

FALL/WINTER 2010

management ethics

IN THIS ISSUE

Editorial

Why Privacy Matters

Privacy by Design: Achieving
Consumer Trust and Freedom
in the Information Age

Hiring in a
Social Media Age

Privacy Law:
Questions and Answers

Business Ethics Scholarship

Ethics and Privacy in Information Systems

BY SHEERIN KALIA

Personal information is highly accessible online and through information systems in organizations. Some businesses take advantage of that accessibility by using such information to data-mine, recruit and select employees, inform product development choices, and determine marketing strategies, among other things. Anyone whose personal information is viewed, stored, used or disclosed would likely be concerned about the implications of that accessibility and unfettered use.

To some extent, legal requirements discipline the collection and use of personal information but not to the degree that some might believe and not in a consistent manner across jurisdictions. It is for this reason that we decided to explore how ethics can fill the gap between what the law requires and what is good corporate behaviour, or at least provide a different perspective to inform sound business practices. We were fortunate enough to have Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, Dr. Avner Levin of Ryerson University, Dr. Chris MacDonald, a Visiting Scholar at the University of Toronto, and Christine Lonsdale, a Partner at McCarthy Tétrault LLP agree to provide us with their thoughts on different aspects of the topic.

My personal thoughts on the issue are admittedly simplistic. I want people to trust me so I try not to repeat any information given to me that does not seem directly related to a person's business activities and professional pursuits. That means I try not to repeat personal information such as family status, religious beliefs, political views, personal relationships, health concerns, etc., unless someone specifically tells me to repeat what they have said. When I think of the collection and use of personal information by businesses, I believe that the approach should be the same. Yet, it is not. The reality is that businesses use personal information in ways that may not be disclosed to or understood by the originators of the information. Some of the arguments made to support such use include: 1) those who make personal information available on the internet or to businesses should have a lowered expectation of privacy for any

purpose, 2) personal information used for product development ultimately benefits the individuals whose information is used, by way of improved product choices (i.e. benefits outweigh costs), and 3) it is not wrong if it is not against the law.

Numbers one and two are interesting arguments and do call my simplistic approach into question, particularly where no one objects and where discernible benefits are felt after such use. But, there is no guarantee that a business will know of all objections to its business strategy right away. And, objections voiced later will most likely be accompanied by higher costs associated with damage control. Number three, on the other hand, brings to the fore the age old debate of what is and what ought to be (i.e. positive versus normative ethics) and uses the law as a guide. That is somewhat perplexing. As a lawyer and educator, I have always been careful to point out to clients and students that the law tells us what we must do and nothing more. Whether the law and ethics intersect, or one concept subsumes the other, or one provides a lower or higher standard than the other is not very instructive. The bottom line is that to avoid reputational risk, loss of customers, and loss of investors due to poor ethical decision-making, good decision-makers must ask: After complying with the law, what else should we do, if anything? It is our hope that the articles in this issue, which contain thoughtful analysis and practical strategies, will assist our readership in answering that question. 🍁

Why Privacy Matters

BY CHRIS MACDONALD, Ph.D.

VISITING SCHOLAR, CLARKSON CENTRE FOR BUSINESS ETHICS AND
BOARD EFFECTIVENESS AND AUTHOR OF BUSINESSETHICSBLOG.COM

There's a lot to know about privacy – how to protect it, when to give it up, what its ethical limits are. But perhaps the greatest challenge facing businesses with regard to privacy is to understand what privacy really is, and why it matters. That may sound obvious, but it's not. Some of the biggest companies on the planet have stumbled over a fundamental inability to understand those two key issues.



WHAT IS PRIVACY?

Privacy, at its most basic, is about having a sphere of personal control from which others can be excluded at will. It refers not just to information, though that is certainly a key component of privacy. Privacy is also about freedom of action, action that is not hindered by the prying eyes of neighbours, governments, or corporations. The more such freedom we have, the more privacy we have. Another way of stating it: according to legal scholar Lawrence Lessig,¹ privacy is best understood as an ideal that stands in contrast to the ideas of monitoring and searching. Roughly speaking, the less one's life is monitored, and the less one is subject to being searched, the more privacy one has.

“REVEALING MORE OR DIFFERENT INFORMATION TO SOME PEOPLE THAN YOU DO TO OTHERS IS A FUNDAMENTAL PART OF HOW WE DEFINE, DEVELOP AND MAINTAIN OUR MOST IMPORTANT RELATIONSHIPS.”

WHY DOES IT MATTER?

Privacy matters to us for three main reasons. One reason is that knowledge is power. If people have just the right knowledge about us, they can use it to harm us or to manipulate us or sometimes just to embarrass us. That is, one reason privacy matters to us is that control of information has consequences that matter to us. A second reason isn't about consequences, but rather about human dignity. Respect for human dignity means allowing persons a realm of private thought and action that is not subject to control or scrutiny by others. And a third and easily-overlooked reason we value privacy has to do with relationships. Philosopher James Rachels put forward the influential view that privacy is crucial to the way we define our relationships with other individuals and institutions.² To be intimate with someone – whether we're talking about romantic intimacy or the intimacy of friendship or the intimate trust between patient and physician – is to entrust them with information not shared with the world at large. Privacy is the means by which we signal the significance of our personal and professional relationships.

MISUNDERSTANDING PRIVACY

It is crucial for businesses to understand the significance of privacy – not just its legal significance, but the moral significance that underpins legislated protections for privacy and the values that might prove instructive

where legislation is silent. A failure to truly understand privacy can easily corrode trust. For example, Facebook CEO, Mark Zuckerberg, argues for universal openness. He claimed, and I believe wrongly, that trying to keep certain information private constitutes a moral failing. “Having two identities for yourself,” he said in an interview, “is an example of a lack of integrity.”³ In my view, this statement reflects a fundamental misunderstanding of one of the three crucial reasons why privacy matters, namely that revealing more or different information to some people than you do to others is a fundamental part of how we define, develop and maintain our most important relationships. The result of this view has been additional media scrutiny, along with calls from some privacy experts for consumers to avoid Facebook altogether.

A FINAL THOUGHT

When companies are considering their commitment to proactively safeguarding the privacy of their customers and clients, it may be instructive for them to consider the role that the privacy of corporate information plays in their own daily operations. For example, a case currently before the U.S. Supreme Court (*Federal Communications Commission v. AT&T Inc.*, No. 09-1279) will consider, at a very fundamental level, whether corporations are the kinds of entities that can have a right to personal privacy of the type that is commonly attributed to individuals. The Court will have to consider just how much weight to attribute to such privacy, and how much protection it should be afforded. Of course, when a company asserts its own privacy rights, it is in at least some cases thereby protecting the privacy of its clients, along with the rights of its shareholders. But the key point here is that when companies think about the value of privacy, they would do well to consider how much privacy also matters to *them*. 🍁



CHRIS MACDONALD, Ph.D.
VISITING SCHOLAR, CLARKSON
CENTRE FOR BUSINESS ETHICS
AND BOARD EFFECTIVENESS
AND AUTHOR OF
BUSINESSETHICS.BLOG.COM

REFERENCES

- 1 Lawrence Lessig, “The Architecture of Privacy” (Paper presented at Taiwan Net Conference, Taipei, March, 1998), online: http://www.lessig.org/content/articles/works/architecture_priv.pdf
- 2 James Rachels, “Why Privacy is Important” *Philosophy and Public Affairs*, 4:4 (1975) 323-333.
- 3 Kim-Mai Cutler, “Why Mark Zuckerberg needs to come clean about his views on privacy” <http://venturebeat.com/2010/05/13/zuckerberg-privacy/> (citing David Kirkpatrick's 2010 book, *The Facebook Effect*)

Privacy by Design: Achieving Consumer Trust and Freedom in the Information Age

BY ANN CAVOUKIAN, Ph.D

Information and Privacy Commissioner of Ontario



Today, all organizations face complex, growing information management challenges in an era of unlimited data creation, use, storage, and disclosure. Not only has personally identifiable information become more voluminous, granular and ubiquitous, it is also accessible by more and more entities, for more and more purposes, across ever-expanding (and increasingly complex) networks. As soon as data is linked to an individual, thereby identifying him or her, many ethical, legal and economic privacy considerations arise. Privacy is essential for a free and democratic society and, it is also good for business. Respecting privacy brings discipline and accountability to an organization's information management practices, and promotes enduring customer confidence and trust.

The Information and Privacy Commissioner of Ontario (IPC) has written extensively about the privacy challenges emerging from the many effects of information and communication technologies (ICTs) that are transforming modern organizations.¹ In today's hyper-connected world, the typical enterprise operation has become considerably more data-intensive, and transformed into a knowledge-based service provider.

In our 2006 paper, *Privacy and the Open Networked Enterprise*, we examined the impacts of ICTs on enterprises and espe-

cially upon their management of personal information, and predicted five major informational privacy challenges for the next generation:

1. outsourcing of data to other organizations
2. internal threats to data holdings
3. individual participation in managing one's own personal data
4. indiscriminate collection from external sources, lacking in accountability
5. deploying new technologies without building in privacy

An additional challenge is the need for organizations to comply with a patchwork of legal, regulatory and contractual privacy requirements across multiple jurisdictions. These requirements are also subject to change. There is growing pressure around the world to pass new statutes and regulations to hold firms more accountable for their (personal) information management practices, and for any negative effects they may have on individuals. Current data security and marketing practices are under scrutiny in numerous jurisdictions.

These are indeed big challenges, which will require holistic, comprehensive, integrative solutions.

CHALLENGING PRIVACY SOLUTIONS

The solutions required will be equally challenging because they will be highly complex and interdisciplinary in nature. They may also vary from one jurisdiction to another, and from one context to another.

Legislation and regulatory oversight should certainly form part of the solution but is not a panacea. Statutes establish general frameworks and priorities but are typically reactive in nature, rarely offering specific or detailed guidance, with oversight agencies mandated to interpret them, ill-equipped to provide early guidance or approval of new information technologies, systems or projects. The result is usually after-the-fact oversight, where harms must first occur, be detected, and then reported before the requirements of law are invoked, and corrective measures applied.

We want people to enjoy the benefits of innovation — new conveniences and efficiencies — while also preserving informational control and freedom of choice. Always a social value and norm, privacy has nonetheless evolved beyond a legal compliance requirement to be recognized as a market imperative and a critical enabler of trust and freedoms in our information society.

There is a growing understanding that innovation and competitiveness must be approached from a “design-thinking” perspective — namely, a way of viewing the world and overcoming constraints that is at once holistic, interdisciplinary, integrative, creative, innovative, and inspiring.

Privacy, too, must be approached from the same design-thinking perspective. Privacy must be incorporated into networked data systems and technologies, by default. Privacy must become integral to organizational priorities, project objectives, design processes, and planning operations embedded into every standard, protocol, or process that touches consumers’ lives. The IPC seeks to make this vision possible by establishing a universal framework for the strongest protection of privacy in the modern era.

In brief, the scale and complexity of current information systems, networks and practices require a new and updated set of universal privacy design and practice principles that are at once robust, comprehensive, and capable of assuring privacy and trust amidst the new global realities.

As suggested above, these global realities include a networked world with invisible borders and opaque jurisdictions, wherein (personal) data is constantly moving around the clock. Everything has become instantly searchable, retrievable, and usable. A million new participants and devices join the online dialogue every day. We need a set of organizing principles to engineer privacy into the Internet 2.0 of social networking and interactive media, cloud computing, ubiquitous surveillance, and personalized, predictive data-mining.

While some naysayers and doomsayers say “Privacy is dead”, we know that is not the case, but an overhaul is needed to the 30-year old principles of fair information practices² (“FIPs”) in order to keep step with the requirements of the modern Information Age.

THE PRIVACY BY DESIGN CHALLENGE

Our *Privacy by Design* (“PbD”) approach emerged in the mid-1990s, in response to the design of large-scale information systems. PbD represents an extension of the Privacy Enhancing Technologies (“PETs”) concept. Both are principles-based approach to building privacy into information systems, but PbD goes beyond specific technologies and includes accountable business practices and operations, physical architectures and networked information ecosystems.³

While classical PETs should not serve to impair system functionality, PbD goes beyond this to accommodate legitimate business objectives and functions of the information system—seeking to minimize any privacy-invasive risks or impacts, from the outset.⁴ Taking a distinctively positive-sum, as opposed to a zero-sum approach, PbD promotes a doubly-enabling, win-win approach to privacy and (not versus) other functionalities.

The *Privacy by Design* approach is built upon seven Foundational Principles:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy

A full description and discussion of these principles may be found in IPC publications available at www.privacybydesign.ca and www.ipc.on.ca

PRIVACY BY DESIGN AND THE FAIR INFORMATION PRACTICES

The universal privacy principles contained in Fair Information Practices are affirmed by those of *Privacy by Design*, but are extended to create a higher global standard. PbD represents a significant “raising” of the privacy “bar.”

In particular, the following three PbD Foundational Principles go farther than traditional FIPs:

Proactive not Reactive; Preventative not Remedial/ Privacy as the Default – This involves demonstrating a clear commitment, at the highest levels, to proactively set and enforce high standards of privacy – generally higher

than the standards set out by global privacy laws and regulation. This can be achieved many ways, but typically by starting at the top with a clear commitment from the leaders or Executive. See, for example, the IPC's "Privacy and Boards of Directors" paper.⁵

Privacy Embedded into Design – This involves putting in place a systemic program or methodology to ensure that privacy is thoroughly integrated into operations. It should be standards-based and amenable to review, validation, and incremental improvements. All privacy threats and risks should be identified and mitigated to the fullest extent possible, in a documented action plan. See, for example, the IPC's 2009 "Accountability" paper.⁶

Full Functionality – Positive-Sum not Zero-Sum – All legitimate business interests and objectives are identified early, desired functions are articulated, agreed metrics applied, and unnecessary trade-offs rejected in favour of achieving multi-functional solutions. The technology, process or infrastructure must deliver measurable positive-sum privacy results – PbD is doubly-enabling in nature, permitting full functionality – real, practical results and strong privacy protection – with beneficial outcomes to be achieved for multiple parties or stakeholders. When the privacy solution turns a privacy-invasive technology into a privacy-respecting one, such as video surveillance or biometrics, with no loss of functionality, then we call that a transformative technology.⁷ Positive-sum results should be made public in order to become best practices.

The *Privacy by Design* approach is now being recognized around the world, not only by leading business organizations but, notably, by public policymakers and legislators: In a March 2010 Opinion issued on the eve of a major European undertaking to review and revise European Data Protection Laws, the European Data Protection Supervisor (EDPS), Mr. Peter Hustinx, observed:

"Trust, or rather its absence, has been identified as a core issue in the emergence and successful deployment of information and communications technologies. If people do not trust ICT, these technologies are likely to fail.⁸ ... Such trust will only be secured if ICTs are reliable, secure, under individuals' control and if the protection of their personal data and privacy is guaranteed. To significantly minimise the risks and to secure users' willingness to rely on ICTs, it is crucial to integrate, at a practical level, data protection and privacy from the very inception of new ICTs. This need for a "Privacy by Design" approach should be reflected in the EU data protection legal framework at different levels of laws and policy making".⁹

"THE PRIVACY BY DESIGN APPROACH IS NOW BEING RECOGNIZED AROUND THE WORLD, NOT ONLY BY LEADING BUSINESS ORGANIZATIONS BUT, NOTABLY, BY PUBLIC POLICY-MAKERS AND LEGISLATORS"

Mr. Hustinx's call for a more comprehensive, proactive approach to privacy is being echoed by Data Protection authorities around the world, and with good reason. In 2001, marketing guru Bruce Kasanoff wrote presciently:

"One thing is certain: Technological advances will force changes in the laws around the globe that protect individual privacy. If you wait for these changes to become obvious, you will forfeit a powerful competitive advantage. People trust leaders, not followers. Once legislation creates new standards for appropriate behaviour, the public will be drawn to companies that can claim to have followed such standards before they were mandatory."¹⁰

CONCLUSION

"Privacy is good for business" is a mantra of the Information and Privacy Commissioner of Ontario that has, within 15 years, become a legal, market and functional requirement, not only for businesses but for ALL organizations – public, private and non-profit – that handle personal information. The proposition is straightforward: build privacy into your data management systems from the outset and reap the many rewards of enhanced trust and consumer confidence. The new realities and challenges of the Information Age require more robust fair information practices to be applied to a wide range of application scenarios, in multiple jurisdictions around the world. Privacy by Design, as reflected in the seven Foundational Principles, responds directly to this need. 🍁



ANN CAVOUKIAN, Ph.D.
INFORMATION AND PRIVACY
COMMISSIONER OF ONTARIO

REFERENCES

- 1 Ann Cavoukian and Don Tapscott, *Privacy and the Open Networked Enterprise* (2005, rev. 2006) at www.ipc.on.ca/images/Resources/priv-opennetw.pdf
- 2 See, for example, Ann Cavoukian, Ph.D., *Creation of a Global Privacy Standard* (November 2006) at www.ipc.on.ca/images/Resources/gps.pdf
- 3 Ann Cavoukian, Ph.D., *Privacy by Design* (Jan 2009) at www.ipc.on.ca/images/Resources/privacybydesign.pdf
- 4 Ann Cavoukian, Ph.D., *Moving Forward From PETs to PETs Plus: The Time for Change is Now* (Jan 2009) at www.ipc.on.ca/images/Resources/petsplus_3.pdf
- 5 Ann Cavoukian, Ph.D., *Privacy and Boards of Directors: What You Don't Know Can Hurt You* (2003, revised 2007) at www.ipc.on.ca/images/Resources/director_2.pdf
- 6 Ann Cavoukian, Ph.D., Martin Abrams, and Scott Taylor, *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices* (Nov 2009) at www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf
- 7 Ann Cavoukian, Ph.D., *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum* (March 2009) at www.ipc.on.ca/images/Resources/trans-tech.pdf
- 8 Peter Hustinx, EDPS, *Opinion on Privacy in the Digital Age: "Privacy by Design" as a key tool to ensure citizens' trust in ICTs*, Para 113 in www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf
- 9 Peter Hustinx, *Press Release* <http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/10/6>
- 10 Bruce Kasanoff, *Making it Personal: how to profit from personalization without invading privacy*, (Perseus, 2001) p. 65

Hiring in a Social Media Age

BY AVNER LEVIN, SJD

CHAIR, LAW & BUSINESS DEPARTMENT, TED ROGERS SCHOOL OF MANAGEMENT, RYERSON UNIVERSITY

The number of organizations that rely on the information they collect through Google, Facebook and Spokeo is continuously on the rise.¹ Are current practices, of using online information for hiring decisions, ethical? May they be conducted ethically under certain conditions? This article will look at some common practices in order to address these questions.

HIRING PRACTICES

Organizations display a wide range of hiring practices and policies regarding online information. One of the most common practices is the unauthorized use of such information in order to formulate a decision or an opinion about a candidate. In its simplest form this amounts to googling a person, not by authorized human resources personnel but by someone such as a future immediate manager. In more sophisticated forms these unauthorized individuals embark on “fishing” expeditions on popular social media such as Facebook, taking advantage of unrestricted profiles or working through ‘friends’ of ‘friends’. Not all information about a candidate originates *with* the candidate, and organizations often discover such information on the social media platforms of others. The source of the information has ethical implications that are important to this discussion.

As use of online information increases so does the incorporation of this practice into formal organizational policy. Online sources may be accessed by human resources personnel, or by another party who has been contracted to provide such information. One popular example is Spokeo, an online business that aggregates information from a variety of online sources, including online social networks, and that offers subscriptions to its database.²

In an attempt to control the use of on-line media, firms may implement a practice that requires the candidate to be informed if on-line information is used in the hiring practice. This does not guarantee, however, that the practice is followed. Additionally, some organizations have taken the position that not disclosing such investigations is important to ensure that the information collected is authentic, and that hiring for certain sensitive positions, such as law enforcement positions, would be compromised otherwise.

Finally, it should be noted, that although they are a shrinking minority, there are organizations that have taken the position that they already have a hiring process that works for them and produces desirable candidates, and that in light of the success of their existing process they see no need to take online information into consideration as part of their hiring decisions.

ETHICAL IMPLICATIONS AND CONSIDERATIONS

Several other facts must be taken into consideration in light of the range of approaches to the use of online information. Individuals are comfortable posting large amounts of personal information online, but they generally do so while differentiating between destinations for this information. Individuals expect that information will not be shared between these destinations. This expectation is known as “network privacy”.³ Organizations, by and large, refuse to accept such network privacy concerns as valid, and adhere to the traditional approach by which personal information that is to be kept private must not be disclosed in the first place.⁴

The ethical question, therefore, is clear: should organizations use information that was not provided online with the intention of use by them? In light of current practice this may be a moot question, but it remains a question worth asking. Would organizations use information in the hiring process that would result in illegal discrimination? For example, is and, more importantly, should information about a candidate’s race, national or ethnic origin, sexual preference or religion be used? How does this compare with the use of other information not intended to be received as part of an application for employment? There does not appear to be an easy answer to this question, but it is a pity that organizations are at least not considering its implications as they develop information gathering policies and practices.

Organizations that use online information about candidates face additional ethical questions. Is it ethical to collect such information outside of the regular hiring process in for example, the performance evaluation process? Is it ethical not to disclose such collection either before or after it has occurred? And is it ethical to base hiring decisions on information that is derived from sources when you have no way of knowing whether or not they have biases against the candidate?

The answers to some of these questions appear easy enough. First, there does not seem to be either an ethical way or justification, for collecting, and then acting upon, information outside of an organization's defined hiring process. Unauthorized googling, for example, while perhaps irresistible, is unethical. Needless to say, more thorough unauthorized investigations into information online are all the more unethical and should not be condoned. Organizations that strive to operate ethically should, prior to any discussion on the merits of using online information, therefore prohibit such unauthorized practices and enforce them internally.

Second, except for a few, ultra-sensitive, positions, there appears to be no good reason not to disclose to a candidate that the hiring process will involve collection of online information. Organizations routinely disclose to candidates the extent and nature of other information that will be collected about them, through such means as background checks. They might easily include online sources in such a list – and indeed some organizations are beginning to do just that.

Third, although a process based on disreputable sources cannot in the end be ethical itself, not every external source is disreputable. Obviously sources will vary in terms of reliability. In this limited sense, it is more ethical to rely on information provided by the candidate than it is on information provided by others. True, it is possible for people that dislike the candidate to provide correct, even if unflattering, information about a candidate. If an organization were to verify such claims then it would probably be ethical to rely on such corroborated information as well. However, organizations that engage in such practices, let alone have such policies, are few and far between.

There is space here to raise one more ethical consideration which, is perhaps the most basic one, and was alluded to above. An organization must ask itself if its existing hiring process that does not rely on online information is broken. If it works well and selects candidates that go on to become successful, productive employees, then why would it change current practices and, from an ethical perspective, there must very strong reasons for incorporating additional online information. Only if the existing process is broken will an organization look into revising the process, including perhaps, but not obviously, online information.

RECOMMENDATIONS AND CONCLUSION

In the not too distant future every candidate may have an online digital record of his activities, hobbies, friends, political positions and basically, his life. If this information is provided to organizations, they will for the first time, have easy access to information about candidates that they have not traditionally collected. The boundaries between work and private life will blur to an extent that individuals will no longer be able to separate these parts of their life. To navigate this new terrain ethically organizations should consider the following recommendations:

- Develop an understanding of online social media and their role in the culture and communication behaviour of their candidates.
- Formulate, disclose to candidates, and enforce internally clear, transparent rules and guidelines about the use of social media for hiring purposes. Some examples:
 - If you look at online information – say so
 - List your sources and let the candidate know in advance
 - Ignore third parties with agendas that you do not share.
- Resist the temptation to seek unnecessary online information, and if such information is obtained, or unsolicited information is received, refrain from using it.


Hopefully, the suggestions and discussion above may lead to more ethical behaviour that future candidates will no doubt appreciate. 🍁



AVNER LEVIN, SJD
CHAIR, LAW & BUSINESS DEPARTMENT,
TED ROGERS SCHOOL OF MANAGEMENT,
RYERSON UNIVERSITY

REFERENCES

- 1 For a comparison of how the landscape has changed take a look at the first survey conducted in Canada about this issue in 2008, and published by the Privacy Institute as "The Next Digital Divide: Online Social Network Privacy" (available at http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_QSN_Report.pdf) and compare it with Microsoft's comprehensive survey released earlier this year (available at <http://www.microsoft.com/privacy/dpd/research.aspx>).
- 2 <http://www.spokeo.com>
- 3 For more on this see Levin, A., Sanchez Abril, P., "Two Notions of Privacy Online" *Vanderbilt Journal of Entertainment and Technology Law* 11 (4) 1001-1051 (2009).
- 4 The legal aspects of this issue are beyond the scope of this article.



Privacy Law: Questions and Answers

BY CHRISTINE LONSDALE
PARTNER, MCCARTHY TÉTRAULT LLP

WHY IS PRIVACY IMPORTANT TO BUSINESS?

Perceived inattention to privacy issues in today's information economy presents regulatory risk, litigation risk and reputational risk. First, privacy regimes in many jurisdictions are being brought up to date with communications technology. Many of these new laws carry significant penalties for breaches. No organization wants to be the subject of an investigation by a privacy commissioner because privacy breaches and investigations often become very public affairs. Privacy breaches can also lead to expensive and very public class action law suits by individuals who feel that their personal information has been misused or carelessly handled. Practically speaking, people do not normally or knowingly do business with or give their personal information to a business they do not trust. As a result, a business with a comprehensive approach to privacy can gain a significant competitive advantage through enhanced customer loyalty and retention, and improved quality of data.

WHY SHOULD MY BUSINESS HAVE AN UP-TO-DATE PRIVACY POLICY?

In order to demonstrate a culture of privacy that permeates all aspects of the business, a clear and comprehensive privacy policy is essential. Key features of a privacy policy are to:

- Identify the entities covered by the policy;
- Identify the type of personal information that may be collected;
- Identify the purposes for which personal information is collected, used and disclosed.
- Identify the types of persons with whom the organization may share personal information, such as service providers, sub-contractors, law enforcement, etc.
- Provide information on how an individual may request access to his or her personal information; and
- Provide contact information for the privacy officer.

Privacy policies should be clear and readily understood by a business' customers, partner organizations and its own employees. The Privacy Commissioner of Canada recently found that Google breached the *Personal Information Protection and Electronic Documents Act* (PIPEDA) when vehicles collecting data for Google's Street View software collected payload data from unencrypted WiFi networks. Google had a privacy policy in place which required counsel to review all codes and products to determine if privacy issues were raised. However, an engineer for Street View made this determination unilaterally without reference to counsel resulting in the breach.

WHEN SHOULD AN ORGANIZATION CONSIDER A PRIVACY AUDIT?

A privacy audit should be the starting point for any organization looking to implement a comprehensive approach to privacy. A privacy audit will identify gaps in an organization's privacy policies opposite the relevant legal requirements, recommend measures for filling those gaps, and even provide training on privacy for employees and management. A privacy audit should answer the following questions about personal information used within an organization:

- What personal information is collected?
- Who is it collected from?
- How does it enter the organization?
- For what purposes is it used?
- For what purposes is it disclosed outside the organization and to whom?
- Where is it stored and how is it secured?
- What are the relevant documents within the organization?
- How well is the privacy policy known and applied within the organization?

These are essential questions that every organization should consider in today's business environment. These are also questions to which every organization should, in turn, demand answers, when entering into information outsourcing contracts with third parties. Being able to demonstrate that your organization has considered and answered these questions in a systematic fashion can be a major advantage when seeking to enter into contracts which involve sharing personal information with other enterprises.

“IN ORDER TO DEMONSTRATE A CULTURE OF PRIVACY THAT PERMEATES ALL ASPECTS OF THE BUSINESS, A CLEAR AND COMPREHENSIVE PRIVACY POLICY IS ESSENTIAL.”

WHAT LEGISLATIVE CHANGES ARE ON THE HORIZON?

New Law In May 2010, Alberta amended the *Personal Information Protection Act* (PIPA). The amendments set out new reporting requirements when a security breach poses a real risk of significant harm to an individual and allow for sanctions of up to \$10,000 for individuals and \$100,000 for corporations for failure to give notice. The PIPA amendments also provide individuals who have suffered harm resulting from a breach with a statutory cause of action against a person convicted under the Act.

Proposed Law Bill C-29, which would amend PIPEDA, underwent its first reading in federal parliament in May 2010. At the time of writing, these amendments have not been passed. The most significant amendments are to the notification requirements under the Act, which would require organizations to report to the Privacy Commissioner any “material” security breaches. The amendments do not impose sanctions on organizations found to be in contravention of the Act, but they do allow the Privacy Commissioner to conduct investigations and audits of an organization's information handling practices and to respond to complaints.

Proposed Law In May 2010, the federal government re-introduced the *Fighting Internet and Wireless Spam Act* (FISA). If passed, FISA would prohibit unsolicited commercial communication by electronic means, starting from the assumption that all electronic messages are unwanted spam and requiring either express or implied consent from the recipient. FISA would also prohibit unauthorized installation of commercial software, such as spyware, and unauthorized compiling or supplying of electronic addresses. In terms of enforcement, FISA

provides for extended liability and allows for sharing of evidence with international partners to pursue spammers operating out of foreign jurisdictions.

WHAT IS MY LITIGATION RISK?

A class action lawsuit has recently been initiated against Facebook in Manitoba. The lawsuit alleges that Facebook changed its privacy policies without proper notice, allowing previously protected personal information, such as pictures, photos, and user names, to enter the public domain without user consent. The lawsuit also alleges that Facebook improperly shared user information with third party advertisers and developers, such as Zynga. Facebook and Zynga, which run popular games like Farmville, have also been the targets of class actions in California over similar allegations. The Manitoba lawsuit has not been certified yet, but it illustrates two things. Litigation in the U.S. is often a bellweather for what will occur in Canada. Second, although privacy breaches can initially appear to have only minor risks, the institution of a class action can be a very newsworthy and costly event. 🍁



CHRISTINE LONSDALE
PARTNER,
MCCARTHY TÉTRAULT LLP

New EthicsCentre Members



BDC is Canada's business development bank. From more than 100 business centres across Canada, it promotes entrepreneurship by providing highly tailored financing, venture capital and consulting services to entrepreneurs.



Investors Group has been helping Canadians achieve their financial goals for over 80 years. With a heritage of grassroots involvement, corporate funding, and project initiation, the company has created a strong culture of caring for communities. Investors attracts people who are both ambitious and care about those they serve. This translates into a deep interest in community needs and a sustainable focus on corporate citizenship.

Business Ethics Scholarship

Gail Henderson, a doctoral student in law at the University of Toronto, has been awarded the 2010 Ethics Centre graduate scholarship (\$5000) in business ethics. Her project considers whether boards of directors of Canadian companies have a fiduciary duty to future generations to consider environmental impacts from operations. The project is timely in light of the reliance of the Canadian economy on resource extraction, and the Deep Horizon blowout in the Gulf of Mexico. Eighteen applications for the scholarship were received from across the country. Details of the 2011 scholarship will be posted on the Centre's website in early 2011.



BOARD OF DIRECTORS

M.J. (Mimi) Marrocco,

University of St. Michael's
College, Chair

Michael Davies, (Ret.) General
Electric Canada Inc., Vice Chair/
Secretary

Georges Dessaulles,
Vice Chair

Joan Grass, Business Ethics
Consultant, Vice Chair

Derek Hayes, (Ret.) CIBC, Past Chair

Blair Peberdy,
Toronto Hydro, Vice Chair

Vincent C. Power,
Sears Canada, Treasurer

Thomas A. Bogart,
Sun Life Financial Inc.

Louise Cannon,
Scotiabank

Hentie Dirker,
Siemens Canada Limited

Simon Fish,
BMO Financial Group

Ruth Fothergill,
Export Development Canada

Sally Gunz,
University of Waterloo

Howard Kaufman,
Fasken Martineau DuMoulin LLP

Christopher Montague,
TD Bank Financial Group

Philip Moore,
McCarthy Tétrault

Mario Nigro,

Blake, Cassels & Graydon LLP

Flip Oberth,
Flipside Solutions Inc.

Hilary Randall-Grace,
Deloitte & Touche LLP

Robert Timberg,
Former Director, Ethics, Nortel

Maureen Wareham,
Hydro One Inc.

Robert Yalden,
Osler, Hoskin & Harcourt LLP

STAFF

Hélène Yaremko-Jarvis,
B.C.L., LL.B., Executive Director

Lois Marsh, Administration

CALENDAR OF EVENTS

LUNCHEON EVENT

January 12, 2011 - Dr. Hentie Dirker
Regional Compliance Officer, Siemens
Canada Limited, *The Siemens Story*

LUNCHEON EVENT

March 9, 2011 - Ellen Roseman
Reporter, Toronto Star
Who's afraid of financial literacy?

MANAGEMENT ETHICS

is published seasonally by EthicsCentre CA. We welcome appropriate announcements, letters to the editors, short articles of 300 to 1,000 words (which will be subject to usual editorial processes) and suggestions from readers.

Management Ethics is edited by Sheerin Kalia.

Back issues of Management Ethics are on-line at the Centre's web site. The opinions expressed in Management Ethics do not necessarily represent the opinions of EthicsCentre CA.

This newsletter may be reproduced without permission as long as proper acknowledgment is given.

YOU CAN REACH US AT:

One Yonge Street, Suite 1801,
Toronto, Ontario M5E 1W7

Phone: 416-368-7525

Fax: 416-369-0515

E-mail: editor@ethicscentre.ca

Web site: www.ethicscentre.ca

Design & Layout: Context Creative
Printing: Courtesy of The Canadian
Institute of Chartered Accountants.

Charitable registration number:
12162 1932 RR0001