A Discussion Paper on

Privacy Externalities, Security Breach Notification and the Role of Independent Oversight

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

Prepared for
The Eighth Workshop on the Economics of Information Security
University College, London, England
June 24, 2009

November 2009

Acknowledgment

Commissioner Cavoukian gratefully acknowledges the work of Fred Carter, Senior Policy & Technology Advisor at the IPC, in the preparation of this paper.

Information and Privacy Commissioner,
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Executive Summary

Building upon theories of data privacy and security externalities, mandatory breach notification and breach notification fatigue, this discussion paper describes the pivotal role of the Office of the Information and Privacy Commissioner (IPC) of Ontario, Canada, *in achieving socially-optimal, positive-sum outcomes for all stakeholders through Privacy by Design*.

Key Messages:

- Applied *Privacy by Design* is the most effective way for organizations to prevent data privacy and security breaches and to minimize the severity of their impact, but sometimes more incentives are needed to enhance breach detection and response capabilities.
- Breach notification laws prescribe new responsibilities and costs for organizations to manage personal information in accountable ways, but can have unintended consequences if breaches are over or underreported as a result.
- Prescribing mandatory breach notification via statute is hard — assessing breach risks and appropriate remedies can be highly contextual and variable activity.
- The IPC is routinely notified of breaches across the public and health-care sectors, allowing us to play an integral role early in the crises. We advocate for the privacy interests of the individual, and encourage proactive cooperation, reporting and harm mitigation from the organizations.
- The IPC is uniquely placed to encourage development and adoption of best practices for breach prevention, detection, and notification. By mitigating risks and harms early, we can achieve socially-optimal, positive-sum outcomes.
- Opportunities abound to apply *Privacy by Design* principles to organizations, networks, and possibly even to entire data governance eco-systems.

Introduction

The purpose of this paper is to revisit my views about (negative) *privacy externalities* that I wrote about back in 2002, in my book *The Privacy Payoff*.[1] The impetus for this was an invitation to present a paper at the Eighth Workshop on the Economics of Information Security in June 2009.

This was an excellent opportunity because much has happened since 2002. The incidence (and costs) of identity theft — a type of negative externality arising from poor information security practices — continue to grow in tandem with the collection, use, disclosure and retention of personal information by organizations, public or private.[2]

In response, mandatory breach notification laws have been enacted by lawmakers in the U.S. and abroad. The underlying premise is straightforward: transparency (about breaches) will help ensure accountability.

As the independent oversight agency for three privacy and access to information laws, the Office of the Information and Privacy Commissioner for Ontario, Canada (IPC) plays a unique and pivotal role, as this paper will set out below. Ontario is the sole jurisdiction in Canada to date to have statutory requirements for the notification of privacy breaches.[3]

Externalities and the Production of Social Goods

First, some theory. An externality is typically defined as "a secondary or unintended consequence." Externalities can be positive or negative.

In economics, an externality (a.k.a. "spillover") of an economic transaction is an impact on a party that is not directly involved in the transaction. In such a case, prices do not reflect the full costs or benefits in production or consumption of a product or service. A positive impact is called an external *benefit*, while a negative impact is called an external *cost*. Producers and consumers in a market may either not bear all of the costs or not reap all of the benefits of the economic activity. For example, manufacturing that causes air pollution imposes costs on the whole society, while fireproofing a home improves the fire safety of neighbours.

In a competitive market, the existence of externalities can cause distortions in the production and consumption of social goods, and in the overall costs and benefits to society (defined as the sum of the economic benefits and costs for all parties involved). To continue with the pollution example, the costs of treating the negative effects of pollution may well exceed the value of the manufacturer's production, resulting in a net cost to society. And, even if effective pollution controls were available that would raise overall benefits to society, the manufacturer may still lack incentives to invest in them — resulting in the under-production of clean air.

1 Ann Cavoukian, Ph.D., *The Privacy Payoff* (McGraw-Hill, 2002) see pp. 99-101
2 For a discussion of the contributory role of organizations to the identity theft problem — and how applied privacy can improve data security, see *Identity Theft Revisited: Security is Not Enough* (Sept 2005)
3 Personal Health Information Protection Act, 2004

Incentives can be realigned, for example, by regulation. Costs can be imposed on organizations for failing to install effective pollution controls. But such incentives can, in themselves, also introduce negative externalities if the costs are excessive or fail to be effective in reducing pollution and its negative impact. This theory can be applied to organizations that handle personal information.

Loss of Privacy as a Negative Externality

Violation of information privacy can be viewed as an external cost, or negative externality, in the same way that environmental pollution is considered an external burden. Data breaches are like pollution: a preventable byproduct of organizational activities that exposes people to harms. The challenge in both cases is to maximize social welfare while minimizing everyone's costs to optimal levels.

As I wrote in my 2002 book *The Privacy Payoff*:

> "[B]usinesses that indiscriminately misuse consumer information often create an external cost in the form of privacy infringement, and that cost is borne by the individual whose private life has been exposed, whose safety is perhaps compromised or whose mortgage or job applications have been unfairly rejected."

To that list of negative privacy externalities I would add "and whose identity is fraudulently stolen and reputation ruined." My 2002 message that "businesses, not consumers, create these "privacy externalities" through loss and misuses of customers' personal information" was the focus of my 2005 paper *Identity Theft Revisited: Security is Not Enough*,[4] which advocated *Privacy by Design* as the most cost-effective organizational approach to enhancing data security.

Nobel laureate Ronald Coase argued that to maximize society's welfare the burden should be placed where the cost is the least. I noted in 2002 that…

> "…placing the onus on companies to remedy or prevent privacy violations would increase their costs and these costs, in turn, would eventually be passed on to customers. In both cases, the externality exists, regardless of who bears the costs…
>
> "The question that then arises is how these costs should be handled. Should they be dealt with in a proactive manner, where privacy practices are built up from, or in a reactive, liability regime that compensates a person or group of people for damages caused by unauthorized or improper use of their personal information? Coase and subsequent researchers have demonstrated that it is socially desirable for an externality to be eliminated when the expense of doing so is less than the damage it causes. That said, what is the least costly way of eliminating the externality? **We believe that the cost of proactively implementing privacy practices designed to prevent the externalities from developing would be far less expensive that the cost of privacy infringement that would result from a liability regime** — litigation, regulatory penalties, loss of consumer confidence and trust, damaged reputation, lost business, loss of market share, and inaccurate, poor-quality information."[5]

4 Ann Cavoukian, Ph.D., *Identity Theft Revisited: Security is Not Enough* (Sept 2005)
5 *The Privacy Payoff*, pp. 99-101 — text emphasis added.

I have always argued that it is in the interests of organizations to build privacy early and thoroughly into their information architecture and operations. Doing so would proactively minimize risks, harms and costs to both the organization and to the individual., realizing powerful competitive advantages through enhanced confidence, trust and repeat business — the "privacy payoff."

Since then, the *Privacy by Design* approach has become more relevant than ever in today's world of ubiquitous availability of personal data, where transparency and accountability for data (mis)use are becoming opaque "in the Cloud", and the negative privacy externalities of misuses of personally-identifiable information are themselves magnified by network effects.

Misaligned Incentives = Poor Data Security, Privacy

Identity fraud and theft are visible evidence of harms arising from breached data security and privacy architectures. A relatively rare phenomenon one or two generation ago, identity theft has reached epidemic proportions, affecting as many as one in five Americans each year according to some estimates, fuelled by the explosive growth of personal data use across all of society.

As Daniel Solove has observed, we are seeing the development of "architectures of vulnerability" in which people are vulnerable to significant harm and are helpless to do anything about it.[6]

The problem of identity theft, Solove contends, arises from architectures of vulnerability in which personal information is not protected with adequate security. The identity thief's ability to so easily access and use our personal data stems from an architecture that does not provide adequate security to our personal information and that does not afford us with a sufficient degree of participation in the collection, dissemination, and use of that information.[7]

There is growing recognition that the single leading source of vulnerability to identity theft arises not from the behaviour of individuals themselves (e.g., not shredding sensitive documents before disposal), but from data-rich organizations. By recent estimates, some 30 per cent of identity theft can be traced back to the large-scale mismanagement or loss of personal data by organizational custodians.[8]

If privacy harms such as identity theft are indeed a consequence, or negative externality, of the mismanagement of personal data by organizations, then what, in turn, is the cause of organization mismanagement?

Cambridge professor Ross Anderson argued, in his seminal 2001 paper[9] that a *misalignment of incentives* was the root cause. That is, organizations had insufficient incentives to invest in strong data security and accountable privacy practices because, in essence, they didn't have to. Consider that lost or "stolen" customer or employee data often does not deprive an organization of its continued availability or use, as would loss or theft of physical property. Further, the (negative) consequences of poor security and misused data fall mainly if not entirely upon individual victims, often at a later

6 Daniel J. Solove, "Identity Theft, Privacy, and the Architecture of Vulnerability", George Washington University Law School, Hastings Law Journal, Vol. 54, p. 1227, 2003
7 *ibid*.
8 Javelin Research, "Identity Fraud Survey Report: 2006," Javelin Strategy & Research, 2006
9 Ross Anderson, "Why Information Security is Hard - An Economic Perspective" (2001)

date. Finally, causal linkages between data mismanagement, privacy and security breaches and their downstream negative impact on individuals, are hard to prove, diminishing accountability.

Absent legal or ethical duties, organizations often have few incentives to report or notify customers of breaches. As Bruce Schneier has noted, it is common courtesy that when you lose something that belongs to someone else, you should tell them.[10] But incentives for firms to do so have been weak. Indeed, from the perspective of many organizations, notifying customers, authorities and the public holds only downside potential.

As a result, the loss and theft of personal data went undetected and unreported for many years, denying individuals the opportunity to take appropriate countermeasures. It would seem that misaligned incentives have resulted in the underproduction of good data security and privacy practices and related "social goods."

In the wake of the first major breaches to be publicly disclosed under California's seminal breach disclosure law, SB1386[11], I strongly advised public and private enterprises to adopt a proactive, positive-sum, *Privacy by Design* approach. Building upon Professor Ross Anderson's insights into why organizations under-invest in good data security and privacy, I affirmed in my 2005 paper *Identity Theft Revisited: Security is Not Enough* that it was the responsibility of all organizations to ensure that individuals do not suffer harm because of inadequate data security and breach notification practices — practices about which individuals have little or no knowledge or say.

My *ID Theft Revisited* paper described how applying information privacy principles in a thoroughgoing manner throughout an organization could improve information security — e.g., by minimizing data collection and use wherever possible, and by vesting data subjects with more participative rights wherever possible as necessary checks in the data management life cycle.

I argued then — as I still argue today — that good privacy is good business. It is in the organization's self-interest to be responsible custodians of personal data, to be proactive and accountable in their data management practices to earn the enduring trust and confidence of customers, employees, business partners, regulators and the public at large.

I wanted then — as I still do now — to achieve a virtuous circle whereby good security and strong privacy reinforce each other (rather than security *vs.* privacy) and, together, generate *positive* externalities in the form of enhanced operational efficiencies, greater customer trust, and enduring competitive advantage. Privacy is foremost a business issue rather than a compliance issue.

Aligning Incentives: Mandating Notification of Breaches

Moral suasion and enlightened self-interest are not, apparently, enough to alter the structure of incentives, and to achieve socially-optimal outcomes. Stronger incentives are needed. Enter law and regulation into the mix.

10 Schneier on Security: "Breach Notification Laws" (January 21, 2009) at: www.schneier.com/blog/archives/2009/01/state_data_brea.html
11 California Civil Code 1798.82

Since the advent of California's SB 1386, more than 40 U.S. states have enacted statutes requiring organizations to notify customers in the event of a privacy or security breach involving personal information.[12]

The laws are based upon a simple idea, namely, that greater transparency will alter the structure of incentives and lead to more accountability, better security and privacy practices, and fewer harms. Well-designed regulation can harness market forces by incenting organizations to improve data security and breach detection practices, thereby generating positive privacy externalities and socially optimal outcomes for everyone concerned.

Noted security expert Bruce Schneier well-summarized the public goods expected from mandatory public disclosure of breaches.[13] They:

1. enable affected individuals to take appropriate countermeasures to protect themselves from harmful consequences;

2. inject market discipline (arising from increased transparency) that encourages better security and privacy practices; and

3. provide valuable information for public research and education purposes.

This approach to requiring openness and transparency about breaches has caught on in many jurisdictions around the world, including in Europe and Canada. Ontario is the only jurisdiction in Canada that has statutory breach notification requirements to individuals, under the *Personal Health Information Protection Act* — which the IPC oversees.

Do Mandatory Notifications Generate Negative Externalities?

But has mandatory breach notification been effective in achieving its objectives of improving organizational data security and accountability practices *and* reducing the incidence and harms of identity fraud? The record to date is mixed.[14] Breach disclosure laws have certainly had some beneficial effects in raising public awareness and improving corporate security practices, but any overall reduction in privacy harms to consumers have not yet been clearly established. One recent study concludes that mandatory breach notification laws have had negligible impact in reducing the incidence or severity of ID theft in the United States since 2004.[15]

Certainly, there is much more detailed information being collected for education and research purposes about publicly reported breaches.[16]

12 For an inventory of state laws, see National Conference of State Legislatures, State Security Breach Notification Page at www.ncsl.org/programs/lis/cip/priv/breach.htm

13 Schneier on Security, supra note 10

14 See, for example, discussion in Schwartz, Paul M. and Janger, Edward J., Notification of Data Security Breaches. Michigan Law Review, Vol. 105, p. 913, 2007; Brooklyn Law School, Legal Studies Paper No. 58. and Canadian Internet Policy and Public Interest Clinic (CIPPIC), "Approaches to Security Breach Notification: A White Paper," (January 9, 2007)

15 See Sasha Romanosky, Rahul Telang and Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?" (September 16, 2008)

16 See http://datalossdb.org/ and www.privacyrights.org/ar/ChronDataBreaches.htm which maintain up-to-date records about data breaches involving personally identifying information.

Thanks to growing awareness of the many costs of dealing with data privacy breaches[17], organizations are beginning to internalize the costs in a more proactive manner, and are investing more in data security, access controls and audit capabilities.[18] Standards and best practices are emerging to help organizations deal with the riskiest areas of information management, such as "leakage" from wireless connections, payment terminals, insecure laptops, portable devices and insider threats. In some instances, separate statutes have been passed to make these practices mandatory, such as truncating payment card information on receipts, effectively supporting breach notification requirements.

From the perspective of individuals, breach notification requirements have given rise to a wide range of new activities and services intended to help them prevent, detect and mitigate some of the harmful effects of a privacy breach, from credit-freeze, credit-monitoring and credit-repair services to insurance and litigation services. Increasingly, in serious breaches, organizations are proactively paying the costs of these services on behalf of affected customers.

Nonetheless, if the jury is still out whether statutory notification requirements have reduced identity theft and other negative privacy externalities in the most cost-effective and socially optimal way, the general consensus seems to be that notification requirements have *generally* been a positive development.

Yet there are mounting arguments that rigid notification requirements may introduce new and distorted incentives, unnecessary costs and other negative externalities.[19]

Artificially high thresholds for organizations to define and report breaches, for example, can result in under-reporting of serious breaches. This is especially the case when legal requirements to assess likelihood of "harm" to customers are interpreted and applied by the very organizations suffering the breach, who may be susceptible to biases. As the Information Policy Institute notes:

> "A firm may not have an incentive to notify consumers of breaches when the cost of the notification exceeds the expected damage to the firm. That is, even if the costs of notifying a customer are smaller than the damage that will be mitigated, a firm has no incentive to bear this cost if the damage it will be spared is less than the costs of telling the consumer. […] Second, a firm may run the risk of damage as a result of notification itself. Reputational damage has been mentioned, but a firm also faces the risk of legal action…"[20]

Similarly, the availability and use of exemptions to notify, as in the case of encrypted or anonymized data, or to delay notifying, as in the case of "safe harbour" provisions, can also result in under-reporting. For example, it must be tempting for some organizations to assert that the lost or stolen data in question remains effectively secured and/or unreadable — and is therefore exempt from any notification requirements at all.

Under-reporting may also arise from incentives to wilfully leave undetected possible breaches which have, in fact, occurred. Why invest in breach detection and reporting mechanisms that create additional costs (from the point of view of the organization)?

17 Reports by the Ponemon Institute are noteworthy. See the "2008 Annual Study: Costs of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions."

18 See, for example, "Security Breach Notification Laws: Views from Chief Security Officers," a study conducted fro the Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law (December 2007)

19 See, for example, discussion in Michael Turner, "Towards a Rational Personal Data Breach Notification Regime," Information Policy Institute (June 2006) and Paul Schwartz and Edward Janger, supra note 13 at page 928

20 Michael Turner, supra note 18 at page 12

To the extent that breach notification requirements introduce incentives for organizations to under-report serious breaches in a timely and effective manner, then the effectiveness of the laws — and perhaps their social utility — may be called into question.

Businesses have argued the opposite, that is, that notification thresholds are too low and should be *raised*. Rigid, mandatory reporting requirements can impose excessive and unnecessary costs to organizations with little or no marginal benefits in terms of actually reducing harms. In support, they point to evidence that suggests the likelihood of breached data being directly used for harmful purposes in many instances to be very low or unlikely.[21] Further, direct causality between breach and the crime is very difficult to establish.[22] The proposition here is that the burdens and costs of notification requirements should be commensurate with their utility for minimizing demonstrable risks to the data subjects.

The case against mandatory breach notification is further supported by arguments that breach notices are rarely read or acted upon by recipients[23] (except in a negative way, e.g., initiating complaints, switching businesses, litigation, etc.[24]). Breach notices are often lengthy and hard to read, with few obvious remedies or actions available for individuals to take in response beyond vigilance and forebearance. As a result, they often get tossed into the garbage. How many times can someone check or freeze their credit rating, for example? In the case of non-financial personal data, such as health information, the appropriate course of action available to individuals maybe even less obvious, further diminishing the value of the notification.

Indeed, there is growing evidence that a new type of negative externality and sub-optimal outcome has emerged from the systemic consequences of mandatory breach notification requirements — notification fatigue. In the beginning, when they were novel, breach notification letters had a significant effect on raising awareness and stimulating corrective behaviour on the part of both organizations and individuals. Over time, however, while the number of notification letters has continued to grow (In 2008 Maryland residents received over 200 such breach notifications![25]), the marginal utility and value of notification letters has levelled off and perhaps diminished as people become inured to receiving them and less concerned.

As the number of notifications continues to increase over time (and the aggregate costs of notification), public reactions and concerns may well plateau and taper off (if they have not already done so). The social and economic benefits of mandatory notification may be subject to the law of diminishing returns. More is not always better.

Can there be too much notification? A tension exists between too little and too much notification, and with it socially optimal levels of security and privacy protections.

21 See, for example, ID Analytics, "ID Analytics' First-Ever National Data Breach Analysis Shows the Rate of Misuse of Breached Identities May be Lower than Anticipated," News Release (December 8, 2005)

22 For a discussion of how harms occur at locations other than the breached entity, see "ID Analytics, National Data breach Analysis 6" (2006) at 14 -18

23 Recent survey findings suggest that consumers do not understand the importance of data breach notifications and, as a result, fail to protect themselves from higher risks of fraud. See: Javelin Strategy & Research, "Data Breach Notifications: Victims Face Four Times Higher Risk of Fraud" (2009)

24 The 2007 Ponemon Institute survey on notification of data breaches revealed 20 per cent of U.S. recipients reported terminating their relationship with a company after being notified of a data breach. Five per cent hired lawyers

25 Lee Gomes, "The Hidden Cost of Privacy," *Forbes Magazine*, June 8, 2009, at: www.forbes.com/forbes/2009/0608/034-privacy-research-hidden-cost-of-privacy.html

Establishing Breach Facts, Risks and Remedies Is Hard

Establishing precisely, in advance, the circumstances, criteria and method of proper notification for all privacy breach scenarios is surprisingly hard –not only because of the secondary consequences of failing to get it right, but because the real world always throws in twists and variations that complicate the calculus of breach detection, management and response.

- For purposes of breach reporting and notification: Some hard questions include:
- What happened? Is it an incident or breach?
- How large is the breach, and has it been contained?
- What are the legal requirements to notify, if any?
- What contextual or environmental factors must be considered?
- Who is at risk, and what are the likely risks of harm?

Other difficult questions that must be addressed when dealing with a real or suspected breach of policies and of personal information might include:

Whom to notify (e.g., senior management, police, other organizations and agents, credit reporting agencies, regulatory agencies, data subjects);

- Timing of notification — when to notify;
- Contents of notice — what to say;
- Form and style of notice — appropriate language;
- Means of notification — how to notify (e.g., e-mail, public notices); and
- Collateral and follow-up customer support.

Not all breach scenarios necessarily or automatically invoke notification. Consider the following scenarios (are they breaches or incidents?):

- Temporarily misplaced physical documents;
- Lost PDA or blackberry device;
- Errant faxes;
- Use of unsecured wi-fi connections;
- Use of free webmail services to send work home and back;
- Misplaced USB keys – contents unknown;
- Unauthorized viewing or copying of screen data; and
- Overheard conversation in an elevator.

Is it necessary to notify everyone, every time, the same way? The precautionary principle suggests that notification should occur wherever there exists *any* risk to the individual, however small, on the basis of the belief that the individual rather than the organization is best-placed to assess what harms are possible and to decide what countermeasures may be necessary to take. But as we have seen above, over-notification fatigue can result, imposing unnecessary costs upon organizations for little or no marginal welfare benefit to consumers.

Is it possible to develop an all-purpose formula to calculate breach notification requirements? Notification would be an expensive and pointless exercise if alternate, more proportional and customized remedies and courses of action were available.

We need to get the balance right, and to achieve socially optimal results. We need to think positive-sum.

Independent Advice and Oversight: the Role of the IPC

As an independent agency of the Ontario legislature, the IPC is mandated to oversee and apply three privacy and access to information laws covering provincial, municipal and health-care sectors. The IPC serves as ombudsman, investigator, mediator, educator, and advocate with some order-making powers.

In 2004, Ontario became the first jurisdiction in Canada with mandatory privacy breach notification requirements to patients under the *Personal Health Information Protection Act* (*PHIPA*), and still remains the only jurisdiction with such a requirement as of 2009. And it is a broad definition:

> *PHIPA* – Section 12(2) "Notice of Loss" reads: "Subject to … exceptions and additional requirements, if any, that are prescribed, a health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost or accessed by unauthorized persons." 2004, C.3, Sched. A, s.12(2)

Although the covered entities must notify data subjects directly, in practice they have been voluntarily reporting breaches to the IPC at the earliest stages. Since 2004, hundreds of data breaches have been reported to the IPC by public hospitals, community health centres, clinics, doctors, and other health-care professionals of all stripes. These self-reported breach statistics are in turn compiled and reported in IPC annual reports.

As we noted in 2008:

> "Custodians have also demonstrated a commitment to privacy in their approach to dealing with privacy breaches. *PHIPA* includes a requirement for health information custodians to notify individuals of privacy breaches related to their personal health information. However, custodians have taken this requirement one step further, by reporting privacy breaches to the IPC and enlisting our assistance in ensuring that such breaches are responded to in an appropriate manner. This openness on the part of custodians has expanded the IPC's role beyond that which was anticipated by the drafters of the legislation. Accordingly, the IPC has had to develop new policies and procedures for handling such self-reported breaches. The IPC welcomes and encourages this openness on the part of custodians, and commends them for being so forthcoming."

This unexpected development has allowed the IPC to play vital roles at the earliest and most critical of breach management stages, acting as advocate for the privacy of the patient's personal health information, gaining insights into the nature of detected breaches, and offering independent advice and expert guidance that is best suited to the needs of everyone involved, given the facts and circumstances of the situation.

Personal health information is highly sensitive in nature, meriting the strongest of protections under the law, but its loss or theft poses different risks and harms to individuals than, for example, financial data. Responding appropriately and effectively to breach notification requirements requires both delicacy and compassion. The IPC, with its consultative, cooperative and pragmatic stance, is well placed to help. As a result, health information custodians across Ontario have come to recognize the value of pre-emptively including the IPC in its crisis management and remediation efforts.

Several hundred health information-related breaches have been voluntarily self-reported to us. The majority (over 90 per cent) are dealt with at the early intake stage, meaning that the custodians are deemed to have responded to the breach in a satisfactory way. A small percentage (5-7 per cent) of self-reported breaches require closer scrutiny. One has resulted in a full investigation, resulting in a public report and Order.

The experience has also transformed the IPC. Back in 2006 we wrote that:

> "[t]he introduction of *PHIPA* has changed the role of the IPC quite dramatically. The IPC no longer restricts its activities to areas which are traditionally associated with an independent tribunal, created primarily to resolve complaints. The IPC now also provides assurances that the information practices of certain prescribed organizations meet acceptable standards and, more frequently, acts as an educator and advisor in a variety of matters relating to *PHIPA*."[26]

IPC involvement has given us ongoing insights into the nature of data breaches occurring across Ontario. For example, the most commonly reported threats to personal health information self-reported by custodians involved the theft of laptop computers or the loss of personal health information when employees have removed records from the workplace.

We have also gained many insights into the range and effectiveness of breach response options — valuable insights that enable us to offer useful guidance, such as our fact sheet, *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector* — that covers a number of specific steps for custodians to take following a privacy breach. The *Guidelines* include steps that can be taken to avoid privacy breaches and how to respond, contain, investigate, remediate, and notify affected parties of a privacy breach.

Even more remarkably, public institutions covered under Ontario's two freedom of information and privacy protection *Acts* (*FIPPA* and *MFIPPA*), which have no breach notification requirements, have also been voluntarily self-reporting data breaches to us, prior to *PHIPA*'s 2004 enactment. In fact it was the public institutions that first started self-reporting long ago. In her *Special Report to the Legislative Assembly on the breach relating to the Province of Ontario Savings Office* in 2000, the Commissioner made the following recommendation:

26 Office of the Information & Privacy Commissioner of Ontario, *2006 Annual Report*, p. 17

> "Upon learning of a possible incidence of non-compliance with the *Freedom of Information and Protection of Privacy Act*, a government organization should notify the Commissioner as quickly as possible."[27]

Since that time the number of public institutions self-reporting has steadily increased. In 2008, for example, the IPC received over 150 such notifications, allowing us to play important new roles in mitigating the costs and harms of breach management across the entire Ontario public sector. These public sector personal information custodians, too, recognize the value of the IPC's cooperative approach and advice.

The IPC has capitalized on the opportunity to provide guidance, not only directly on a case by case basis, but also in the form of best practices such as *What to do if a privacy breach occurs: Guidelines for government organizations*, our publication for the public sector that provides guidance on how to identify and contain a privacy breach, who to notify, and what proactive steps to take to avoid one. At the same time, we jointly issued a *Breach Notification Assessment Tool* with the Office of the Information and Privacy Commissioner of British Columbia to assist organizations in making key decisions about notification after a privacy breach has occurred. The *Breach Notification Assessment Tool* provides checklists of factors that should be taken into consideration when deciding whether to notify, when and how to notify, what to include in a notification and what other organizations should be contacted.

Finally, our unique vantage point and role has enabled us to seize the opportunity to promote effective *Privacy by Design* practices at the most 'teachable' of moments, going far beyond minimal legal requirements, in the case of security, to ensure "adequate physical, administrative, and technical measures" to safeguard personal data under custody or control against theft, loss, and unauthorized use or disclosure" as well as "to ensure that the records containing the information are protected against unauthorized copying, modification or disposal."

Summary

Violations of information privacy can be viewed as an external cost, or negative externality, in the same way that environmental pollution is considered an external burden. Nobel laureate Ronald Coase argued that to maximize society's welfare the burden should be placed where the cost is the least. In the case of privacy breaches, that would require organizations to remedy the externality of identity theft, for example, by adopting effective measures to prevent, detect and notify customers of data breaches and any related risks.

However, placing the onus on organizations to prevent and remedy privacy violations would increase their costs and these costs, in turn, would eventually be passed on to customers, e.g., the costs of added security measures, and of notification and credit report monitoring for breach victims.

To maximize society's welfare, there would have to be a few additional constraints. Not only should costs be placed with businesses, but these costs should be minimized. This is why I advocate *Privacy by Design* as the most cost-effective approach in the long run; an ounce of prevention is worth a

27 *A Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information by the Province of Ontario Savings Office*, (2000) page 29

pound of cure, especially when the "cure" — breach notification and remediation efforts — has become more mandatory and expensive than ever.

Since the mid-1990s, when I first became Privacy Commissioner, I have consistently argued that good privacy practices are good for business, and that adopting a *Privacy by Design* approach ensures effective privacy — maximizing the welfare of customers — with minimal costs. During this time, incentives to build in privacy early and systematically have grown with the advent of data breach disclosure and other accountability requirements. We are approaching a phase whereby all organizations, regardless of statutory requirements, are widely expected to have credible security and privacy practices in place by default, including robust mechanisms to prevent, detect and report breaches.

However, mechanisms that are put in place to prevent privacy violations should be structured so as to minimize any negative unintended consequences in other areas, e.g., reduced business functionality, excessive notification costs, and notification fatigue of recipients. A flexible approach is needed: any solution should evolve as conditions change since in today's world protection of privacy is akin to hitting a moving target (e.g., the security and identifiability of data).

These constraints placed on organizations impose enormous difficulties in finding optimum solutions. Organizations interact with clients within the larger context of a dynamic society. In essence we are dealing with a complex system: a system in which large networks of freely-acting individuals with no overriding central control and relatively simple rules of interaction give rise to complex collective behaviour, sophisticated information processing, and adaption via learning or evolution. "Complex systems often exhibit nontrivial emergent and self-organizing behaviour which cannot be predicted" In fact in many cases, it is theoretically impossible to predict future outcomes based on current inputs.

Traditional solutions to negative externalities involve imposing regulations on businesses which require that they modify their behaviors in certain ways to achieve elimination or minimization of the negative externality. But experience has demonstrated that such regulations are problematic.[28] They require additional costs for a bureaucracy to oversee compliance both in the government and in companies; they rarely are the optimum solution primarily because one is attempting to regulate a complex system; they are static solutions in that they become outdated when conditions change; and they often have negative unintended consequences, at times, which cancel out the intended benefit of the regulation.

Automatic breach disclosure requirements, when set at thresholds either too low or too high, can also impose net costs on society, causing no end of debate about how best to codify such requirements in law or regulation. A flexible approach seems advisable, given the wide range of circumstances and harm factors involved from one breach to the next.

We believe that the IPC plays a unique and pivotal role in helping organizations respond to data breaches in a responsible, pragmatic and effective manner. Legislation alone cannot accomplish this. Nor would purely voluntary measures.

28 See, *inter alia*, discussions in: Paul Schwartz and Edward Janger, "Notification of Data Security Breaches." Canadian Internet Policy and Public Interest Clinic (CIPPIC), "Approaches to Security Breach Notification: A White Paper," and Romanosky *et alia*, "Do Data Breach Disclosure Laws Reduce Identity Theft?"

By allowing flexibility according to contextual factors, applying my office's evolving expertise at the early stage of breach crisis management can help organizations avoid excessively burdensome, irrelevant or costly requirements AND ensure that the legitimate rights and needs of data subjects to be informed are met, and that the risks of harm are mitigated to the fullest extent possible.

We believe that we are helping to achieve socially optimal results in a way that legislation alone, with its one-size-fits-all approach, cannot.

This is evidenced by the spontaneous and broad based emergence of self-reported breaches in areas where no prior legal requirement to do so exists, as well as the emergence of new collaborative roles for my office that were unanticipated by the drafters of Ontario privacy legislation.

Conclusion

Since the mid-1990s, when I was appointed Privacy Commissioner, I have consistently argued that good privacy practices are good for business, and that adopting a *Privacy by Design* approach to operations ensures effective privacy — maximizing the welfare of customers — with minimal costs.

Since then, incentives for organizations to build in privacy early and systematically have grown with the advent of data breach disclosure requirements. In Ontario, these disclosure requirements have, in practice, afforded my office unparalleled opportunities to work together with affected organizations to devise the appropriate harm-mitigation response at the earliest stages of the crisis. And, thanks to the flexibility afforded by privacy regulation in Ontario, we can also help them build good privacy and security early and directly into their information systems, processes and architectures so that such breaches do not recur in the future.

Perhaps the time has now come to apply the *Privacy by Design* approach not only to the information technologies and to the practices of organizations, but to entire systems of data governance and privacy oversight!

Appendix

Select Resources

Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada:

- **What to Do if a Privacy Breach Occurs: Guidelines for Government Organizations** (December 2006) at: www.ipc.on.ca/images/Resources/priv-breach-e.pdf
- **Breach Notification Assessment Tool**
  Jointly with the Office of the Information & Privacy Commissioner for British Columbia (December 2006) at: www.ipc.on.ca/images/Resources/ipc-bc-breach-e.pdf
- **What to Do When Faced With a Privacy Breach: Guidelines for the Health Sector** (June 2006) at: www.ipc.on.ca/images/Resources/hprivbreach-e.pdf
- **Privacy and Boards of Directors: What You Don't Know *Can* Hurt You**
  Privacy is a business issue, not just a compliance issue (July 2007) at: www.ipc.on.ca/images/Resources/director_2.pdf
- **Identity Theft Revisited: Security is Not Enough**
  The paper looks at the growing problem of ID Theft, and asks how organizations, as custodians of this data, can help mitigate the risks to individuals and to themselves (September 2005) at: www.ipc.on.ca/images/Resources/idtheft-revisit.pdf
- **A Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information by the Province of Ontario Savings Office, Ministry of Finance** (April 2000) at: www.ipc.on.ca/images/Resources/up-poso_e.pdf

Ross Anderson, **Why Information Security is Hard - An Economic Perspective** (2001) at: www.cl.cam.ac.uk/~rja14/Papers/econ.pdf

Canadian Internet Policy and Public Interest Clinic (CIPPIC), **Approaches to Security Breach Notification: A White Paper** (January 9, 2007) at: www.cippic.ca/documents/bulletins/BreachNotification_9jan07-print.pdf

Chris Hoofnagle, **Measuring Identity Theft at Top Banks**, 2008 (University of California, Berkeley) at: http://repositories.cdlib.org/bclt/lts/44

ID Analytics

- **ID Analytics' First-Ever National Data Breach Analysis Shows the Rate of Misuse of Breached Identities May be Lower than Anticipated**, News Release (December 8, 2005) at: www.idanalytics.com/news_and_events/20051208.html
- **National Data Breach Analysis**, Report (January 2006) at: www.idanalytics.com/assets/whitepaper/BreachWhitePaperFinal.pdf

Javelin Strategy & Research, **Identity Fraud Survey Report: 2006. Data Breach Notifications: Victims Face Four Times Higher Risk of Fraud** (2009) at:
www.javelinstrategy.com/lp/Data-Breaches-LP.html

Thomas M. Lenard and Paul H. Rubin, **Much Ado about Notification**. Regulation, Vol. 29, No. 1, pp. 44-50, Spring 2006; Emory Law and Economics Research Paper No. 06-08. Available at SSRN: http://ssrn.com/abstract=898208

National Conference of State Legislatures (NCSL), **State Security Breach Notification Page,** at:
www.ncsl.org/programs/lis/cip/priv/breach.htm

Ponemon Institute, **2008 Annual Study: Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions** (2008) at: www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf

Sasha Romanosky, Rahul Telang and Alessandro Acquisti, **Do Data Breach Disclosure Laws Reduce Identity Theft?** (September 16, 2008) Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268926

Samuelson Law, Technology & Public Policy Clinic, University of California – Berkeley School of Law, **Security Breach Notification Laws: Views from Chief Security Officers**, (December 2007) at:
http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf

Bruce Schneier, **Breach Notification Laws,** Schneier on Security (January 21, 2009) at:
www.schneier.com/blog/archives/2009/01/state_data_brea.html

Bruce Schneier and Marcus Ranum, **Face-Off: State Data Breach Notification Laws-Have they Helped?** (Jan 20, 2009) at: www.searchsecurityasia.com/content/face-state-data-breach-notification-laws-have-they-helped

Paul M. Schwartz and Edward J. Janger, **Notification of Data Security Breaches**. Michigan Law Review, Vol. 105, p. 913, 2007; Brooklyn Law School, Legal Studies Paper No. 58. Available at SSRN: http://ssrn.com/abstract=908709

Daniel J. Solove, **Identity Theft, Privacy, and the Architecture of Vulnerability** George Washington University Law School, Hastings Law Journal, Vol. 54, p. 1227, 2003. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416740

Information and Privacy Commissioner,
Ontario, Canada
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
CANADA

Telephone: (416) 326-3333
Toll-free: 1-800-387-0073
Fax: (416) 325-9195
TTY (Teletypewriter): 416-7539
E-mail: info@ipc.on.ca
Web Site: www.ipc.on.ca