintained in North America. The Canadian constitutional charter relies on the classical liberal idea that private power and public power are different. It does not violate one's rights of free expression for a newspaper editor to refuse to print an article; it does if the RCMP hauls the author off to jail when it is published. The attempt to simultaneously maintain rights under the *Charter* alongside a European-influenced model of data protection will be problematic.

Some would argue that *PIPEDA* avoids this problem, because it applies only to the commercial sector. Canadians thus avoid having to craft exemptions from *PIPEDA* for government. But the problem of the rules' overbreadth as applied to the private sector remains. Some might assert that people acting in the commercial sphere do not have human rights. The *Charter* does not say this, however. Furthermore it can be difficult to draw bright lines between the commercial sector and any other area

of human endeavor. For example, a firm typically has limited rights to demand a warrant or other legal process to refuse regulators, law enforcement, or national security authorities access to their premises or data the firm has collected. But this will affect the privacy rights of their customers as well.

Lawmakers originally crafted exemptions from *PIPEDA* to forestall some conflicts between privacy and other constitutional principles. But this seems to reduce principles as fundamental as freedom of expression to a mere exception from data protection. The Canadian Supreme Court once stated that:

> Society has come to realize that privacy is at the heart of liberty in a modern state . . . . Grounded in a man's physical and moral autonomy, privacy is essential for the well-being of the individual . . . . The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state. (*R. v. Dyment*, 427)

This statement was made in a case involving the seizure of a blood sample without a warrant by the RCMP; that is, involving the public sector. However, some privacy scholars have taken the statement to apply to data protection of regulation of the private sector, as well; in which case the implication is that data protection ought to take precedence over other human rights (Levin and Nicholson 2005, 378–379; 395). Historically, data protection (compared to the older law of privacy focused on the public sector) is a novelty compared to classic rights such as free expression; and furthermore even traditional rights of privacy are not given priority over other traditional rights – as they do not conflict, there would be no need. One might plausibly argue that privacy has assumed more importance recently, because of technology. But more than technology has changed. The growth of modern administrative states, which routinely manage the day-to-day lives of citizens to a significant degree, has eroded other fundamental rights such as property rights, due process, and freedom of contract. Privacy today has enhanced importance, not because it ought to, but because privacy is being asked to substitute for other rights, now weakened. If one is concerned about human rights, one ought to work towards buttressing rights *other* than privacy.

*Privacy has enhanced importance because it is asked to substitute for other rights.*

As Richard Epstein (2014) puts it, "It is virtually impossible to envision how the state could interfere with, let alone terrorize, religious and political institutions if in all cases it systematically and unflinchingly protected property rights and economic liberties for its citizens . . ." (383).

Informational privacy cannot do the job alone; ultimately, it is not coherent to trust public administrators with broad discretion and powers over our actions, while insisting that we do not trust them with information.

The structural oddity of describing freedom of expression as an exception to privacy law might be of less substantive importance, if the exemptions were broad and well developed. However, the exemptions tend to be narrow and poorly developed. For example, in Canadian law and the law of many European countries, exemptions protect data processing *solely* for journalistic, literary, or artistic purposes. This potentially shrinks the universe of data available for these purposes substantially, because it forecloses cost sharing between data compiled for commercial or other purposes. This is problematic in Europe (Erdos 2012) and is likely to affect Canada as well. A database from which one can generate a list of mailing addresses for people with pets might be used by a pet store, by an animal rescue society, or by a legislator interested in animal cruelty; regulations making it harder to maintain such lists for for-profit purposes will affect nonprofit users as well.

What should policy-makers do to improve this situation? First, refrain from more stringent regulation of the private sector. Second, consider how to liberalize the existing rules and/or, at the very least, strengthen and broaden exemptions. We take up this topic of practicable solutions again in Part IV. In the next section we assess the consistency between data protection principles and other principles of commercial law.

## Data Protection and Commerce: Privacy Policy Problems

This section assesses data protection as applied in the commercial world, with an emphasis on electronic commerce. As the fair information principles were developed into laws, *notice and choice* became a key focus of data protection efforts in Canada and other jurisdictions (Cate 2006). *Notice and choice* typically refers to a consumer's ability to review an organization's privacy policy, and either opt in or opt out.

The idea that policy-makers might improve the lot of consumers by requiring disclosure is familiar one. This intention lies behind food labelling requirements and the package inserts with fine print required in medicines. At a superficial level, a similar notice and choice policy for data seems harmless. One might explain notice and choice as giving one a property right in personal information about oneself, which one then may choose to alienate, or not (Weiland 2006, 3; Purtova 2009). Why not? The answer emerges from the analysis laid out below. Usually, a notice and choice regime for data is neither necessary nor helpful in preventing any specific or concrete harm. And, in the context of data protection discussions, notice and choice is often given an interpretation that makes it more burdensome than appears at first glance.

### 1) The overbreadth problem with notice and choice

In Europe, emphasis on notice and choice is articulated as an attempt to give the consumer control over her information, a level of control necessary to support individual autonomy (Burdon 2011). This rationale has support in Canada (*Alberta Information and Privacy Commissioner v. United Food and Commercial Workers, Local* at paragraphs 13, 19). References to autonomy sound impressive, but are rather vague. What concrete harms are to be prevented? How does a broad notice and choice regime prevent them? What about the effect of reducing available information on others' autonomy? Such questions are generally neither asked nor answered.

If one were starting the search for broad general privacy principles anew, without reference to existing regimes, one might expect good candidate principles (supposing that there are any) to emerge from a review of the areas in which data-related issues (credit reporting, marketing, medicine, wiretapping, the non-profit sector) seem most pressing. But, sought by means of such an overview, the selection of notice and choice as an omnibus principle seems dubious. Indeed, the report of the 1976 Privacy Commission in the US (1977, 18) recommends that the parameters of fair practices vary depending on the context, suggesting that the Commission did not find any omnibus principles compelling. So, for example, a fairly formal legal authorization-and-access regime was proposed for medical privacy (even there, a full informed consent regime was rejected) (314), but the idea of a legally enforceable obligation even to comply with an opt-out request was rejected for ordinary marketing lists (147–151). Elsewhere, such as the processing of credit information (let alone criminal information), the idea of notice and choice was rather obviously not a good fit. When it comes down to details, the case for a broad approach to managing privacy problems, as opposed to a more sector-specific approach, is hard to make convincing. Broad starts to look over-broad.

In drafting Canada's data protection laws, some aspects of this problem were recognized. Canadian lawmakers made *PIPEDA* applicable only in the commercial sector. This reduces the scope of the problem but does not solve it. The literal application of principles of notice and choice would still

often be incompatible with ordinary commercial life. One could not stuff a business card into one's pocket without getting caught up in legalities. Thus an array of exemptions to the rules had to be crafted. Canadian data protection law carefully exempts data intended for personal or household purposes. Credit reporting is permitted as a reasonable purpose. And so on.

*It is acceptable to learn about other people and use that information so long as concrete harm is not done.*

But from the start, the exemptions were too narrow and too few. Important exemptions were left out; for example, under Canadian federal law there is no exemption to allow for the transfer of data without consent when one business is purchased by another (which Bill S-4 would correct). We discuss the problem of exemptions concerning fraud prevention below in Part III. The need for an endless hodgepodge of exemptions is another red flag; the basic idea of a broad notice and choice regime is flawed. What was needed was broad legislative recognition that it is acceptable for people to learn about other people and use that information in the economy, so long as no concrete harm is done.

### 2) The formality of notice and choice will be inconsistent with ordinary expectations

Further support for the thesis that a broad notice and choice regime is a poor fit in many commercial transactions is found in comparing data protection principles with other familiar legal principles, which form the basis of people's expectations in markets.

One central problem in commercial law is the question of consent. Often, implied consent is enough to form a valid contract (as when one orders food in a restaurant). The terms of a contract are ordinarily enforceable even if one party has not actually read them, provided reasonable measures were taken to bring them to his attention and he could have read them (as with parking ticket stubs) (*Thornton v. Shoe Lane Parking Ltd.).* Courts will take into account whether the terms are ordinary ones. Strong advocates for data protection seem inclined to ask for explicit formal mechanisms for consent (such as opt-in) in every transaction involving data (increasingly, almost every transaction). This degree of formality in ordinary transactions will be out of line with ordinary expectations, just as it would be if one were presented with a formal written contract for food service upon sitting down in a restaurant.

This preference for formality would be less problematic if the default rules when such formalities are neglected were not also counter-intuitive. Filling gaps in contract law is an ordinary function of statute law, but statutes do not ordinarily do this by imposing terms that amount to an abrupt departure from usual practice. Data protection turns the presumption in favour of the free flow of information on its head. Before, in general, in both private and business life one was free to learn about other people, and to record and transmit that information, without any explicit notice and consent requirement (with exceptions). More or less the same rules applied in people's personal lives and in their business lives (again with exceptions).

The introduction of significant gaps between the ground rules for ordinary transactions (personal or commercial) and commercial data transactions means that for most economic actors (consumers and entrepreneurs alike) data protection ideas will often be counter-intuitive. One might expect to be handed some papers with fine print about one's personal information when one is being prepped for surgery, and even take the time to read it. Likewise if one is visiting an adult web site. But not when one is buying socks or gourmet popcorn.

Web sites have made steady progress towards compliance with notice and choice rules. In 2001, only about half of Canadian web sites surveyed had a privacy policy; by 2006, almost all had one (Information and Privacy Commissioner 2001; Canadian Internet Policy and Public Interest Clinic 2006a). Consumers are much slower than commercial actors to "comply" with notice and choice formalities; they rarely read privacy policies (Cate 2006; Regan 2001). Given the gulf that has opened between ordinary ground rules and rules for managing data, it is perhaps more appropriate to be merely surprised by the degree of progress rather than disappointed with it.

*Consumers rarely read privacy policies.*

This positive view is unlikely to be appreciated by many strong data protection advocates, many of whom seem to see markets in information as sinister.[10] From their perspective, privacy regulation is not successful unless it actually prevents, on balance, a great deal of information from freely circulating in the market – rather as if we were still living in the 1970s. But a *balanced* notice and choice regime is unlikely to accomplish this, because consumers often freely share information when given a choice.[11]

This is consistent with a sense that imposing a strict regime of notice and choice top-down may be too much, too soon. Bill S-4 thus declined to expand the authority of the Privacy Commissioner to make rules or orders, or impose statutory damages.

Bill S-4 offers new language on "valid consent":

> [T]he consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

A sensible reading of the new language would interpret this as consistent with other commercial cases. Commercial actors are not expected to ensure that individual consumers actually read or understand the fine print, only that consumers of the type they expect would have an opportunity to understand it. But a failure to disclose unusual terms, especially those to which no consumer would be likely to agree, would be recognized as problematic. The intention of the new language was to give more guidance in cases involving vulnerable populations, particularly children (Industry Canada 2014).

*Privacy advocates say privacy policies are either too short to be informative or too long to be readable.*

An alternative approach to this problem would be to devise separate rules for children. As general legislation, a drawback of the new wording is that it might invite an inquiry into the clarity and simplicity of privacy policies generally. Advocates for stronger privacy continue to be concerned that privacy policies are either too short to be informative or too long to be readable (Farmer 2013).[12] Capturing the complexities of business practices changing in the face of innovation and technology both simply and accurately in contractual language is not an easy problem. In a wide array of contexts (real estate transactions, leases of homes and cars, credit applications, intellectual property licensing, and so on) most firms find that they cannot have both. Contract terms tend to be accurate but not simple. Policy-makers should avoid obliging firms to do what has in other contexts proved to be impossible.

The language of S-4 could be improved by specifying that otherwise valid consent should be invalidated only if the understanding of a material term is at issue. As a general rule, consent to usual and customary terms would not be invalidated. But policies drafted in good faith that incorporate no shocking terms (or fail to disclose shocking ones) should be upheld.

The likely outcome of stricter enforcement of notice and choice as envisioned by strong privacy advocates would be that businesses, especially small ones, would find themselves in a legal quagmire, the "successful" resolution of which would make little material difference to consumers.

## Conflict with Major Policy Goals: Competition and Growth

The previous section looked at conflicts between data protection ideals and the ordinary rules for household and commercial transactions from the standpoint of the individual. This section assesses the larger implications of this, examining the conflict between the goals of data protection and the goal of supporting a competitive and growing open economy.

A number of studies draw attention to the potential of data protection to slow economic growth, describing how data protection might affect retail businesses (Turner 2001), advertising, and the economy as a whole. A study by the Conference Board of Canada (Burt, Grant, and Butler 2012) found that the total cost of administering privacy regulations was about $3.8 billion (30), that privacy regulation will reduce cumulative nominal business investment between 2011 and 2030 by $18.8 billion (31), and notes that small and medium businesses are especially likely to bear the brunt of added regulation (36). A study of the effect of data protection in the EU on advertising suggests that the rules make it even more difficult for web sites offering hard-to-monetize general content (such as news) to finance their operations (Goldfarb and Tucker 2011). The study concludes that:

> [A]ds have experienced a reduction in effectiveness of 65% on average in terms of changing stated purchase intent . . . this provides empirical evidence that privacy regulation can reduce the effectiveness of advertising. Furthermore, we show that the loss in effectiveness has been particularly pronounced for websites with more general content that could not be easily linked with a specific product, such as news and Web services sites. (70)

Another study found that data protection in Europe has reduced venture capital investment in European online advertising companies of around $249 million over nine years (Lerner 2012). The costs of data protection include both the costs of the regulation to existing firms and its effect on existing products, but also the harder-to-estimate losses due to the fact that some firms and products will never come into existence under such a regulatory regime.

Also, data protection is likely to impose costs on consumers because it will affect the structure of existing markets. The structure and substance of data protection laws will often disfavour new enterprises and protect established ones, reducing consumer choice (Campbell, Goldfarb, and Tucker 2013; Geradin and Kuschewsky 2013).[13] In 2006 (11, 23, 37, n.53, 38) and again in 2011 (23), the OECD has noted, for example, that data protection rules reduce the flow of information enough that consumers can become "captives" of their own bank.

Strong data protection regulation often will mean less competition and the loss of the benefits of data sharing. These benefits include:

- A wider array of products and services, as providers in niche markets are able to use data to design products and find buyers.
- Lower prices and better product quality, a result of competition enabled and intensified by the use of data.

- The availability of free products and services funded by advertising.
- Avoiding the annoyance of irrelevant sales pitches and ads through the use of targeting.
- Control of fraud and other security risks through data sharing (discussed further in Part III below), and reduction of costs due to effective fraud control.

Data protection is not unambiguously pro-consumer. No adequate regulatory structure or process exists to allow for the correction of this effect. The Office of the Privacy Commissioner will advocate for privacy; lobbyists will advocate for their business or sector. But no one advocates for goods and services that do not yet exist, or for positive externalities of free data flows not yet captured by an existing business model.

*Data protection is not unambiguously pro-consumer. No adequate regulatory structure or process exists to correct this effect.*

Strong privacy advocates argue that growth would be enhanced, not reduced, by more privacy regulation (Weiland 2006, 5), because consumers are wary of venturing online due to privacy concerns. But the evidence that the growth of commerce is slowed or lost because of this effect is weak.

First, these arguments are usually based on consumer opinion polls and surveys, surveys that inquire whether consumers are concerned about their privacy. Public opinion polls are often not a good guide to what makes good policy. Many consumers have a stated preference for buying "made in Canada" or local goods (Business Development Bank of Canada 2013), but this does not mean legislators should adopt policies to squeeze out imports. This aside, one wants to be careful about what surveys and studies one relies on. Privacy studies and surveys tend to employ leading questions, especially "subtle leads," where the context or wording of the questions will tend to affect the answers.[14] The degree of distortion this introduces is substantial; in one study, 21 percent of respondents reported that they "often" or "always" click on privacy policies (Phoenix Strategic Perspective Incorporated 2013, ii); behavioral studies suggest that the real number is likely to be closer to 1 percent (Cate 2006, 361; Regan 2001). The designers of privacy surveys are either unaware of the professional literature describing how to conduct unbiased interviews, or all too aware of it. By contrast, behavioural studies tend to show that consumers have little concern about privacy in the abstract (Joinsen, Reips, Buchanan, and Schofield 2010, 3–4).[15] Observers of comparative growth rates of electronic commerce in Canada and abroad cite as significant the high costs of shipping in Canada (Smyrlis 12 May 2013; Brown 28 June 2012) and other commercial factors.[16] Privacy issues rarely rate a mention. (The possible exception is financial fraud;[17] we discuss the most effective way to address this in Part III ).

Advocates for stronger privacy regulation tend to argue that the gap between what consumers say and what they do is due to market failure in the provision of privacy. This should be viewed with skepticism. This gap has two possible explanations. One is that what consumers say in response to surveys does not reflect their true preferences; the design flaws of a significant percentage of privacy studies make this likely. The second is that their behaviour does not reflect their true preferences. This is much less likely. We noted in Part II, Data Protection and Commerce: Privacy Policy Problems, that there is no reason to expect demand for formal notice and choice on either the business side or the consumer side. One would see demand only to solve particular problems or in special market niches, such as adult web sites. Some argue that a privacy market failure is due to a lack of information, leading consumers to trade short-term gain for long-term harm in the form of less privacy (Acquisti

2002, 17; Rubenstein 2012; 1433–1434). But the Internet certainly leaves consumers free to seek out more information if they want it (Spulber 2009). And consumers are, given the news coverage of identity theft and credit fraud, perhaps far more aware of the harms of loss of privacy than of the benefits of it. All in all, the case of market failure in privacy is very weak.

The data protection regulatory process lacks a system by which conflicts between data protection and fundamental goals such as competition are recognized. The present system of exemptions is likely to prove far too conservative. One candidate is regulatory discretion. We take this up below, in discussing the characteristics of a regulator in Part III. Another candidate is a data protection regime that is generally more liberal than the present regime, which we describe in Parts III and IV.

# III Concrete Problems: Fraud, Security, and Spam

The term *data protection* encompasses not only general rules based on the fair information principles but also rules focused on defined problems like fraud, security breaches, and unsolicited commercial email (which we call "spam," to avoid the awkward "UCE"). One can imagine a world where policy-makers made no attempt to apply the fair information principles to every data transaction. Instead, new rules focused on specific issues like spam or security breaches are adopted only as needed, while the familiar laws against fraud (pre-dating data protection) are updated. Today, many commentators consider laws addressing security breaches and spam (and sometimes fraud) to be forms of "data protection." Below we ask whether treating these special problems as "data protection" issues (to be addressed by vigorous application of broad fair information principles) will strengthen or weaken the effectiveness of policies undertaken in each area. We also examine the operation of these more narrowly focused laws to derive lessons useful in improving general data protection.

## Fraud

Statistics about crimes like identity theft are often cited in support of expanding data protection enforcement. Several forms of financial fraud involve the misappropriation of personal data; these include identity theft, credit card fraud, phishing, and so on, reports Canwest News Service in a November 18, 2008 article for Canada.com titled "Identity Theft Plagues Canadians as Online Shopping Grows." Does it follow, however, that more vigorous enforcement of broad data protection principles would be effective in fighting fraud? Not necessarily.

*The data protection model does not work well in thinking about fraud.*

There is only *some* overlap between the enterprise of data protection and the enterprise of fighting fraud. Encouraging businesses to be careful with information they hold might reduce the amount of information easily available to exploitive bad guys (Smyth and Carleton 2011). In general, though, the data protection model does not work well in thinking about fraud. To oversimplify the enterprise of data protection, one might say it acts as a brake on flows of data in general, as if the use of data were

harmful in itself. But in fighting fraud the harm is financial, and the use of data is either bad (used by the perpetrator) or good (used to prevent or remedy fraud). The perpetrators of fraud are often starting with little information – an email address, a mailing label, or a phone number, information that will be widely available even under a vigorously enforced notice and choice regime. Once one is trying to find the perpetrators of fraud or prevent its occurrence, one will notice that the problem is not too much information, but a lack of it.

In Canada as in Europe, policy-makers try to accommodate the need for "good" data to fight fraud under exemptions that allow data to be used to investigate violations of the law; Canadian rules note that "prevention" is permissible and "investigative bodies" (for example, forensic accountants) may be certified to access data for purposes of fighting fraud. However, the certification process is slow. The extent to which the law allows mass data processing to administer anti-fraud measures by merchants (as opposed to case-by-case investigations by specialized investigators) is unclear.

Looking forward, existing data protection law will often conflict with new methods of fraud control. These new methods involve a wide array of economics actors, from consumers and merchants up to banks and trade associations, public agencies, and Internet service providers. The focus is on prevention, which is far more effective at reducing losses from fraud than post hoc measures (United Kingdom 2010). Some of the most effective methods of fraud prevention involve extensive data sharing in the private sector,[18] everything from deep packet searches to continuous real-time monitoring of transactional data[19] and blacklists.[20] Because the existing exemptions in many data protection regimes are poorly developed, private-sector organizations may hold back from data sharing out of concerns about liability (Eurofinas and ACCIS 2011, 7; 23; 29). The rules may allow data sharing for purposes of fighting fraud but not allow the system to be used for other purposes like marketing – which makes the system prohibitively expensive (Staten and Cate 2003). Some types of data sharing will simply not be permitted.

*Data protection law is not structured to focus on real harm.*

Because fraud control is permitted only as an exception to broad data protection rules, there is a danger that enforcement priorities will be skewed away from taking effective measures to address real harm. Compare a phishing scam that results in the emptying of a number of bank accounts to a popcorn seller's failure to provide formal notice and choice before trading its customer list to a soft drink merchant. Only the phishing scam involves real, concrete harm in the traditional sense cognizable by courts, or that would be likely to cause significant human suffering. Common sense would make the detection and prevention of phishing scams a priority in allocating enforcement resources. But data protection law is not structured to focus attention on real bad guys doing real harm. Fraud ought to be a higher priority for enforcement, especially if one is concerned with supporting trust in electronic commerce.

Laudably, Bill S-4 would clarify that fraud prevention is an acceptable use of data under data protection, and aims to set out rules for the use of data for fraud prevention by any entity, moving away from the model in which fraud is addressed only by certified investigative bodies (7(3)(b)(2)). Justin Ling, writing for the *National Post* on April 13, 2014 in an article titled "New Bill to Crack Down on Illegal Downloads has Privacy Experts Worried", reports that some have criticized proposals to expand exemptions allowing data to be used to enforce compliance with other laws, because of concern about police abuses, or with certain types of agreements (particularly copyright licensing). Policy-makers should address problems with police abuses by improving the accountability and transparency of police institutions; likewise, policy-makers should address copyright problems by reforms to copyright law.

## Security Breach Disclosure Requirements

Above we set out reasons that data protection is likely to be regulatory overkill, and may do more harm than good in the fight against fraud. Security breach disclosure requirements tend to be an exception. Unlike general notice and choice requirements, rules requiring firms to report significant breaches of security are a focused effort to address a concrete problem (Lawford and Lo 2011); the rules operate when a problem has arisen, not in every data transaction. Such requirements would arguably be a reasonable fit in a privacy regime friendly to open markets. There is some evidence that these laws can reduce some types of fraud.[21]

*Security breach disclosure requirements can reduce some types of fraud.*

Bill S-4 would make the reporting of security breaches mandatory at the federal level in Canada (Alberta has such a law already; some other provincial laws apply in the health sector).[22] It also includes criminal penalties intended to address concerns that some businesses deliberately conceal security breaches under certain circumstances. These more stringent penalties can be handed down only by a court following a prosecution by the Auditor-General.

Perhaps the most significant question to ask is how extensive the benefits of the disclosure rules will prove, compared to the costs. A failure to disclose something will not necessarily, after all, be the proximate cause of any significant harm. To put this point another way, breach disclosure rules address the problem of hacking (and related fraud or harassment) indirectly, not directly; this indirect approach can distract policy-makers from the real issue. For example, imagine that a security breach at Firm A results in the disclosure of a list of social insurance numbers. Will this be harmful, or not? There is no reason that it ought to be harmful. A social insurance number functions as a unique name. These unique numeric names help large administrative entities avoid confusing one "Mary Smith" with another "Mary Smith." "Mary Smith's" accounts can be identified reliably, even when her name changes due to marriage or divorce. As names, social insurance numbers ought to be public (an unknown name is of little use) and hard to change (like one's real name). So, why would the breach in question be harmful? Some organizations use social insurance numbers not as names, but also to authenticate a person's identity and confirm that she is entitled to access the account, using it the way a password should be used.[23] A good password needs to be both absolutely confidential and easy to change if it is compromised. Characteristics that make a good name make a bad password. Using a social insurance number as a password is a poor practice (Harley 2009). Whether or not the security breach at Firm A is harmful depends on the security practices of other organizations beyond Firm A's control (include entities in the public sector). One can point a finger at Firm A, but the underlying bad security practice has not really been addressed. These laws therefore raise both fairness and effectiveness concerns, and their costs, benefits, and effects should be carefully watched.

## Anti-Spam Rules

Laws intended to combat unsolicited commercial email, including Canada's Anti-Spam Legislation (CASL), tend to be popular. From a consumer standpoint, spam is a nuisance, and, because much of it does not come from legitimate businesses, a fraud risk. But CASL offers a prime example of a policy venture likely to be less effective than it could be, while at the same time being too strict. The concepts in the law are derived from general data protection principles, rather than being developed bottom-up by considering the nature of the problem.

CASL attempts to reduce spam by imposing a heavily weighted notice and choice regime for the use of email addresses in a commercial context. Since many deceptive emails originate outside Canada, it is not clear how effectively the law can be enforced against the worst offenders. Legitimate businesses already make efforts to avoid annoying their consumers with too much unwanted email; though this might take the form of opt-out rather than opt-in, legitimate firms are not the main source of the problem. Nor are individuals engaging in occasional commercial transactions like garage sales; they are subject to the law nonetheless writes Barry Sookman for the *Financial Post*, in "Delete this Anti-Spam Law," published February 28, 2013.

One significant issue with CASL is it potentially imposes penalties likely to be out of proportion to the harm.[24] Legislators sometimes impose such rules to achieve deterrence in spite of a law being hard to enforce. But empirical research on deterrence shows that effective deterrence primarily depends upon the likelihood of being caught, not the severity of the penalty.[25] Light penalties deter when the probability of being caught is above a certain threshold. If the likelihood of detection falls below a certain threshold, a harsh penalty will not deter. As a general rule, penalties out of proportion to the harm done are neither effective nor fair, and should be avoided.

# IV The Privacy Regulator

Legislators designed The Office of the Privacy Commissioner to function as an ombudsman. As such, it has broad discretion and weak enforcement powers; the office's activity involves advocacy and persuasion, not handing out fines or other judgments enforceable in a court of law. The Privacy Commissioner's 2013 proposal to expand its enforcement powers would have changed this. Bill S-4 would maintain the ombudsman model, though the Commissioner would have an expanded role relating to security breaches. Bill S-4 proposes only modest enhancements to the Commissioner's authority, such as the expansion of the time window for the Commissioner to bring certain problematic cases to court.

In considering whether legislators should expand the powers of the Commissioner, one ought to consider the reasons the ombudsman model was used originally. One was that the privacy law was comparatively young. A second reason was that policy-makers understood that the application of the law would require a lot of flexibility, especially given the pace of technological change in the sectors most likely to be affected (Office of the Privacy Commissioner 2006). Both these conditions still hold.

There are other, rarely articulated reasons to prefer an ombudsman model for the Office of the Privacy Commissioner. The *Privacy Act* gave the Office of the Privacy Commissioner a role in overseeing public sector authorities' data handling practices. In overseeing government agencies, the Office of the Privacy Commissioner is tasked with representing citizens' interest in privacy in ways likely to conflict with other agencies' missions. The Office of the Privacy Commissioner is expected to counter the other agencies' insistence on pursuing methods and goals in conflict with privacy. As a counterweight, the Office of the Privacy Commissioner advocates for privacy, while the other public sector actor can be relied on, in presenting its own case, to advocate for other aspects of the public interest such as competition, law enforcement, or increasing tax revenues. A rough and ready accommodation of these conflicting interests would thus (hopefully) be achieved. Should the Privacy Commissioner be given enforcement powers over other public sector agencies, this balancing process would be upset. Thus the Privacy Commissioner was not, for example, given the power to fine the Finance Minister. Ultimately, disputes with public agencies that cannot be satisfactorily resolved through the Privacy Commissioner's advocacy are referred to the federal courts for resolution, under independent judges – who are not expected to be advocates, but, rather, to be objective.

When legislators expanded the role of the Privacy Commissioner to oversee data practices in the private sector, however, the balance between privacy and conflicting goals such as competition has potential to be upset. We assume that private sector actors in regulatory proceedings represent their own interests, narrowly conceived. Private entities are neither tasked with nor expected to defend broad public interests. They might make public interest arguments – they might even make them very well – but they are not generally considered credible representatives of the public interest. In a conflict between a specialized Privacy Commissioner and a private sector actor, therefore, with the Privacy Commissioner advocating for privacy, other public values are in danger of being given short shrift. This is an important reason to maintain the Commissioner in a primarily persuasive role.

*The Privacy Commissioner should remain in a persuasive role, and not expand enforcement powers.*

In proposing that its enforcement powers be strengthened and expanded, the Office of the Privacy Commissioner describes some of the powers of the Federal Trade Commission (FTC) in the US. However, the FTC is a fundamentally different type of agency. The FTC is responsible not only for fraud enforcement and deceptive trade practices (where the agency is instructed to act in the "public interest"), but also promoting competition. The agency sometimes functions as an advocate in narrow contexts, but for the most part, like a court, it is expected to be objective. Regulatory proceedings initiated by the FTC are unlikely to proceed as if privacy principles ought to take precedence over conflicting principles intended to foster competition, economic growth, freedom of association, effective consumer protection, or free expression. Indeed, this might be one of the reasons that privacy regulation in the US is more liberal than in countries with a specialized privacy regulator.

Proposals to expand the powers of the Office of Privacy Commissioner are in tension with these goals. It would be especially inappropriate for legislators to give an agency tasked with an advocacy mission the additional role of arbiter of conflicts and disputes, which would require objectivity and the full consideration of public goals, principles, and interests that may be in tension with privacy. This is particularly true when it is acting as a regulator of the private sector.

# V Recommendations: Towards a Better Model of Privacy Regulation for Canada

There are good reasons to question the expansion of data protection regulation. The process by which data protection principles were promulgated has been truncated, compared to other legal regimes for the resolution of conflicts over information. When considered as a set of rules to be applied day-to-day, data protection is far from optimal. Its broader principles are often in conflict with other policy goals. There is no structure or process by which the problem of keeping privacy in balance with competing goals and values such as free expression or competition is systematically addressed. Increasing the powers of the regulatory office is likely to do more harm than good. From

the standpoint of fairness and regulatory quality control, it will not do to make an advocacy office an arbiter of disputes, a maker of rules, or a punitive power.

What is to be done? A partial answer is, learn as much as possible from the history of data protection, and move towards the next generation of rules. This section sets out some lessons derived from earlier parts of the paper.

## Step Away from Top-Down, One-Size-Fits-All Rules

Proponents of new rules might argue that they are necessary to promote autonomy, human dignity, or other intangible benefits. Such benefits are important and worth respecting – but they are also highly abstract and elusive concepts. Proponents of new rules should present convincing and specific evidence that the rules they propose would unambiguously provide the benefits they claim. As a general rule, the legal system is too expensive and clumsy an instrument to use to fine-tune the human condition. Law and regulation are better suited to the more straightforward task of resolving concrete disputes, or enabling people to avoid disputes by supplying neutral ground rules.

*Data protection law and policy should be informed and anchored by identifying real problems involving concrete harm.*

Whenever possible, data protection law should be anchored closely to real cases and to real contexts. This does not mean that developments in data protection law should be driven by the news cycle. People selling and buying news stories are apt to dwell on the negative and to feed vague fears. What it means is this: Data protection law and policy should be informed and anchored by identifying real problems involving concrete harm. Rules not needed to address a concrete problem should be avoided, or be maintained as aspirations, voluntary models, or guidelines. In studying real problems, note that some problems are specific only to certain technologies or business models. Attempts to regulate specific technologies are likely to become outdated. But trying to apply broad "technology-neutral" principles in such cases is likely to result in a poor fit between the problem and the solution.

The best approach is a minimal regulatory regime. If only rules necessary to address concrete problems are adopted, the problem of outdated rules or "poor fit" will be minimized.

## Maintain Consistency with Substantive Legal Principles Consistent with Open Markets

Comparing ideas in data protection to other legal regimes will help keep data protection rules in line with ordinary expectations formed in other contexts – whether personal, commercial, or constitutional. And it will keep data protection rules consistent with other rules that serve as ground rules to enable a thriving open market. Other areas of law that ought to be considered include contract law, the common law of privacy, copyright and trademark law, competition law, constitutional law, and ordinary rules for deciding damages and harm.

In contract law, for example, the idea that people might be held to a contract with commercially usual and reasonable terms even though they have not read or entirely understood the fine print is a familiar one. Implied consent is perfectly acceptable in a wide range of contexts. Whatever imperfections might result from this phenomena in the markets for rental cars, software, or electronics, do not

displace our normal observation that markets get better results than regulation. Consumers may not have perfect information, but if they are free to seek it that is usually enough.

Another central problem in legal regimes from corporate law to real property is how to manage situations where the right to control a resource and the right to possess it is divided among one or more people. Legal rules enable such arrangements when necessary to support or enhance markets. In corporate law, the owners of the firm are distinct from managers; the rules enable this arrangement because corporate structures are economically productive. For the most part, however, legal rules try to limit the opportunities given to remote claimants to interfere with those in possession of a resource. Otherwise, the system foments disputes and drains resources, wasting surplus on lawyers that could have gone to doctors or teachers or inventors. With physical property like real estate and chattels, the possessor is partly protected from remote claimants by legal presumptions like those that gave rise to the saying "possession is nine tenths of the law." Other legal rules protect a purchaser for value acting in good faith. This issue also appears with a vengeance in information law (for example trade secret law), as every copy of the information potentially creates a new possessor or controller whose rights need to be managed. Thus far, data protection theories have paid little attention to this problem. Countless persons are likely to possess information relating to the data subject, who retains rights of control for extended periods of time.

*Data protection is likely to be an expensive regime.*

Data protection is likely to be an expensive regime indeed. Those who want to expand it should bear a heavy burden of proof going forward that this game is worth the candle. Policy-makers should consider whether data protection law could be improved, by introducing ideas such as the good faith purchaser for value. Another idea worth considering is inspired by trade secret law; in some circumstances a claimant can lose the right to complain of the loss of confidentiality if he makes information public. (The Canadian Supreme Court, among others, suggests in *Alberta Information and Privacy Commissioner v. United Food and Commercial Workers* that one's conduct in public may still be entitled to privacy protection, a problematic rule that ought to apply only in exceptional circumstances).

Consistency with other law is particularly important when it comes to thinking about harm and damages. Because information law is hard to enforce, it is tempting for policy-makers to try to manufacture compliance by enacting penalties out of proportion to the harm done. Policy-makers hope that imposing severe penalties in token cases will have a deterrent effect. The case of copyright shows that this is not an effective strategy. Data protection law should be informed by this experience. Data protection penalties and enforcement should be proportional to the harm done. The rules for determining damages and harm should be consistent with those in contract law generally. Generally, the law does not impose penalties for symbolic reasons. Nor does it support the recognition of new types of legal "harm" without real, concrete damages as ordinarily understood. Nominal damages are the exception – and they are nominal. Cognizable damages will usually mean financial harm, but not always; it can also mean uses of information that are truly offensive or deeply distressing (following the common law) or, sometimes, within the bounds of free expression, harmful to reputation. Embarrassment[26] alone will not qualify ordinarily. Canadian data protection law allows a court to award damages, including an amount to compensate for any humiliation the complainant has suffered. This provision goes far enough; legislators need not go further in the direction of recognizing symbolic or emotional harms.

Because broad prophylactic data protection rules such as the idea of notice and choice are in tension with the ground rules for other ordinary transactions, policy-makers would do more harm than good to move towards more stringent enforcement. Notice and choice ideas have some value as aspirational principles, creating a model for consumers or businesses looking for more certainty. Where ordinary commercial transactions are concerned, self-regulation and recommended best practices should suffice. The Privacy Commissioner's advocacy role is appropriate. But neither businesses nor consumers will benefit if legislators also are seduced by advocates, and come to share the pessimism about ordinary transactions and technologies that seems to characterize many advocates in thinking about data issues. Whether, ultimately, there ought to be more data flowing through the economy, or less, ought to remain an open question. Different sectors are likely to yield different results at different times.

## Focus Enforcement on Bad Actors

To reduce online fraud, one must focus resources on catching bad actors and stopping *harmful* uses of information. Bill S-4 would take helpful steps towards clarifying the fraud exemption. Enforcement resources should likewise be directed to the fight against fraud. The Privacy Office can continue to be valuable as an advocate alongside other experienced players involved in making policies concerning fraud and security, as these efforts can raise civil liberties concerns.

However, privacy rules for the private sector should not be distorted to solve problems with law enforcement, such as a lack of transparency and accountability for police organizations. These should be managed by reviews to laws governing the public sector. Privacy law should not be used as a substitute for reforms needed elsewhere.

## Maintain the Privacy Commissioner in an Advocacy Role

The Privacy Office should remain in its role as an advocate, both in public sector and private sector cases, and should continue to address controversies case by case, which will help slowly add context and detail to data protection principles. Furthermore, the Office should be required to comply with general rules intended to raise the quality of regulations, such as assessing paperwork burdens or cost-benefit analysis. Guidelines for the conduct of studies and surveys to raise awareness of the problem of "push-poll" questions would be helpful.

In the public sector, it is neither necessary nor desirable to have the Office step out of its advocacy role. This is also true when it comes to the private sector, for different reasons. Data protection law is not sufficiently mature to be enforced as if it were something like trademark law. Furthermore, an office given an advocacy mission will not be likely to decide cases in a way that recognizes and properly resolves the conflicts between privacy and other principles. Regulators, judges, and arbiters ought to be objective and independent; they are not advocates except in the general sense of being expected to serve the interests of the public.

## Revisit Mechanisms for Revision

This analysis frequently notes that exemptions from data protection law, including those to recognize rights of free speech or the need to fight fraud, are not well developed. Parliament receives and reviews regular reports from the Privacy Commissioner, and may act on recommendations to reform the law (to avoid uncertainty or policies driven by the news cycle, it may be unwise to consider changes more often than every three to five years). But it should be noted that the Privacy Commissioner is expected to act as a privacy advocate, a role apt to conflict with the role of developing exemptions to take into account principles of free expression, competition, and so on in writing its own opinions. Also, the

Privacy Commissioner may not have the necessary expertise in competition law, free expression law, fraud enforcement, or contract law generally. We therefore recommend that Parliament continue to invite participation in the reform process by other institutional actors, private interests, and others need to contribute a balanced perspective. By contrast, instructing courts to consider familiar constitutional principles to maintain balance in cases under data protection rules would be useful; judges generally have the background necessary to apply the idea consistently.

# VI Conclusion

Critics of data protection point out the rules have proved costly. But the expansion of most regulation and law or its enforcement is costly. The question is, what is the nature of these costs? One might reasonably ask the public and private sector to spend more to establish compliance with rules that produce proven benefits or prevent concrete harm, and that are necessary, mature, and a good fit with the context in which they are to be applied. But in too many instances, data protection rules fail to meet these criteria. Expanded enforcement of the rules is likely to run ordinary people into trouble for behaving in perfectly ordinary ways. Exemptions intended to recognize that there are benefits as well as costs to sharing information are not well-developed and mature, and tend to be far too conservative in their effect, protecting established information-sharing institutions but hampering new ones. Data protection rules are likely to conflict with other principles and goals, such as healthy and vigorous competition. Finally, the existing data protection regime does not suit the needs of those in the front line of consumer protection facing fraudulent schemes.

Canada should move away from broad and abstract data protection principles towards a new model for privacy. Policy-makers should recognize the following guidelines:

- Recognize that data protection law is not sufficiently mature for conventional enforcement methods, especially given the truncated nature of the process by which it has been developed.
- In trade negotiations, insist that differences between national regimes be tolerated, just as they are tolerated in areas such as judicial process, patent law, and in other areas. Harmonization is a goal for the very long run and has drawbacks as well as benefits.
- Ensure that common-law concepts from contract law and tort law, developed over the course of many generations in real-world conflicts and cases, and familiar in the commercial sector, inform data protection decisions. In contract law, for example, implied consent, not explicit consent, is ordinarily perfectly acceptable. Those acting in good faith ought to be protected from extensive liability. Emotional or symbolic damage are rarely compensable, except under extreme circumstances. Penalties ought to be in proportion to the harm.
- Recognize that the problem of rapid technological change and the complexity of the information landscape are in themselves a compelling argument for minimal data protection regulation. Broad abstract rules are unlikely to provide enough clarity to economic actors, and will result in a regulatory regime that is a poor fit in many contexts. More specific rules are likely to become outdated rather quickly. The best way to avoid this dilemma is to adopt only minimal regulation. The second best way is to adopt responsive rules governing specific sectors (children, health care) after real problems have arisen and have been studied for some time. Common law case-by-case resolution is also likely to result in rules of higher quality.

- Fraud is a real problem for both consumers and merchants. Addressing fear of financial loss, not abstract concerns about privacy, is most likely to support an atmosphere of trust online. Enforcement resources should be narrowly focused on bad actors.
- Amend exemptions to data protection rules to ensure that potentially conflicting values and goals such as free expression, competition, and security are liberally accommodated. These fundamental values ought not to be narrowly confined by poorly articulated, narrow exemptions.
- Maintain the Office of the Privacy Commissioner in its role as an ombudsman. As an advocate for privacy, the office is unsuited to design neutral rules for the private sector or to decide disputes.
- Ensure that quality controls on studies or surveys relating to privacy and funded by the public sector are in place. Require cost-benefit analysis of rules, including anti-spam laws and data breach notification provisions.
- Maintain the distinction in Canadian law between privacy rules for the public sector and rules for the private sector. Be aware that the European model of privacy does not make a clear distinction between these spheres. This may lead that model to include rules for the public sector that are too lenient, and rules for the private sector that are too strict.

Attention to these ideas will move Canada towards a model of privacy regulation for Canada that will support innovation and competition while protecting consumers from fraud and other real hazards.

*Note of Appreciation*

The author thanks Briana Brownell for excellent research support.

# About the Author

Solveig Singleton is a lawyer and the author of many articles on technology law and policy. Ms. Singleton served as a consultant on Microsoft's Technology, Academics, and Policy project between 2008 and 2012. Ms. Singleton is a former adjunct senior fellow with the Progress and Freedom Foundation and director of information studies for the Cato Institute. She has also served as a senior technology analyst for the Competitive Enterprise Institute's Project on Technology and Innovation. Ms. Singleton also served as vice chair of publications for the Telecommunications and Electronic Media Practice Group of the Federalist Society for Law & Public Policy Studies from 1996–1999. Her undergraduate degree is from Reed College, where she majored in philosophy. She then graduated cum laude from Cornell Law School and worked for two years at a boutique telecommunications law firm. She grew up in Nelson, British Columbia, Canada.


Produced in co-operation with Canada's Digital Policy Forum.

CDPF's mission is to enable thoughtful dialogue between industry, government and civil society, and produce policy ideas that advance the digital economy (digitalpolicyforum.ca).

# References


8 Anne, c. 19 (1710) [*Statute of Anne*].

15 U.S.C. § 45(a)(1).

Acquisti, Alessandro. 2002. "Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments." Workshop on Socially informed Design of Privacy enhancing Solutions.

*Alberta Information and Privacy Commissioner v. United Food and Commercial Workers, Local 401*, 2013 SCC 62.

*An Act to amend the Personal Information Protection and Electronic Documents Act*, 41st Parliament, 2nd Session (Bill C-475).

Beier, Friedrich-Karl and Arnold Reimer. 1955. "Preparatory Study for the Establishment of a Uniform International Trademark Definition." *Trademark Reporter* 45: 1266–1308.

Bradford, Mike. 2011. "The Challenges and Opportunities for Sharing Data to Combat Fraud: An Independent Report Covering Europe, the U.S. and Canada." Regulatory Strategies Limited.

Brown, Matthew. June 28, 2012. "Canadian eCommerce and United States eCommerce–A Comparison." Available at http://www.pfsweb.com/blog/canadian-ecommerce-and-united-states-ecommerce-a-comparison.

Burdon, Mark. 2011. "Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws." *Santa Clara Computer and High Tech Law Journal* 27: 63–129.

Burt, Michael, Michael Grant, and Erin Butler. 2012. *Exploring the Iceberg: The Economic Impact of Privacy Policy, Laws and Regulations on Commercial Activity.* Ottawa: Conference Board of Canada.

Business Development Bank of Canada. 2013. "Mapping Your Future Growth: Five Game-Changing Consumer Trends." Business Development Bank of Canada.

Campbell, James, Avi Goldfarb, and Catherine Tucker. 2013. "Privacy Regulation and Market Structure." Social Science Research Network Working Paper.

*Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11.

Canadian Internet Policy and Public Interest Clinic. 2006a. "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?" Canadian Internet Policy and Public Interest Clinic.

———. 2006b. "On the Data Trail: How Detailed Information About You Gets Into the Hands of Organizations with Whom You Have No Relationship." Canadian Internet Policy and Public Interest Clinic.

Cate, Fred H. 2006. "The Failure of Fair Information Practice Principles." In *Consumer Protection in the Age of the Information Economy*, edited by Jane K. Winn, 341–379. Burlington, VT: Ashgate Publishing Company.

Choi, Jay Pil, Chaim Fershtman and Neil Gandal. 2010. "Network Security: Vulnerabilities and Disclosure Policy." *Journal of Industrial Economics* 58: 868–894.

*Convention for the Protection of Human Rights and Fundamental Freedoms.* November 4, 1950. 213 U.N.T.S. 221, Eur. T.S. 5.

Council of European Municipalities and Regions. 2012. "Revise the Existing Directive for the Public Sector." Council of European Municipalities and Regions.

CyberSource. 2012. "2012 Online Fraud Report: Online Payment Fraud Trends, Merchant Practices and Benchmarks." CyberSource.

*Demcak v. Vo*, 2013 BCSC 899.

Descôteaux, David and Berin Szoka. 2013. "Protecting Personal Data: The Economic Impact of Regulating the Internet." Montreal Economic Institute Economic Note.

Epstein, Richard A. 2014. *The Classical Liberal Constitution: The Uncertain Quest for Limited Government.* Cambridge, Massachusetts: Harvard University Press.

Erard, Brian. 1992. "The Influence of Tax Audits on Reporting Behavior." In *Why People Pay Taxes: Tax Compliance and Enforcement*, edited by Joel Slemrod, 95–114. Ann Arbor: University of Michigan Press.

Erdos, David. 2012. "Confused? Analysing the Scope of Freedom of Speech Protection vis-à-vis European Data Protection." Oxford Legal Studies Research Paper No. 48.

Eurofinas and ACCIS (Association of Consumer Credit Information Suppliers). 2011. "Fraud Prevention and Data Protection." Eurofinas and the Association of Consumer Credit Information Suppliers.

European Union. 1995. "Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." *Official Journal L.* 281.

Farmer, Steven P. 2013. "New Watchdog Study Shows that Approximately Half of All Web Privacy Policies are Non-Compliant and Risk Enforcement Action." Pillsbury Winthrop Shaw Pittman LLP. Available at http://www.lexology.com/library/detail.aspx?g=0214d620-8da8-413c-be03-4e17884fd8d5.

*Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996.

Geradin, Damien and Monika Kuschewsky. 2013. "Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue." Social Science Research Network Working Paper. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088.

Gill, Martin, Douglas S. Smith, and Martin Hemming. 2006. "Perceptions on the Impact of Data Protection Legislation on the Successful Private Sector Investigation of Fraud: A Preliminary Study." Fraud Advisory Panel.

Goldfarb, Avi and Catherine E. Tucker. 2011. "Privacy Regulation and Online Advertising." *Management Science* 57(1): 57–71. Available at http://dx.doi.org/10.1287/mnsc.1100.1246.

Harper, Jim and Solveig Singleton. 2001. "With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us." Competitive Enterprise Institute.

Hayes, John. 2002. *Interpersonal Skills at Work 2nd Edition*. New York: Routledge.

Hessing, Dick J., Henk Elffers, Henry S. J. Robben, and Paul Webley. 1992. "Does Deterrence Deter? Measuring the Effect of Deterrence on Tax Compliance in Field Studies and Experimental Studies." In *Why People Pay Taxes: Tax Compliance and Enforcement*, edited by Joel Slemrod, 291–92. Ann Arbor: University of Michigan Press.

Industry Canada. 2004. "Chapter 2: Consumers and Changing Retail Markets." *Consumer Trends.* Canada. Available at http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02096.html.

Industry Canada. April 8, 2014. "Harper Government Introduces New Law to Protect the Personal Information of Canadians Online: Canada's *Digital Privacy Act* Will Protect Consumers and Businesses, Children and Seniors." Canada. Available at http://news.gc.ca/web/article-en.do?nid=836559.

Information and Privacy Commissioner. 2001. "Best Practices for Online Privacy Protection." Information and Privacy Commissioner.

Jamal, Karim, Michael S. Maier, and Shyam Sunder. 2004. "Enforced Standard versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in The U.S. and The U.K." Yale ICF Working Paper No. 04-38.

Joinson, Adam N., Ulf-Dietrich Reips, Tom Buchanan, and Carina B. Paine Schofield. 2010. "Privacy, Trust, and Self-Disclosure Online." *Human-Computer Interaction* 25: 1–24.

*Jones v. Tsige*, 2012 ONCA 32.

Kadish, Sanford H., Stephen J. Schulhofer, Carol S. Seiker, and Rachel Barkow, eds. 1995. *Criminal Law And Its Processes: Cases and Materials,* 6th ed. New York: Little Brown & Co., Law & Business.

Kerber, Wolfgang and Oliver Budzinski. 2004. "Competition of Competition Laws: Mission Impossible." In *Competition Laws in Conflict: Antitrust Laws in the Global Economy,* edited by Richard. A. Epstein and Michael S. Greve, 31–65. Washington D.C.: AEI Press.

Kitten, Tracy. November 25, 2013. "Using Big Data to Prevent Fraud: Why More Institutions Will Turn to Analytics in 2014." *FraudBlogger.* Available at: http://www.bankinfosecurity.com/big-datas-tie-to-fraud-prevention-a-6251/op-1.

Lawford, John and Janet Lo. 2011. "Data Breaches: Worth Noticing?" Public Interest Advocacy Centre.

Lerner, Josh. 2012. *The Impact of Privacy Policy Changes on Venture Capital Investment in Online Advertising Companies*. Analysis Group.

Levin, Avner, and Mary Jo Nicholson. 2005. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground." *University of Ottawa Law & Technology Journal* 2 (2): 357–395.

*Licensing of the Press Act 1662* (14 Car. II c. 33).

McKinsey Global Institute. 2011. "Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity." McKinsey Global Institute.

Narayanan, Meyyappan, Bonwoo Koo, and Brian Paul Cozzarin. 2012. "Fear of Fraud and Internet Purchasing." *Applied Economics Letters* 19: 1615–1619.

Office of the Privacy Commissioner. 2006. *Statutory Review of the Personal Information Protection and Electronic Documents Act: Background Information on the OPC's Consultation.* Ottawa:

Office of the Privacy Commissioner of Canada. Available at: http://www.priv.gc.ca/parl/2006/sub_061127_e.asp.

Office of the Privacy Commissioner of Canada. 2013. *The Case for Reforming the* Personal Information Protection and Electronic Documents Act. Ottawa: Office of the Privacy Commissioner of Canada.

Organisation for Economic Co-operation and Development [OECD]. 1980. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Organisation for Economic Co-operation and Development.

———. 2006. "Competition and Regulation in Retail Banking." Report Prepared for Roundtable on Competition and Regulation in Retail Banking held by the Competition Committee in October .

———. 2011. "Bank Competition and Financial Stability." Organisation for Economic Co-operation and Development.

Paster, Benjamin G. 1969. "Trademarks – Their Early History: Part I." *Trademark Reporter* 59: 551–572

*Personal Information Protection and Electronic Documents Act* (PIPEDA). R.S.C. 2000, c.5.

Phoenix Strategic Perspectives Incorporated. 2013. "Survey of Canadians on Privacy-Related Issues". Ottawa: Office of the Privacy Commissioner of Canada.

*Privacy Act,* R.S.C. 1985, c P-21.

Purtova, Nadezhda. 2009. "Property Right in Personal Data: Learning from the American Discourse". *Computer Law and Security Review* 25: 507–521.

*R. v. Dyment*, [1988] 2 S.C.R. 417.

Regan, Keith. June 15, 2001. "Does Anyone Read Online Privacy Policies?" *E-Commerce Times*. Available at: http://www.ecommercetimes.com/story/11303.html.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2008. "Do Data Breach Disclosure Laws Reduce Identity Theft?" Carnegie Mellon University Working Paper.

Rothemund, Marc and Maria Gerhardt. 2011. "The European Credit Information Landscape". The European Credit Research Institute (ECRI) and the Association of Consumer Credit Information Suppliers (ACCIS).

Rubinstein, Ira. 2012. "Regulating Privacy by Design." *Berkeley Technology Law Journal* 26: 1409–1456.

Smyrlis, Lou. May 12, 2013. "Experts' Commentary on the Hot Issues and Topics of the Canadian Transportation Industry." *CTL Experts' Blog*. Available at: http://blog.ctl.ca/lou/2013/05/transportation-costs-creating.

Smyth, Sara M. and Rebecca Carleton. 2011. "Measuring the Extent of Cyber-Fraud in Canada: A Discussion Paper on Potential Methods and Data Sources." Research and National Coordination Organized Crime Division Law Enforcement and Policing Branch Public Safety Canada. Report No. 020.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. "E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior." EC '01 Proceedings of the 3rd ACM Conference on Electronic Commerce in New York, NY.

Spulber, Daniel F. 2009. "The Map of Commerce: Internet Search, Competition, and the Circular Flow of Information." *Journal of Competition Law & Economics* 5 (4): 633–682.

Staten, Michael E. and Fred H. Cate. 2003. "The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA." *Duke Law Journal* 52: 745–786.

Statistics Canada. nd. "Individual Internet Use and e-Commerce, 2012." *The Daily*. Statistics Canada Catalogue number 11-001-X.

———. 2009. "Internet Shopping in Canada: An Examination of Data, Trends and Patterns." Statistics Canada Catalogue number 88F0006X.

Stephan, Paul B. 2003. "Competitive Competition Law: An Essay Against International Cooperation." University of Virginia Law & Econ Research Paper No. 03-3.

Stolte, Keith M. 2006. "How Early Did Anglo-American Trademark Law Begin? An Answer to Schechter's Conundrum." *Fordham Intellectual Property Media and Entertainment Law Journal* 8: 505–547.

Sweet, David. 2012. "E-Commerce in Canada: Pursuing the Promise." Report of the Standing Committee on Industry, Science and Technology prepared for the 41st Parliament, 1st Session.

*Thornton v. Shoe Lane Parking Ltd.* [1971] 2 W.L.R. 585 (C.A.).

Turner, Michael. 2001. "The Impact of Data Restrictions On Consumer Distance Shopping." Privacy Leadership Initiative. Available at: http://www.privacyalliance.org/resources/turner.pdf.

United Kingdom. 2010. *A Fresh Approach to Combating Fraud in the Public Sector: The Report of the Smarter Government Public Sector Fraud Taskforce*. National Fraud Authority.

United States. 1973. *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computer, and the Rights of Citizens.* U.S. Department of Health, Education and Welfare, Advisory Committee on Automated Personal Data Systems in the Department of Health, Education and Welfare.

———. 1977. *Personal Privacy in an Information Society*. The Privacy Protection Study Commission.

———. 1998. *Privacy Online: A Report to Congress*. Federal Trade Commission.

———. 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress.* Federal Trade Commission.

Weiland, Markus. 2006. "Economics and Privacy: A Survey of Research on 'Economics and Privacy' and 'Incentives and Privacy.'" Dresden University of Technology.

Witte, Ann D. 1983. "Crime Causation: Economic Theories." In *Encyclopedia of Crime and Criminal Justice,* edited by Sanford H. Kadish, 316–322. New York: The Free Press.

Zaller, John and Stanley Feldoman. 1992. "A Simple Theory of the Survey Response: Answering Questions versus Revealing Preferences." *American Journal of Political Science* 36 (3): 579–616.

# Endnotes

1 For instance, *Convention for the Protection of Human Rights and Fundamental Freedoms* (1950), Art. 8 of the European Convention of Human Rights asserts the "right to respect for private and family life."

2 Some Canadian provinces created a tort of invasion of privacy by statute, and a similar right is established by the Civil Law of Quebec. The Ontario Court of Appeals recognized the privacy tort "intrusion upon seclusion" in *Jones v. Tsige,* but the British Columbia Supreme Court declined to recognize this tort in *Demcak v. Vo*.

3 The *Act* directed the Office of the Privacy Commissioner to oversee compliance with the law, and gave the courts a right of review in some cases. Primary responsibility for compliance rests with the Treasury Board.

4 *See, e.g.*, the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996. Other provinces, including Ontario, New Brunswick, and Newfoundland have enacted rules considered substantially similar concerning health information.

5 Wolfgang Kerber and Oliver Budzinski, 2004, "Competition of Competition Laws: Mission Impossible," which describes the spread of antitrust laws between countries, development of antitrust law in Europe, and problems with harmonization; see also Paul B. Stephan, 2003, "Competitive Competition Law: An Essay Against International Cooperation," which describes policy problems resulting from harmonization.

6 McKinsey Global Institute, 2011, "Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity," compares consumer surplus and other benefits from the Internet in Canada, the US, and other countries.

7 In 2000, the Federal Trade Commission cited a study from Jupiter Research suggesting that privacy concerns would cause consumers to withhold $18 billion in spending from e-commerce, and presented graphs projecting rates of growth with and without new privacy legislation. But actual growth rates substantially exceeded the highest estimates (Harper and Singleton, 2001, 10).

8 "[W]e find that the performance of the two regimes, as measured by the number of email messages sent to those who do and do not give consent to receive such messages, is almost identical. With only a few exceptions, most e-commerce sites honor the choice exercised by the registrants. Under both regimes, a few websites flood their registrants with commercial email messages . . . Registrants who indicate their willingness to receive commercial email messages receive a comparable level of message traffic under both regimes. On the notice/awareness dimension . . . the overall performance of the standards and enforcement regime of the UK is about the same as that of the evolutionary regime of the US" ( Jamal, Maier, and Sunder 2004).

9 See Keith M. Stolte, 2006, "How Early Did Anglo-American Trademark Law Begin? An Answer to Schechter's Conundrum," and Benjamin G. Paster, 1969, "Trademarks – Their Early History: Part I," which describes Roman civil actions.

10 One headline calls attention to "leaking" web site data, which suggests a security problem, but the issue was simply the use of information by third-party analytic or advertising firms, and no harm is reported. *See* Christine Dobby, September 25, 2012, "Websites Leaking Users' Personal Information: Privacy Commissioner," *Financial Post*.

11 "[R]egardless of their specific privacy concerns, most participants did not live up to their self-reported privacy preferences. As participants were drawn into the sales dialogue with an anthropomorphic 3-D shopping bot, they answered a majority of questions, even if these were highly personal. Moreover, different privacy statements had no effect on the amount of information disclosed; in fact, the mentioning of EU regulation seemed to cause a feeling of 'false security'" (Spiekermann, Grossklags, and Berendt 2001).

12 Some researchers have suggested that the creation of a regulatory model "standard form" privacy policy would be helpful. This is questionable. Such a form would easily be copied by fly-by-night businesses and phishing sites.

13 Data can also be used in ways that are anti-competitive. However, the main effect of data protection regulation will be to reduce competition, because of the importance of data in the design and offering of new products and by new firms. Anticompetitive uses of data will be more problematic when only a few firms (especially larger, established firms) can access data easily.

14 "Subtle leads are questions that may not be immediately recognised as leading questions. Harris (1973) reports studies which demonstrate that the way a question is worded can influence the response" (Hayes 2002, 116); see also John Zaller and Stanley Feldoman, 1992, "A Simple Theory of the Survey Response: Answering Questions versus Revealing Preferences."

15 "In 2012, 28% of Canadians who used the Internet never erased their browser history. In contrast, 16% of Internet users deleted their browser history after each use and 56% did so occasionally . . . The percentage of Internet users that employed security software on their computer or other devices edged down to 81% in 2012" (Statistics Canada, 3).

16 "The two main reasons identified by Internet users who did not make an online purchase were a preference to shop in person (30%), and having no interest (31%) in shopping online" (Statistics Canada, 1).

17 Several reports agree that some concern about online fraud is a factor. However, many rely on self-reported data and may be unreliable. For instance, Narayanan, Koo, and Cozzarin (2012) found the possibility of online fraud is a major concern of Canadian households considering purchasing goods online; Statistics Canada (2009) found that publicity about data breaches may affect consumers' willingness to buy online; *see also* Phoenix Strategic Perspectives Incorporated, 2013, "Survey of Canadians on Privacy-Related Issues", 12; and David Sweet, 2012, "E-Commerce in Canada: Pursuing the Promise."

18 "It is vital for effective defence against the threat of fraud that businesses can see what has happened elsewhere and recognise the pattern. They can do this only if a firm which has been targeted by fraudsters is willing and able to exchange details with others who might become future victims. Equally, the public sector holds information which could be of vital importance to firms to verify employment records of potential staff members, to check credit claims and to avoid becoming the victims of identity fraud" (Gill, Smith, and Hemming 2006, 4).

19 "Using big data to track such factors as how often a user typically accesses an account from a mobile device or PC, how quickly the user types in a username and password, and the geographic location from which the user most often accesses an account can substantially

improve fraud detection" (Kitten 25 November 2013); CyberSource (2012) describes the potential of merchant analysis of sufficiently large volume of current transactional data to prevent fraud, and the effect of privacy regulation (4).

20 Bradford (2011) describes the potential of data sharing in real time to combat fraud and describes the data protection regime as an obstacle to fraud prevention, including prohibition on blacklists (7, 24).

21 Romanosky, Telang, and Acquisti (2008) find that data breach disclosure laws reduce identity theft by about 6 percent; but Choi, Fershtman, and Gandal (2010) find that data breach disclosure laws may invite further attacks.

22 Provinces with data breach notification requirements for health information include Ontario, Newfoundland, and New Brunswick.

23 *See, e.g.,* CBC News, 14 April 2014, "Stolen Social Insurance Numbers Can Cause Many Problems," CBC News.

24 The maximum administrative monetary penalty for violating CASL is $10,000,000 for organizations, and $1,000,000 for individuals. Whether and when such high penalties are imposed in practice remains to be seen. Conceivably, the temptation could be avoided, as enforcers are asked to consider these factors: The purpose of the penalty; the nature and scope of the violation; whether the person has a history of violations; any financial benefit the person obtained through the violation; the person's ability to pay; and "any other relevant factor." Section 20, CASL. In 2017, a private right of action under CASL will take effect, with a statutory penalty of $200 per occurrence, not to exceed $1,000,000 a day for each day the offence occurred.

25 *See* Kadish and Schulhofer (eds.), 1995, *Criminal Law And Its Processes*; Ann D. Witte, 1983, "Crime Causation: Economic Theories," in *Encyclopedia of Crime and Criminal Justice*; Dick J. Hessing, Henk Elffers, Henry S. J. Robben, and Paul Webley, 1992, "Does Deterrence Deter? Measuring the Effect of Deterrence on Tax Compliance in Field Studies and Experimental Studies," in *Why People Pay Taxes: Tax Compliance and Enforcement*; and Brian Erard, 1992, "The Influence of Tax Audits on Reporting Behavior," in *Why People Pay Taxes: Tax Compliance and Enforcement*.

26 *See An Act to amend the Personal Information Protection and Electronic Documents Act,* 2nd Session, 41st Parliament (Bill C-475), which defines "harm" to include "bodily harm, humiliation, embarrassment, injury to reputation or relationships . . .".

MACDONALD-LAURIER INSTITUTE

*True North in Canadian Public Policy*

## Critically Acclaimed, Award-Winning Institute

**The Macdonald-Laurier Institute fills a gap in Canada's democratic infrastructure by focusing our work on the full range of issues that fall under Ottawa's jurisdiction.**

- The Macdonald-Laurier Institute fills a gap in Canada's democratic infrastructure by focusing our work on the full range of issues that fall under Ottawa's jurisdiction.
- One of the top three new think tanks in the world according to the University of Pennsylvania.
- Cited by five present and former Canadian Prime Ministers, as well as by David Cameron, the British Prime Minister.
- First book, *The Canadian Century: Moving out of America's Shadow*, won the Sir Antony Fisher International Memorial Award in 2011.
- *Hill Times* says Brian Lee Crowley is one of the 100 most influential people in Ottawa.
- The *Wall Street Journal*, the *Economist*, the *Globe and Mail*, the *National Post* and many other leading national and international publications have quoted the Institute's work.

"The study by Brian Lee Crowley and Ken Coates is a 'home run'. The analysis by Douglas Bland will make many uncomfortable but it is a wake up call that must be read."
FORMER CANADIAN PRIME MINISTER PAUL MARTIN ON MLI'S PROJECT ON ABORIGINAL PEOPLE AND THE NATURAL RESOURCE ECONOMY.

## Ideas Change the World

Independent and non-partisan, the Macdonald-Laurier Institute is increasingly recognized as the thought leader on national issues in Canada, prodding governments, opinion leaders and the general public to accept nothing but the very best public policy solutions for the challenges Canada faces.

CTV
SUN NEWS NETWORK
corus ENTERTAINMENT
cpac
tvo
CBC news
WALL STREET JOURNAL
FP Foreign Policy
The Economist
THE HILL TIMES
THE GLOBE AND MAIL
CANADA'S NATIONAL NEWSPAPER • FOUNDED 1844
NATIONAL POST

**For more information visit: www.MacdonaldLaurier.ca**

# About the Macdonald-Laurier Institute

## What Do We Do?

**When you change how people think, you change what they want and how they act.** That is why thought leadership is essential in every field. At MLI, we strip away the complexity that makes policy issues unintelligible and present them in a way that leads to action, to better quality policy decisions, to more effective government, and to a more focused pursuit of the national interest of all Canadians. MLI is the only non-partisan, independent national public policy think tank based in Ottawa that focuses on the full range of issues that fall under the jurisdiction of the federal government.

## What Is in a Name?

**The Macdonald-Laurier Institute exists not merely to burnish the splendid legacy of two towering figures in Canadian history – Sir John A. Macdonald and Sir Wilfrid Laurier – but to renew that legacy.** A Tory and a Grit, an English speaker and a French speaker – these two men represent the very best of Canada's fine political tradition. As prime minister, each championed the values that led to Canada assuming her place as one of the world's leading democracies. We will continue to vigorously uphold these values, the cornerstones of our nation.


SIR JOHN A. MACDONALD


SIR WILFRID LAURIER

## Working for a Better Canada

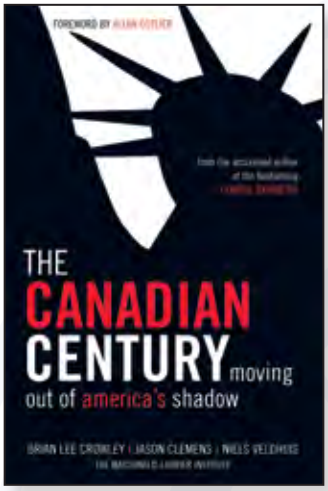
**Good policy doesn't just happen; it requires good ideas, hard work, and being in the right place at the right time.** In other words, it requires MLI. We pride ourselves on independence, and accept no funding from the government for our research. If you value our work and if you believe in the possibility of a better Canada, consider making a tax-deductible donation. The Macdonald-Laurier Institute is a registered charity.

## Our Issues

**The Institute undertakes an impressive programme of thought leadership on public policy. Some of the issues we have tackled recently include:**

- Aboriginal people and the management of our natural resources;
- Getting the most out of our petroleum resources;
- Ensuring students have the skills employers need;
- Controlling government debt at all levels;
- The vulnerability of Canada's critical infrastructure;
- Ottawa's regulation of foreign investment; and
- How to fix Canadian health care.

# Macdonald-Laurier Institute Publications



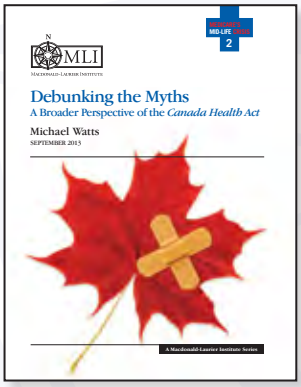

**Winner of the Sir Antony Fisher International Memorial Award BEST THINK TANK BOOK IN 2011, as awarded by the Atlas Economic Research Foundation.**

**The Canadian Century**
By Brian Lee Crowley, Jason Clemens, and Niels Veldhuis

**Do you want to be first to hear about new policy initiatives? Get the inside scoop on upcoming events?**

**Visit our website www.MacdonaldLaurier.ca and sign up for our newsletter.**

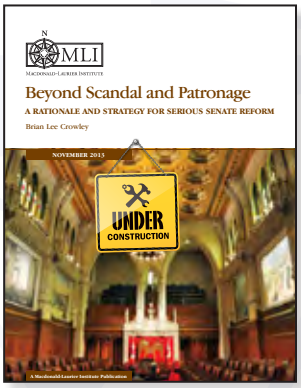
## RESEARCH PAPERS




**Debunking the Myths**
Michael Watts

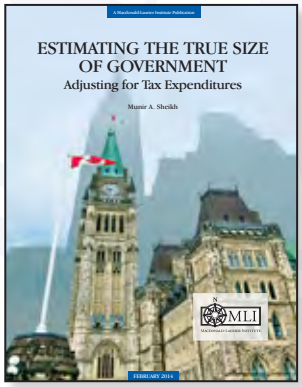

**A European Flavour For Medicare**
Mattias Lundbäck


**How Markets Can Put Patients First**
Audrey Laporte



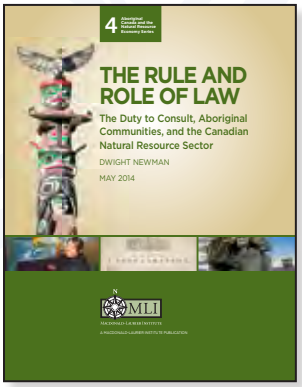

**Beyond Scandal and Patronage**
Brian Lee Crowley


**Oldest Profession or Oldest Opression?**
Benjamin Perrin




**Estimating the True Size of Government**
Munir A. Sheikh


**A Defence of Mandatory Minimum Sentences**
Lincoln Caylor and Gannon G. Beaulne




**The Rule and Role of Law**
Dwight Newman

N

MLI

MACDONALD-LAURIER INSTITUTE

***True North in Canadian Public Policy***


**CONTACT US:** Macdonald-Laurier Institute
8 York Street, Suite 200
Ottawa, Ontario, Canada K1N 5S6

**TELEPHONE:** (613) 482-8327

**WEBSITE:** www.MacdonaldLaurier.ca


**CONNECT WITH US:**

Scan this QR code to get your copy of our iphone app or to visit our mobile website

@MLInstitute

www.facebook.com/MacdonaldLaurierInstitute

www.youtube.com/MLInstitute

## What people are saying about the Macdonald-Laurier Institute

I commend Brian Crowley and the team at MLI for your laudable work as one of the leading policy think tanks in our nation's capital. The Institute has distinguished itself as a thoughtful, empirically-based and non-partisan contributor to our national public discourse.

PRIME MINISTER STEPHEN HARPER

As the author Brian Lee Crowley has set out, there is a strong argument that the 21st Century could well be the Canadian Century.

BRITISH PRIME MINISTER DAVID CAMERON

In the global think tank world, MLI has emerged quite suddenly as the "disruptive" innovator, achieving a well-deserved profile in mere months that most of the established players in the field can only envy. In a medium where timely, relevant, and provocative commentary defines value, MLI has already set the bar for think tanks in Canada.

PETER NICHOLSON, FORMER SENIOR POLICY ADVISOR TO PRIME MINISTER PAUL MARTIN

I saw your paper on Senate reform [Beyond Scandal and Patronage] and liked it very much. It was a remarkable and coherent insight – so lacking in this partisan and anger-driven, data-free, ahistorical debate – and very welcome.

SENATOR HUGH SEGAL, NOVEMBER 25, 2013

Very much enjoyed your presentation this morning. It was first-rate and an excellent way of presenting the options which Canada faces during this period of "choice"... Best regards and keep up the good work.

PRESTON MANNING, PRESIDENT AND CEO, MANNING CENTRE FOR BUILDING DEMOCRACY