Privacy and the Open Networked Enterprise

December 2006

Privacy and the Open Networked Enterprise

Foreword

This white paper represents a joint effort between the Information and Privacy Commissioner of Ontario (IPC) and the New Paradigm Learning Corporation (NPLC). In 2004, the NPLC launched the Information Technology and Competitive Advantage program to examine the impact of information technology on business strategies in the 21st century. This in turn led to the conceptualization of the "Open Networked Enterprise," or the ONE This paper is an analysis of information privacy and security issues relating to **both** companies and consumers.

A number of high-profile privacy breaches have drawn to the attention of consumers how important it is to be aware of who is in possession of their information and how it is being used. Consumers are getting much smarter, no longer blindly accepting that companies need to know everything about them in order to "serve them better" or get better products. Many businesses are now beginning to encounter consumers who want to have a say in what information they will give out and who is permitted to use it. Privacy is no longer just a compliance issue – it has become a business issue. The successful companies of the future will be those who accept the present-day fact that "*privacy is good for business*," and ultimately leads to a competitive advantage.

Ann Cavoukian, Ph.D.
Commissioner
June 2005

The Idea in Brief

Companies that take advantage of an Open Networked Enterprise (ONE) have the ability to become increasingly inter-networked, and to share more and different kinds of information than ever before. But while this network allows for greater transparency of information, it also raises the central issue of privacy. By necessity, within an ONE corporate boundaries blur: in order to facilitate effective collaboration, the ONE compiles highly granular data from disparate sources (i.e., multiple stakeholders) to create a more holistic business intelligence. However, as active ONEs become increasingly global, this information may come from jurisdictions with looser privacy laws than the home company and, problematically, may overlap with personal information.

At stake in this march toward global transparency is the value of information itself, especially personally identifiable information (**PII**). The lifeblood of the 21st century

economy, information must increasingly be viewed as both an asset and a liability that requires responsible management practices. A company adopting an ONE model is confronted with fundamental questions relating to its treatment of information:

1. With whom will it share its **PII**?
2. How will it manage that data internally?
3. How should it involve customers in managing their own **PII**?
4. What personal data will and should it receive from others?
5. Where should it set the limits of **PII** collection by new technologies?

New information technologies inevitably affect levels of personal privacy. History has taught us that excesses and abuses of personal information tend to provoke backlashes in the form of counter-reactive behaviour by consumers and legislative/regulatory bodies. Most, if not all, of the privacy issues described in this paper are currently subjects of heightened public awareness and controversy, and it is public awareness and controversy that lead to regulation and legislation.

For these and many other good reasons, a company's ONE model is well advised to meet the highest standards of responsible information management. By treating personal information responsibly, companies can harness the capabilities of a new breed of consumers, privacy hawks, who have strong views about personal information and privacy. Smart firms will build appropriate and effective privacy policies and practices into their systems. In doing so, these firms can avoid potential disasters and create the conditions for trust, loyalty, long-term relationships and economic advantage. Privacy is no longer a compliance issue; it is a business issue. It must be a business imperative.

The context: privacy and technology

The rise in modern communications has brought the issue of privacy to the forefront of public consciousness. Indeed, the modern concept of privacy emerged in reaction to information and communications technologies in the late 1800s that suddenly make it possible to effectively capture, store and disseminate information on a mass scale never before contemplated. With the development of the photograph, telegraph and mass printing methods the world began to shrink. The emergence of the "yellow press" in the early part of the 20th century triggered the earliest definition of privacy as personal freedom from unwanted intrusions, or "the right to be let alone." From constitutional protection against search and seizure to restrictions upon free speech, to the implementation of slander and tort laws, common law in the 20th century tended to recognize and respond to privacy threats principally in terms of intrusion upon an individual's personal space and private conversations, as well as upon his or her good name and reputation.

The appearance of mainframe computers, centralized electronic databases and computerized records in the 1960s and 1970s triggered the next wave of privacy protections. The large-scale collection by governments of secret, centralized dossiers on citizens and the frequent misuse of that information led to the development of laws to restrict governments' abilities to compile and use such records. At the same time, however, freedom of information laws were also enacted to promote greater openness and transparency for the sharing of new classes of information with multiple stakeholders and to enhance individuals' rights of access to personal information in those databases.

In response to the misuse of large-scale computerized databases by private organizations in the financial, credit and medical sectors, similar "sunshine" laws were also put in place to protect individuals and their highly personal information, such as credit or health records. Fundamental "privacy" principles came into widespread currency, such as those set out by the U.S. Family Educational Rights and Privacy Act of 1974:[1]

- **Collection Limitation:** There must be no personal data record keeping systems whose very existence is secret.
- **Disclosure:** There must be a way for an individual to find out what information about himself or herself is in a record, and how it is used.
- **Secondary Usage:** There must be a way for an individual to prevent information about himself or herself, which was obtained for one purpose, from being used or made available for other purposes without consent.
- **Record Correction:** There must be a way for an individual to correct or amend a record of identifiable information about himself or herself.
- **Security:** Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

By the late 1970s, information and communication technologies were facilitating a growing global trade in, and processing of, personal data. As various countries passed laws restricting the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data, worries arose that global trade would be constrained by the growing patchwork of national laws. In a far-sighted initiative, members of the Organisation for Economic Co-operation and Development (OECD) came together and agreed to codify a set of principles that might serve as a framework for countries to use when drafting and implementing their own laws. The result was the 1980 OECD Guidelines on the

1 **Family Educational Rights and Privacy Act (FERPA)**, (20 U.S.C. § 1232g; 34 CFR Part 99), 1974.

Protection of Privacy and Transborder Flows of Personal Data, a document which expressed and described eight "fair information practices" as follows:

- **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and current.
- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified no later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes, and as are specified on each occasion of change of purpose.
- **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:
  - with the consent of the data subject, or
  - by the authority of law.
- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure.
- **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of stored personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation Principle:** An individual should have the right:
  a) to obtain from a data controller or equivalent, confirmation of whether or not the data controller has data relating to him or her;
  b) to have communicated to him (or her), data relating to him (or her) within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him (or her);
  c) to be given reasons if a request made under subparagraph (a) or (b) is denied, and to be able to challenge such denial; and
  d) to challenge data relating to him or her and, if the challenge is successful, to have the data erased, rectified, completed or amended.

- **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

Since 1980, these voluntary "fair information practices" (FIPs) have been widely adopted around the world in statutes, standards, codes of practice, information technologies, and in norms and common practices. In Canada, for example, businesses, consumers and the government agreed to adopt a comprehensive set of privacy practices, known as the Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), which was subsequently incorporated in its entirety into Canada's private sector privacy law. In the U.S., since the early 1970s, each successive government has remained committed to monitoring the "information practices" of organizations or, more specifically, the methods in which these organizations collect and use personal information and the safeguards they employ to ensure those practices are fair and provide adequate privacy protection. The result of this government intervention has been a series of guidelines and model codes that now represent commonly accepted principles, more formally known as Fair Information Practices (FIPs). Common throughout the U.S., FIPs are five core tenets of privacy protection that have proven both successful and enduring:

- Notice/Awareness;
- Choice/Consent;
- Access/Participation;
- Integrity/Security;
- Enforcement/Redress.

The most essential principle of the five is the first: Notice/Awareness. Consumers need to have knowledge of an organization's privacy and information policies before any personal information can be collected and stored by that organization. This practice specifically protects consumers: without such proper notice, they cannot make any reasonably informed decision regarding the use and disclosure of their personal information. Furthermore, the other principles are only relevant when the consumer has knowledge of an organization's information and privacy policies, and his or her rights as a consumer with respect to those policies. But despite this harmonization, significant variations persist in American law: the OECD Guidelines provide a floor, not a ceiling, for privacy protection.

Regardless of specific interpretation or manner of implementation, the OECD Guidelines and other similar FIPs accomplish two functions:

- They establish and confer broad rights on individuals, or data subjects, with respect to the collection, use and disclosure of their personal information by other parties.

- They set out broad responsibilities and obligations of organizations in respect to the collection, use and disclosure of personal information held in their custody.

The first function is commonly known as *information privacy*: the right or ability of individuals to exercise a measure of control over the collection, use and disclosure of their personal information by others. The second is *data protection*: the responsibility of organizations that collect, use, and disclose personal information to abide by an externally established set of rules.

It is important to understand the distinction between the two functions. The first approaches privacy from the perspective of the individual data subject, the second from the perspective of the custodial organization. Good privacy laws and data protection seek to reconcile the interests and objectives of both parties, but new technologies typically upset pre-existing balances.

What is personal information? Many organizations mistakenly believe that personal information is limited to basic "tombstone" data provided directly by the individual such as name, address, phone number, socioeconomic details and so forth. Although statutory definitions vary around the world, personal information can include far more than this, such as:

- Any information associated or linked to an identifiable individual (e.g., personal preferences, beliefs, opinions, habits, family and friends);
- Physical and biological attributes (photo images, genetic data);
- Account numbers and any unique identifiers associated with an individual;
- Transaction data (record of sales, customer service requests, returns logins, phone calls);
- Transaction data of devices registered to an individual (phone numbers, computer logins, location data);
- Information about an individual provided by third parties (credit reports, employment references); and
- Information inferred, derived, or generated from data held about an individual (profiles, scores).

Privacy and the ONE

Corporate Boundaries, Processes: How can privacy be protected in a business Web? Will the ONE's modular, flexible approach to operations obscure or diminish accountability for unauthorized uses of customer data?

Modus Operandi: When employees become empowered to make decisions and try innovative approaches, will the devolution of authority diminish or enhance overall responsibility for, and adherence to, organizational policies intended to respect customer privacy? Conversely, will heavy-handed workplace surveillance measures and practices discourage employee initiative?

Relationships: Will the ONE go beyond traditional top-down approaches to engage and collaborate actively with clients, fostering what we describe as customer managed relationships?

Information Liquidity: How will the ONE manage the privacy risks associated with reliance on externally networked personal information and automated decision-making?

Technology: Will the ONE steer clear of temptations to use new technologies to collect excessive personal information from customers and employees?

1.0 New Boundaries, New Business Processes

1.1 Context

As companies become inter-networked, they share new kinds of information. Given that the ONE is increasingly global, as networks expand across national as well as statistical boundaries, the risks associated with information sharing increase: information may be shared between companies with different laws governing their treatment of and responsibility to consumer privacy.

In addition, ONE business processes are necessarily characterized by dense interconnections and constantly evolving relationships with a variety of internal and external partners, agents, affiliates and contractors. This modular approach to business affords high degrees of flexibility and adaptation to changing business environments and strategies. It also demands that the ONE focus on its core strengths.

1.2 Privacy concerns: outsourcing and offshoring

Personal data are increasingly handled by third party participants in information networks, and they are dealt with through outsourcing or offshoring practices. In general, "outsourcing" occurs when a company contracts out work to another company. "Offshoring" involves moving the work to another country, whether to a captive entity (i.e., a firm subsidiary) or to a third party supplier.[2]

Such third party data relationships are everywhere; now few businesses can survive without relying on other firms to help provide, process, or manage data. Whether exchanging data with business partners or sharing information internally, each transaction between businesses establishes a data relationship. These relationships must be carefully managed to ensure compliance with both an organization's policies and applicable external regulations around data protection.

In a b-web, information security is only as effective as the weakest link: "If one trading partner has a poor identity management program, another never tests its disaster recovery plan, and a third does not regularly assess its information technology outsourcers' compliance with information security policies, one's own security posture cannot logically rise above the lowest point achieved by these other entities."[3] As more organizations collaborate intimately, it becomes increasingly difficult for senior management to fully identify and manage the larger organization's ever growing risk interdependency. Collaboration has changed the security landscape; the behaviour of a single organization can have a wide-ranging impact on other b-web participants. Senior managers may think their organization is adequately protected when in reality their investments are undermined by process flaws. The statistic of such potential breaches is cause for concern: according to an Ernst & Young global survey, 80 per cent of respondents failed to conduct a regular assessment of their IT outsourcer's compliance with the host organization's information security and privacy regulatory requirements.[4]

Reported information security breaches are occurring with increasing frequency, severity and cost to businesses.[5] Organizations are understandably reluctant to report data security incidents, for fear of the negative effects on their competitive stance, public image and stock value. This reluctance is being trumped now by

2 Offshore Operations: Industry Feedback, Financial Services Authority (FSA), April 2005.

3 Global Information Security Survey 2004, Ernst & Young, p. 3 **http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf**

4 *Ibid*, p. 21.

5 See, for example, CSI/FBI Computer Crime and Security Survey (2002, 2004) **http://www.gocsi.com** and Ernst & Young Global Information Security Survey (2004) **http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf** and Deloitte Global Financial Services Industry Outlook (2004, 2005) **http://www.deloitte.com/gfsi**

new accountability laws and regulations containing mandatory reporting requirements. Quite often, firms are not even aware that data security breaches have taken place if they occurred among business partners and affiliates. New data governance and similar compliance rules will strip firms of any reluctance to assume greater responsibility for and control over the actions of others.

The risks of outsourcing are thus known to be significant: it takes only one incident to damage years of brand building, and with the corporate identity go the trust, loyalty and business of customers, regardless of who is technically or legally liable. One cautionary tale of the risks of insufficient privacy monitoring involves a large national bank that outsourced its customer care and call centre operations to a vendor in the Ukraine.[6] The company concluded contracts with the vendor to ensure that it took full responsibility for complying with all U.S. regulatory requirements, as well as with the bank's own privacy policy, which included a strict do not share with third parties for secondary uses without a consent clause. The Ukrainian vendor also contracted to comply with strict data protection and information security requirements as per the U.S. Federal Trade Commission's Safeguards Rule. Nine months after operations began, thousands of U.S. customers began receiving charges on their credit card statements for magazine subscriptions and online services that they had never purchased. Hundreds complained that they became victims of identity theft, apparently a result of information leaks. A few customers reported that their entire bank balances had been transferred to untraceable locations. In response, the bank hired a forensic expert to determine where the possible data leak could have occurred. It was eventually discovered that the leak had transpired at an offshore outsourced location. It was traced to a new employee of the Ukrainian vendor who had remote access to the company's data warehouse. Notably, investigators found that the vendor's IT director had known about the leak months before the incident occurred, but never bothered to report it.

Such risks are not limited to offshore operations; companies should also determine whether domestic partners observe adequate security standards. In March 2005, for instance, the Federal Trade Commission recently settled a case in which a company that sold a shopping cart application to a Web merchant then provided customer information to other entities, contrary to the merchant's privacy policy.[7] The Web company had failed to ensure partner compliance before signing the contract.

The challenges to ensuring that security standards are met and maintained are significant. The average *Fortune* 500 company typically has over 10,000 contracts and agreements with partners, affiliates, contractors and other third parties, all of

6 Dr. Larry Ponemon, "Are You Practicing Safe Outsourcing?," Darwinmag.com, April 2004 **http://www.darwinmag.com/read/040104/ponemon.html**

7 "Internet Service Provider Settles FTC Privacy Charges," Federal Trade Commission, March 10, 2005 **http://www.ftc.gov/opa/2005/03/cartmanager.htm**

whom affect the treatment of personal information. Just understanding data assets, uses and flows can thus be a daunting task, let alone subjecting these assets, uses and flows to clear and comprehensive policies, and enforceable procedures.

At the heart of the debate over privacy is the issue of corporate *accountability*. Organizations that are most visible or proximate to affected individuals bear most of the negative publicity and criticism for privacy breaches. When a privacy breach occurs, it will matter little to the public that the breach actually occurred at a partner's e-commerce payments processing website platform located in another jurisdiction; the organization that the customer deals with directly bears the most accountability and risk. As the most visible target, such an organization can suffer from diminution of brand and loss of credibility and sales, or by incurring the high costs of litigation, compensating victims, re-engineering information systems, or submitting to extensive audit and certification processes. When it comes to allocating blame, public perception can override corporate reality, and therefore the proximate organization must have the strongest incentive to ensure that personal information is managed responsibly.

1.3 Recommendations

Offshoring, outsourcing and third party data relationships pose significant challenges to the governance of personal information. Meeting these challenges requires coordinated and ongoing management of multiple elements of data policy compliance and risk management across all entities in the data sharing relationship. These elements include risk assessment, monitoring of the sharing relationship and prospective third parties, and substantial monitoring, tracking, classifying and regulation of enterprise data flows. But there is no one-size-fits-all solution; the data collection, storage, use, sharing, oversight and enforcement needs of every firm are unique. We do know, however, that a comprehensive approach is more likely to be successful; one that accounts for people, processes, systems and policies.

Any solution must begin with a regulatory review: numerous laws, both current and proposed, restrict or impose conditions on offshoring and outsourcing activities. According to Alan Westin, founder of Privacy and American Business, provisions for protecting personally identifiable information will play a major role in anti-offshoring bills at federal and state levels. A significant data breach or identity theft scandal in just one overseas location could jump start legislative responses. Ignorance of the law, including potential laws, will be no defence.

Legal requirements regarding the treatment or sharing of personal data will determine the ways in which risk is assessed, and the choice of assessment instruments and approaches. Europe, for example, prohibits transborder personal data flows unless certain "adequacy" requirements are satisfied. In the U.S., firms that outsource are already governed by numerous laws and regulations that impose compliance requirements, such as the Sarbanes-Oxley Act, the Health Insurance

Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act, and the Fair Credit Reporting Act.

Outsourcing that involves personal data in particular has recently been drawing attention from regulatory bodies and the general public. Some state laws require that companies choose domestic over foreign workers to process employee data, while other states require disclosure if work on government contracts is undertaken outside the U.S. Maryland and Massachusetts vetoed similar bills in 2004, but it is expected that those bills will return. There are currently 115 anti-offshoring bills pending in 40 states; the majority aim to limit work contracted out by the state. Many aim also to prohibit state aid for overseas outsourcing, enforce disclosure of call centre locations, restrict outsourcing of personal sensitive data such as health or financial, and in some cases to require consent from customers.

California's legislature passed five anti-offshoring bills in 2004. Protective measures included allowing no state contracts for work performed outside the U.S. and no outsourcing of Social Security Numbers, driver's licences and personal health data. One particular law required overseas call centres to disclose their location to residents of California and local employers to report to the state if they moved operations offshore. Governor Schwarzenegger ultimately vetoed all five bills, but the backlash was significant; it is likely that these bills will re-emerge for a second attempt.

Regulations exist at the national level as well: the U.S. Senate passed the Dodd Bill in 2004, which prohibits the awarding of federal contracts to companies with overseas employees. A proposed House resolution also seeks to enforce consent prior to transferring sensitive personal data to countries that lack adequate privacy protections as defined by the Federal Trade Commission. Hillary Clinton's proposed "Safe ID Act" will prohibit businesses from processing sensitive personal information in foreign countries without offering an opt-out choice to the public. In addition, if the Act passes, businesses will become directly liable for any privacy breaches.

In such an environment, rules for data flows and uses should comply across all jurisdictions to established international benchmarks, like COBIT[8] and ISO 17799.[9] Adherence should be monitored through due diligence, site visits, contractual remedies and third party audit and certification.

To manage an ONE effectively, a company must develop a comprehensive set of objectives and policies regarding privacy and security of data uses and flows. These policies must be clearly expressed and effectively communicated throughout the ONE and to all third parties. Some elements to consider:

8 Information Systems Audit and Control Association, **http://www.isaca.org**

9 ISO 17799 Directory, 2005 **http://www.iso-17799.com**

- Minimize data collection, use and security among partners;
- Develop strong contractual agreements and deterrents for third parties;
- Deploy continuous monitoring, auditing and enforcement mechanisms;
- Implement privacy crisis management protocol in the event of a breach; and
- Develop adequate consumer trust to draw upon in the event of an incident (customers may be more forgiving).

Information and communications technologies (ICTs) can also help maintain security for consumers: firewalls and other filtering software, secure transmissions, handling and storage of data, strong authentication, access controls, extensive logging and audit trails, and other safeguards can be assured in part through ICTs, and can significantly increase consumer security. It must be remembered, however, that a critical element of success fully deploying such systems involves comprehensive education, training and awareness programs for all employees involved in these processes.

With regard to *transparency*, current U.S. legislation requires firms to disclose their outsourcing policies and practices to customers. Knowing that customers will be informed about outsourcing arrangements might motivate companies to make sure those arrangements are secure. One U.S. financial company, E-Loan, not only explains its outsourcing practices to its customers, but actually offers them a choice of whether they would like their financial arrangements processed in-house.

2.0 Modus Operandi

2.1 Context

The modus operandi of the ONE is characterized by flatter hierarchies, greater collaboration, devolved decision making, more risk taking, high flexibility, agility, adaptability, and innovation.

2.2 Privacy concerns: the insider conundrum vs. internal surveillance

In such collaborative environments, organization-wide privacy and security policies governing the use of data can be difficult to implement and enforce. Because such policies are often mandated from above, their hierarchical quality may conflict with the more open, collaborative culture of the ONE. Often such policies are perceived as barriers to new and innovative thinking, products and practices.

At the same time, flatter, decentralized organizations may be well-connected, but they are also more vulnerable. The more that senior management has lost its situational awareness (*the degree of accuracy by which perception of the current environment mirrors reality*) the less likely it will be able to comprehend the

organization's ever growing interdependence. Single events can have profound impacts that cascade across the network. Furthermore, when individual employees are empowered, how do you ensure that they respect privacy policies and principles? How do you ensure that data is protected? If everyone is responsible for privacy and security, then perhaps *no one* is.

Recent data privacy and security breaches have focused the public and lawmakers' attention on the poor information management practices and procedures of businesses, especially since large-scale losses and theft of personal information can have profoundly negative effects on innocent individuals.

2.3 The insider conundrum

It is not uncommon for marketing and communications departments, in the pursuit of quarterly objectives and hard metrics (and when given a free hand), to develop initiatives that bypass privacy policies. In their efforts to ensure security, IT departments want to control and lock down all information assets, often by filtering and logging everything, or otherwise engaging in what could be perceived as nosey employee surveillance practices. Software development teams may add invasive privacy and security features to products that act as spyware. Overzealous human resources departments, looking for the perfect employee, may carry out deeper background checks than necessary or engage in psychological profiling. Any of these activities can land a company in hot water.

Sometimes personal data exposure or misuse occurs by accident, such as when pharmaceutical giant Eli Lilly accidentally exposed the email addresses of 669 Prozac users in the "To:" field of an email marketing solicitation, resulting in an FTC investigation and settlement, as well as a tarnished brand and reputation.[10] Quite often, such data loss or unauthorized exposure occurs as a result of negligence or failure to follow simple policies and procedures, such as when laptops with unencrypted personal data go missing, or when default passwords are not changed.

Inside theft is a big problem. It is well known that insiders who access databases often have network authorization, knowledge of data access codes and a precise idea of the information they want to exploit. Surprisingly, most database applications even sophisticated high-end ones store information in "clear text" that is completely unprotected.

10 "Even the unintentional release of sensitive medical information is a serious breach of consumers' trust," said the Director of the FTC's Bureau of Consumer Protection. "Companies that obtain sensitive information in exchange for a promise to keep it confidential must take appropriate steps to ensure the security of that information." **http://www.ftc.gov/opa/2002/01/elililly.htm**

Further, there are more unauthorized accesses to databases than corporations admit to their clients, stockholders and business partners, or report to law enforcement. Gartner estimates that internal employees commit 70 per cent of information intrusions, and more than 95 per cent of the intrusions result in significant financial losses. A 2002 survey of 163 Fortune 1,000 companies found that 70 per cent of reported security breaches were linked to insiders.[11]

Another survey by the Computer Security Institute revealed that over half of all corporate databases have some kind of breach every year, and the average breach results in close to $4 million in losses.[12] And these are just the security problems that companies report!

Non-technical and behavioral forms of intrusion are also common. What makes the insider threat so daunting is that most breaches do not require sophisticated methods, and they most often occur on site during normal working hours by employees, freelance contractors, employees of corporate contractors, and even clients. In some cases, disgruntled employees simply wish to hurt an organization and its reputation.

Finally, there are the security problems associated with external hackers, thieves, and con artists. Why steal one identity from a trash bin when you can steal a million from an insecure database?

Consider some recent breaches:

- Time Warner reported that a cooler sized container of computer tapes containing personal information of 600,000 current and former employees was lost on its way to a data storage facility in March 2005. The computer tapes contained the names, SSNs, and other data pertaining to current and former employees dating back to 1986.
- Data broker ChoicePoint reported the unauthorized access of over 150,000 detailed dossiers by scam artists over a period of a year. At least 700 known instances of identity theft resulted from this security breach. Poor access control and authentication procedures were blamed.
- Online brokerage Ameritrade disclosed in April 2005 that it had lost a backup computer tape containing records of 200,000 customers.
- A former employee of a Washington area Blockbuster Video store was indicted on charges of stealing customer identities and using them to buy more than $117,000 in trips, electronics, and other goods, including a Mercedes-Benz.

11 Richard Mogul, “Danger Within – Protecting your Company from Internal Security Attacks,” *CSO Online*, August 21, 2002 **http://www.csoonline.com/analyst/report400.html**

12 Computer Security Institute/FBI Computer Crime and Security Survey, 2002.

- LexisNexis reported a privacy breach in its Seisint database division. Hackers accessed more than 300,000 profiles, including SSNs and driver's licence numbers more than 10 times the number originally reported. The company blamed poor access management practices.
- A California medical group is currently informing nearly 185,000 current and former patients that their financial and medical records may have been compromised following the theft of computers containing personal data.
- Health-care giant Kaiser Permanente notified 140 patients that a disgruntled former employee had posted confidential information about them on her blog.
- Tokyo Disney amusement parks reported that personal information on 122,000 customers who bought one year admission passes in 2002 was leaked. Several hundred received fraudulent phone calls or direct mail.
- Bank of America admitted it lost backup tapes containing personal information on 1.2 million federal employees, including several Congress members.

This string of high-profile data security breaches has sparked a public firestorm and closer lawmaker scrutiny of businesses' information management and security practices. A flurry of proposals at federal and state levels intends to ensure that businesses assume more responsibility and liability as custodians of personal data.

In response, businesses have invested heavily in information security. A significant and growing percentage of corporations routinely monitor employee behaviour and activities such as Web surfing and email use. We are seeing a strong surge in interest and demand for identity management, authentication, and role based access systems that track and monitor virtually every employee activity.

The concept behind these security efforts is clear: information is an asset, and access needs to be controlled and predicated on strong identification, authorization and auditability.

Strong security enhances privacy, but this trend seems counter to ONE culture. We are seeing a rise in employee litigation against companies in reaction to excessive monitoring and surveillance. Employee privacy is being pitted against customer privacy and employees are losing.

The fundamental problem, again, is ensuring accountability and governance of personal data while respecting the privacy of customers, data subjects and employees. The rogue actions of some empowered staff, however well-intentioned, can have negative effects on the entire organization. At the same time, a heavily monitored and restricted workforce can become less empowered and more resentful, ultimately to the detriment of the ONE.

2.4 Possible solutions

As with any information privacy and security program, there is no one-size-fits-all solution. Every organization is unique, and a lot depends on the nature of the business, the personal information at stake, and the degree of vulnerability and risks involved.

A continuous privacy awareness and training program for employees is a requirement for success. In fact, the most successful ONEs have well developed corporate cultures of customer privacy *and* respect for employees. Clear and comprehensive privacy policies, effectively communicated and enforced, ensure that privacy and security are infused throughout the organization and promoted as everybody's responsibility. It is also not uncommon for performance appraisals and bonuses to be tied to adherence to corporate privacy policies. At the same time, clear and consistent policies on employee surveillance, communicated well and carried out in a fair and impartial manner with appropriate curbs on potential abuses, can go a long way in dissipating employee fears, resentment, and counterproductive behaviour.

Privacy and security leadership is also a necessity: firms require a strong chief privacy officer (CPO) who understands all aspects of the organization and is capable of navigating and working with all departments. When vested with appropriate oversight and/or veto authority, such an individual can become a champion for privacy within an organization, be able to bridge the divides between higher and lower management and between different corporate divisions, and become the "go to" person whenever there are questions or incipient problems. A champion for strong data privacy and security, the CPO can also put in place credible and effective policies governing the use of workplace monitoring technologies without raising employees' concerns about excessive surveillance. A good CPO can reconcile the apparent contradictions between strong data security and employee privacy on the one hand, and the operational needs of the ONE on the other, thereby fostering a climate of trust and collaboration.

Perhaps most significantly, and today more than ever before, the CPO uses new technological tools and automated mechanisms. For example, new database and data flow "discovery tools" can map organizational information flows and minimize security risks by automatically detecting and responding to possible data misuses at the earliest possible stages through heuristic intrusion detection systems. Similar tools exist to evaluate website compliance to privacy and security standards. There has also been a growth in interest in enterprise identity management, access control and automated content filtering systems.

Just as inbound electronic communications can be scanned for viruses and inappropriate content, so too can outbound messages be scanned for protected intellectual property and "leakage" of sensitive personal information. Best of all, these tools can be automated so that "surveillance" need not be arbitrary or performed by a human, except when suspicious incidents are flagged for follow-up.

The emergence and growth of data security technologies and systems has been remarkable. Such technologies are far too numerous to mention here, but a knowledgeable CPO or Chief Information Officer, would be well aware of the latest data security systems.

Technological tools can also be effective in establishing audit trails. One promising solution is to attach a "condition of use," such as client privacy preferences, directly to the data, so that privacy and security policies are effectively "bound up" with the data the client supplies. The rules relating to data use are "wrapped around" the data itself. In this way, many data privacy and security policies can be demonstrably self-enforcing, with little or no need for direct CPO intervention or oversight. IBM's Tivoli Privacy Manager is one such successful tool.[13]

2.5 Summary

As information needs continue to grow, so too will the challenges of complying with a widening range of anticipated regulatory privacy and security requirements and public expectations. A strong culture of privacy and security, and of employee respect and trust, is the foundation for a successful ONE. To maintain agility and flexibility, an empowered Chief Privacy Officer is needed to install the proper mix of policies, procedures, training and technologies that will serve both to manage personal data throughout the ONE's life cycle and to assure employees that they are not being unfairly watched.

3.0 Relationships

3.1 Context

The success of a company's ONE is a function of positive experiences and strong relationships with customers. Word of mouth endorsements are among the most valuable types of marketing any organization can have, and by providing useful, efficient, personalized services and products, the best companies foster enduring trust, loyalty and repeat business. So valuable is the repeat value of a customer that, increasingly, products are given away at discounted prices in favor of establishing a long-term relationship.

3.2 Privacy concerns: consumer trust

In today's hyper-competitive climate, brand and reputation are shorthand vehicles for conveying trusted information, and fostering and reinforcing positive experiences with customers. Trust takes a long time to build, but a short time to erode and lose. Trust is built by making and keeping promises over time, and being transparent and reliable about your commitments and policies.

13 **http://www-306.ibm.com/software/tivoli/products/privacy-mgr-e-bus**

In order to build a more intimate relationship with consumers, businesses are adopting novel techniques to serve customers with personalized services, such as discounted loyalty cards. Integrated customer relationship management (CRM) technologies provide holistic views of customers, their data and their transaction histories, while providing customers with convenient single-window "no wrong door" portals for efficient service.

We are seeing a trend towards relationship and permission-based marketing in an effort to engage the customer in an ongoing, personalized, customized, 1:1 manner.[14] Such marketing techniques depend on collecting and collating as much information as possible about the client in an effort to differentiate, understand and respond to clients' specific needs and wishes (*ideally before they themselves recognize this!*).

Permission-based marketing may result in less data than that obtained through arbitrary online registrations, but the information thus collected is, without a doubt, far more relevant. Further, permission-based marketing also builds loyalty through trust. To use an analogy, a lot more can be accomplished with a sniper's rifle than a shotgun. A case in point: a 2003 survey of over 1,000 persons across the United States found that 70 per cent of respondents were willing to receive legitimate email marketing messages provided that they had given their consent.[15]

In the spring of 2005, Ipsos-Reid conducted a survey that reported that the number of respondents willing to receive commercial email was increasing, again with the caveat that they had given their permission. The survey found that close to 80 per cent of Internet users have registered to receive email from an average of nine commercial websites.[16] Combined with the latest email filters, Internet users can now customize their choice of exactly which companies are allowed into their inbox, and who goes directly to the trash file.

Thin Data, a Toronto based email service provider, began a permission-based marketing campaign on behalf of Mirvish Productions, a theatre production company in Toronto, Canada. Thin Data sent a monthly email newsletter to over 15,000 subscribers and found it was read by 65 per cent of recipients per month. In comparison, it found that less than 30 per cent of recipients of indiscriminant direct mail campaigns opened emails.[17]

14 Seth Godin, *Permission Marketing* (New York: Simon & Schuster, 1999).

15 "Digital Impact Sponsored Survey Shows Majority of Internet Users Request Legitimate Email Marketing Messages Despite Increasing Concerns Over Spam," *Digital Impact*, December 8, 2003 **http://www.digitalimpact.com/ newspress120803.php**

16 "E-mail ad firms winning war against spam," *The Globe and Mail*, March 15, 2004, B11.

17 *Ibid*.

Permission-based marketing, suggests Seth Godin, is like dating.[18] The company or marketer approaches the consumer to request a date. If the consumer says yes, they go out, and if both parties are interested, self-disclosure of personal details takes place. Trust builds over time, and the relationship may continue, perhaps for years, and in some cases, a lifetime.

Building on the idea of permission-based marketing, the concept of the "Customer Managed Relationship" (or CMR instead of CRM) has emerged, where the customer manages the relationship with the company and controls his or her own data. The most popular industry view holds that customers should own their own personal profile and have access to all the information about themselves across all departments. Additionally, the CMR system should be designed around consumers' needs and desires. An example of this would be Vivendi Universal's Universal Music Mobile, launched in 2001 as one of the first CMR-oriented services offered. The Mobile provides an assortment of music-related multimedia services, and self-service, combined with the billing program, is a major feature of the service: it allows customers to activate multiple services and features online, view their usage, pay or pre-pay online, change service options online, modify their contract, or change billing details themselves. Vivendi Universal took a relatively early lead in letting its customers define how they wanted to communicate with the company, not the opposite. In this kind of relationship, consumers feel a sense of empowerment and control (which equals a feeling of trust and security) over their personal information. IBM Chief Privacy Officer Harriet Pearson refers to this kind of relationship as a "trusted balance" – a willingness to communicate and put into effect a concise set of privacy rules.[19] Also crucial is the fact that this arrangement is about selling an emotion or an experience, the same way that Nike sells an athletic lifestyle. The key to success in a CMR is thus allowing customers not only to feel in control of their choices as consumers, but also to be able to monitor and manage their own personal information if they participate in a CMR by choice, it is a sure sign they trust the company.

But despite growing privacy protocols, people are increasingly wary about disclosing unnecessary information about themselves. If customers think information requests are superfluous, intrusive or unnecessary, they may lie or abandon the process. "Relationships" that are not founded upon genuine dialogue, reciprocity and negotiation can flounder, such as when privacy promises are obscure and written in vague non-committal legalese (and subject to change at any time). Even worse is when the defaults are invasive or perceived to be disrespectful of customers' wishes, such as when a website's registration default is "optin."

18 Seth Godin, *Permission Marketing* (New York: Simon & Schuster, 1999).

19 Aiden Barr, "Privacy is Good for Business," *306.ibm.com*, 1999 **http://www-306.ibm.com/e-business/ondemand/us/customerloyalty/harriet_pearson_interview.shtml**

As far as youth are concerned, it would be in error to dismiss them as apathetic when it comes to concern over privacy. The 2004 Harris Interactive survey of youth found that many of them do in fact care. The degree of concern with "privacy being invaded online" varied by age, with the lowest being eight- to nine-year-olds at 25 per cent, and the highest being 18 to 21-year-olds at over 50 per cent.[20]

"Privacy hawks," as dubbed by Ben Charny, engage in "privacy self-defense" by employing guerilla tactics to protect their personal information.[21] The Pew Charitable Trust describes these cyber renegades as most likely male, with over a third between the ages of 18 to 29, who have been online for three or more years and make up 25 per cent of the Internet population. While by no means a homogeneous group, they hold one common belief: their personal information will ultimately be exploited and "privacy policies" are not always to be trusted. Therefore, they feel that falsifying their personal information is necessary out of self-defence.

In terms of specific tactics to maintain personal privacy, the most common is to simply lie. Those who are aware of a website's limitations understand that they can, with impunity, provide completely false information on a registration form to qualify for access. For some it is even a game of sorts: one can declare oneself as a CEO who lives in Beverly Hills and makes between $0 and $15,000 per annum. Indeed, it would not be surprising to find that the most common Zip code entered on website registration forms is 90210, from the popular 1990s television show, or that Bill Gates has registered with MSN more than one hundred times.

To date there has been only a handful of in-depth studies conducted on individuals who lie when registering online. In 2000 it was found that 20 per cent to 30 per cent of registrants lied (with teenagers being the highest scoring age demographic), but this is considered a conservative estimate.[22] the main reasons cited for lying included distrust over how personal information would be used, avoiding junk mail, and a desire to remain anonymous. This desire for continued privacy is something to take into account when considering the ROI of advertising and marketing budgets.

Another growing method of consumer self-defense is having a secondary, or "disposable," email address. Anyone can log onto Hotmail in five minutes and create an email account based entirely on false information. A 2004 Harris Interactive survey found that youth aged 10 to 21 had an average of two to three email addresses.[23] Some websites such as *Dodgeit*, *Mailinator*, *Spamgourmet* and *Spambob* now even

20 Harris Interactive, *Youth Pulse*, June/July 2004, p. 64.

21 Ben Charny, "Protect your Internet privacy… by lying," *ZDNET News*, August 21, 2000 **http://news.zdnet.com/ 2100-9595_22-523232.html**

22 The Pew Internet and American Life Project, "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," August 2000 **http://www.pewinternet.org/PPF/r/19/ report_display.asp**

23 Harris Interactive, *Youth Pulse*, June/July 2004, p. 53.

offer free disposable email accounts. In the Spring of 2005, *Spamgourmet.com* reported that it had almost 90,000 subscribers with nearly 1.5 million disposable email addresses. The Pew Internet and American Life Project found that 20 per cent of persons who use the Internet have used disposable email addresses, while the number of teenagers who did the same was as high as 56 per cent. It should also be noted that disposable email addresses are not only used to avoid junk mail; they are also a safe vehicle for entering contests, or registering for free gifts or rebates (the address is disposed of once the contest is over, or the gift or rebate has been received).

Privacy hawks and anyone else who wants to remain anonymous online have received help from advances in Internet technology. Mozilla Firefox is an Internet browser that allows for anonymous surfing. Most browsers now include toolbars equipped with a function that blocks pop-up ads and cookies. And almost all email services now come with "block sender" and "junk mail" options that automatically vet email. There is also a host of commercial and free software programs available, such as Ad-Aware and BetaSpyware, that provide real-time defense against unwanted intrusion from hackers and marketers, and other forms of surreptitious data gathering. In fact, these features are becoming so commonplace that disposable email addresses may soon be redundant, because even if unwanted contact is made, a simple click of a button can ban a marketer or advertiser indefinitely. As of April 2005, Ipsos-Reid reported that 77 per cent of Canadians already use such filters while online.[24] In 2003, the Pew Internet and American Life Project found that 37 per cent of Americans used filters while online.[25] In 2005, the number of families with teenagers in the U.S. that used online filters at home was found to be 54 per cent, up from 41 per cent in 2000.[26]

Self-defence of personal privacy is a growing movement, no longer limited to the actions of a few privacy hawks. People are becoming more and more organized; they are becoming connected in their common goal. Strategies, techniques, and tactics in defence of one's privacy are now becoming widespread topics of conversation in chat rooms and on blogs.

Microsoft's small business website offers a top-10 list for successful permission based email marketing, with number 10 being always remember the network effect. "Bad news travels much faster than good on the Internet. An angry online customer can broadcast his ire to millions by creating an 'I hate [your company]' website, emailing an account of their experience to friends, posting it on message boards and other ways. Remember, in this economy the customer is in

24 Ipsos-Reid, "Canadians Winning the War Against Spam," *Ipsos*, March 10, 2005 **http://www.ipsos-na.com/news/pressrelease. cfm?id=2594**

25 Pew Internet and American Life Project, *Spam Survey*, June 10-24, 2003, p. 20.

26 Pew Internet and American Life Project, *Protecting Teens Online*, March 17, 2005, p. 8.

control."[27] For further reading on anti-company websites, Forbes.com has published an online article featuring the top corporate "hate" websites.[28]

3.3 Possible solutions

Strong, clear and overt privacy commitments, honored over time, demonstrate respect for the customer and foster trust and loyalty.

Customer knowledge and consent should be prerequisites for all marketing activities. The customer should be given every opportunity to become a participant in the marketing process, and to provide feedback and direction. New technologies make it possible for organizations to give their customers direct access to all data held on them, as well as other self-serve options.

Trust and brand are easily eroded when privacy commitments are not perceived to be honored, or when the client is denied meaningful opportunities to be a participant in the "relationship." Let CRM morph into CMR!

When it comes to personal information, not sharing is caring. Your customers will thank you. Successful companies need to take a long-term strategic view of value of their customer data and resist the temptation to share it or sell it to third parties without their customers' consent.

Conversely, people will not lie when they feel there is a trusted connection between themselves and a company. They will almost invariably give their personal details if they think a relationship with a particular company is going to benefit them, even if all they want is to stay informed of the latest trends on products and services of interest. And isn't that precisely what you want to pitch to them? Find out what your customers want and give it to them they will keep coming back for more. But give them what they **do not** want and you will drive them away. You decide.

Your privacy mantra should be, "Always ask, never assume."

4.0 Information Liquidity

4.1 Context

An ONE aggregates data from disparate third party sources to create business intelligence that, in turn, may overlap with personal information. Many public databases contain private information that firms can easily access. How can privacy be protected?

27 Derek Scruggs, "10 rules for successful permission-based e-mail marketing," Microsoft.com/small business, April, 2005.

28 Charles Wolrich, "Top Corporate Hate Web Sites," Forbes.com, March 8, 2005.

4.2 Privacy concerns: bad data, bad decisions

"Search, don't sort" is Google's motto and advice to customers. This advice is particularly apt at a time when technology provides individuals and firms with the ability to instantly find, aggregate and distill a virtually unlimited quantity of information for novel uses and competitive purposes.

Taking advantage of this new wealth of data, a new and rapidly growing industry has arisen to collect, analyze, and sell aggregated personal information and profiles. The types of companies that do this are varied, such as TransUnion and Experian, which are credit bureaus to LexisNexis, and most notably ChoicePoint, which is described as a data miner and aggregator. By far, ChoicePoint is the largest data aggregator on the market, with billions of public records in its database.[29] With data that includes motor vehicle registrations, license and deed transfers, military records, names, addresses and SSNs, ChoicePoint routinely sells dossiers to police, lawyers, reporters, private investigators and even to the U.S. Department of Homeland Security.

The direct marketing industry has been transformed and spurred on to new heights by the online environment, where all manner of technologies are being deployed to collect highly granular personal information that is then combined with data available elsewhere and used to profile and predict behaviour. Examples of these technologies include use of "cookies," "Web bugs," and other electronic tools and agents that track online activities.

Attempts to consolidate information is not always successful, however: for instance, online advertising giant DoubleClick's attempt in 1999 to purchase Abacus Direct for $1 billion in order to merge data on Net surfing habits from the five billion ads DoubleClick served per week and the two billion personally identifiable consumer catalog transactions recorded by Abacus was vigorously opposed by privacy advocates and consumers on privacy grounds, prompting a three-year investigation by the FTC. The deal ultimately failed.

Personal consumer information is incredibly valuable to corporations: when Air Canada fell into bankruptcy proceedings, the airline sold off its information assets, which consisted of millions of profiles of Aeroplan members from its popular loyalty program, for nearly CAN $1 billion about three times the market capitalization of the company's airline fleet.

So lucrative is the information profiling industry that online marketers have formed numerous lobby groups and associations such as Network Advertising Initiative (NAI) and Online Privacy Alliance (OPA) in order to help shape the evolution of new laws and regulations that could have a direct impact on their business models.

29 Bob Sullivan, "Database giant gives access to fake firms," MSNBC, February 14, 2005 **http://msnbc.msn.com/id/6969799**

The marketplace for personal information is estimated to be in the tens of billions of dollars per year in the U.S. alone, with businesses as the main customers. In the past six months, several new books documenting the extent of the information aggregation and profiling industry have hit the market. Among the best are *The Digital Person: Technology and Privacy in the Digital Age*,[30] by Daniel Solove, and *No Place to Hide*, by Robert O'Harrow, Jr.[31]

Personal information is collected and sold to firms for a fast growing variety of purposes. Detailed dossiers on individuals are bought and sold like any commodity in a vast and growing "grey market" in order to carry out background checks, to authenticate people, credentials, and claims, to evaluate individual risk, to generate client profiles and make behaviour predictions, to establish metrics, for billing purposes, and for a wide range of "research" purposes, such as marketing and national security. Such information is routinely used by business to make decisions affecting individuals, such as whether or not to hire or promote them, or to grant them credit or insurance, and in general to establish the terms of a company's relationship with an individual.

The availability and use of detailed dossiers on individuals, and the derived profiles or scores, is seen as beneficial to individuals and to society because it helps detect and deter fraud (e.g., in the form of employment background checks); it helps lower transactions costs (e.g., the "miracle of instant credit"); and it enables better servicing of customer needs (e.g., by providing customer profiles). The general goal behind tapping huge database grids is to make more informed, smarter decisions.

Unfortunately, too much personal information liquidity and automated processing can be a liability. The history of privacy in the 20th century has shown that the abuse of personal information collection often provokes public outcries, backlashes, and new regulations and liabilities for organizations that act as data custodians especially when individuals are negatively affected as a result.

We may in fact be witnessing a "perfect privacy storm" right now in the wake of an endless series of large scale privacy and security breaches reported almost daily in the news. Given the ever increasing incidence of identity theft, the public and lawmakers are beginning to demand that businesses begin to shoulder their fair share of responsibility for the many negative effects and costs that fall upon innocent third parties as a result of data mismanagement. New federal laws and regulations are widely expected within the year that will curb excessive business practices involving personal information collection, use and disclosure, and to arm individuals with better knowledge and greater rights of access and redress vis-à-vis those businesses that would collect and use their personal information.

30 Daniel J. Solove, *The Digital Person* (New York: New York University Press, 2004).

31 Robert O'Harrow Jr., *No Place To Hide*, New York, Simon & Schuster, 2005.

As noted earlier, the excesses of the yellow press in the early 20th century spawned the concept of the right to privacy, and led to a variety of legal restrictions and tort remedies for affected individuals. Similarly, abuses of centralized state dossiers and financial credit reports led to the waves of law, regulation, and litigation intended to curb the activity and provide various rights to individuals. Today, similar concerns about the extent and accuracy of personal data contained in blacklists, especially those shared with and used by governments, are the subject of considerable public debate.

Moreover, high-profile stalking and murders (e.g., Rebecca Schaeffer, Amy Boyer) that were facilitated by access to sensitive personal information led to new restrictions and liabilities on the use and disclosure of sensitive personal information. A desire to protect children led to other controls on information about individuals under the age of 13. The negative effects and costs of spam, telemarketing and spyware are also provoking new controls. Most recently, the ChoicePoint data breach has focused the regulatory spotlight on the practices and liabilities of large "infomediaries" who collect and sell personal information. In February 2005, it was discovered by an internal employee of ChoicePoint that identity thieves, in a plot twist taken from a Hollywood movie, were creating false identities to establish accounts with ChoicePoint and then using those accounts to commit identity theft. The employee became suspicious when he noticed that applications from some businesses were coming from a nearby Kinko's. ChoicePoint reacted by notifying close to 200,000 persons, as required by California law, that their personal information may have been compromised. However, the Los Angeles police department believes that as many as 500,000 persons may have been affected.[32] As of April 2005, there are 39 bills (pending in 19 states)[33] that are modeled after California's *SB1386*, which is known for its clause requiring that persons be notified when their personal information has been breached.

There is growing sentiment among lawmakers to place more accountability and liability on those organizations that have used personal information in irresponsible ways. The FTC has shown a willingness to investigate firms that do not live up to their privacy promises and who otherwise engage in unfair and deceptive trade practices involving the use of personal information.

Common privacy issues and liabilities include the following:

- **Failing to inform or seek the permission of the customer to obtain personal information from other sources**, then collating with data provided directly by the customer.

32 Our Georgia History, *ChoicePoint Scandal*, April 2005
http://www.ourgeorgiahistory.com/chronpop/1000072

33 Emily Hackett, *The Problem of Data Security*, Internet Alliance, April 25, 2005.

- **Failing to get explicit informed consent from the customer** to share his or her personal information with third parties and other members of the intelligence network.
- **Obtaining and using old or inaccurate data obtained from third parties**. If incorrect data are used to make decisions affecting an individual, the ONE must be prepared to justify its decision making and face the consequences when incorrect.
- **Automated processing and decision-making can also lead to discriminatory treatment of customers, with no recourse for action**. For example, customers with "undesirable" phone numbers will wait long service times while "desirable" phone numbers get through to customer service right way. Who is accountable when customers are denied service because they have erroneously been placed on a secret networked blacklist?

Networked intelligence and automated decision making tools can be of a great service to the public, but a very real danger exists in that incorrect or outdated personal data can propagate throughout these systems. Again, accountability and responsibility are often diluted when personal data, and in this case, incorrect assessments, are available everywhere, instantaneously.

Companies that rely on other sources for their information and decision making needs must understand that they may nonetheless incur liability and penalties for failing to take responsibility for their actions.

4.3 Possible solutions

As the ONE increasingly taps into the grid of available personal data, it must ensure that this information is

- Legally acquired, used or shared;
- Sufficiently accurate for the identified purposes;
- Appropriate and proportional for those purposes;
- Used in a transparent and defensible manner; and
- Available for access and correction by the individual.

Organizations must be clear and up front about the nature and extent of their information activities involving third parties. For example, a considerable amount of sensitive personal information may be acquired from various sources in order to screen potential employees. The routine sharing and use of information among a large number of affiliates, partners, and subcontractors in the corporate "family" should be made explicit.

Firms should also always explain and justify the use of automated decision making tools. Wherever possible, they should seek the informed consent of their customers, and be prepared to provide access and correction to all data about an individual (not just information supplied directly by the individual), along with an explanation of specific data items. If consent is withdrawn, then the request should be honored throughout the information supply chain, such as agreeing to remove an individual from a mailing list, for example. Increasingly, firms are required in many jurisdictions to provide, on demand, not just access but an account of all uses and disclosures of customer information.

Successful ONEs should strive to maintain and share only the most limited and accurate data or assessments about their customers with others, and should have in place mechanisms to deal with exceptions, corrections and other remedial processes. They should also take appropriate steps to ensure, and to demonstrate, that the networked sources from which they receive and supply customer data are reputable and trustworthy.

5.0 Technology

5.1 Context

Remarkable advances in information and communication technologies make it possible now, on a cost effective scale never seen before, to collect, store, process, and share vast amounts of highly granular personal data. This data become our digital shadows, proxies for the real thing, upon which organizations and governments alike will assess and make decisions both for and about us.

5.2 Privacy concerns:

Over collection and under disclosure
(the law of unintended consequences)
Just because technology lets you do something, should you do it?

It is generally accepted that the development and adoption of new technologies races far ahead of our ability to understand their consequences, let alone control them. Perhaps this is a good thing, since it gives lead time for experimentation and innovation, and at times, unintended consequences.

Organizations that are early developers or adopters of innovative information communication technology (ICT) often stand to gain an advantage over their competitors, especially in new areas and industries. Being an industry pacesetter, however, sometimes comes at the cost of working in grey areas of regulation, and incurring hard to quantify privacy risks and public backlashes. All of the major ICT innovators of the past decade from Microsoft to Intel, Amazon, Google, eBay, and ChoicePoint have attracted their fair share of attention and criticism, not to mention regulatory scrutiny.

Sometimes companies can get too far ahead of the curve and trigger negative public reactions, either because the activity generates negative unintended consequences, or because it is offensive, or susceptible to exaggerated public fears. Privacy concerns are often dormant until shaken by a confluence of circumstances and developments.

Indeed, it is rarely technology itself that constitutes the privacy risk but, rather, the manner in which it is used by human decision makers. For example, where some see utopian efficiencies, conveniences, and personalization in the deployment of RFID applications, others may see dystopian architectures of surveillance and control.

Consider the case of German retailer Metro, which in 2003 began an RFID trial in customer "payback" loyalty cards. Metro did not tell its customers what it was doing or why. When the RFID trial was discovered by accident, it generated a public backlash, resulting in international boycotts that continue to this day.[34] The company's clumsy denials and public relations handling of the incident did little to assuage privacy concerns. Although no law was broken, trust in the large retail store operator was shattered. Metro eventually recalled the loyalty cards and replaced them with non-RFID versions, but the damage was done.

Compare this experience to that of ExxonMobil who, in 1997, developed the wireless payment application known as SpeedPass. Using RFID key fobs, six million consumers have utilized the payment option at 7,500 SpeedPass-enabled locations. The technology has been a great success, enabling Exxon to increase its customer satisfaction, retention rate, and market share.

Unlike Metro, Exxon's initiative was above-board customers enrolled for the tags, clearly giving their informed consent. Secondly, the technology provided clear and demonstrable benefits to all customers allowing fast, convenient, secure payment at the pump obviated the need to produce and use a credit or debit card.

Right now, Metro and several other global manufacturers and retailers contemplating RFID deployment are busy contending with organized worldwide consumer boycotts and considerable attention from a broad range of government and regulatory agencies, privacy advocates, and consumer interest groups.[35]

ONE growth and success will be predicated on a virtually insatiable appetite for information. New technologies allow and even encourage the collection of evermore

34 "Customers say: We aren't your guinea pigs," Foebud.org **http://www.foebud.org/rfid/pressemitteilung/en**

35 See, for example, Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology (January 1, 2005). International Conference of Data Protection & Privacy Commissioners, Resolution on Radio-Frequency Identification (November 20, 2003), FTC RFID Report (March 2005), and RFID Position Statement of Consumer Privacy and Civil Liberties Organizations (November 2003) at: **http://www.privacyrights.org/ ar/RFIDposition.htm**

fine grained data about customers and their transactions that are then analyzed for insights and competitive advantage. What choices will firms make in the responsible use and deployment of technologies that can manipulate this data?

5.3 Digital footprints

Every time a cellphone is used, a website is visited, or a debit card swiped, a digital footprint is created. That digital footprint, pertaining to an identifiable consumer, is used by a company, or companies, to construct a profile of patterns and preferences which can then be used for promotion and marketing purposes.

These digital footprints are very valuable to marketing and advertising departments, and will become even more valuable in the future as tracking technologies improve and proliferate. Internet usage has become one of the most closely tracked activities in the last decade. It has even given birth to an entirely new industry of specialized customer tracking software.

In October 1999, an independent security analyst discovered that RealNetworks had assigned a global unique identification number (GUID) to each of its users who registered with its popular Real Jukebox software, and was using that number to track music listening patterns.

Although RealNetworks claimed that the data were only used for aggregation purposes, GUID technology potentially enabled RealNetworks to create personal profiles that included everything from listening preferences to credit card numbers. This type of data collection was in direct contradiction to RealNetworks' stated privacy policy. The company subsequently amended its privacy statement to alert customers to the types of information that might be gathered, and released a software patch for users to block transmission of their personal information.[36] Angry customers, however, initiated two lawsuits against the company.[37]

Since then, consumer concerns and fears regarding clandestine online surveillance and data collection have continued to grow, and trust is continuously being eroded. Digital rights management technologies, for example, track and control online media usage with fine grained precision. Similarly, spyware small software applications that surreptitiously install themselves on one's computer to track user activities has become a problem of epidemic proportions. U.S. lawmakers are wrestling with the spyware problem through appropriate legislative responses. In an effort to gather increasingly detailed information about online customers and generate metrics for marketing initiatives, many companies routinely insert "Web

36 Courtney Macavinta, "RealNetworks changes privacy policy under scrutiny," C/Net, November 1, 1999 **http://news.com.com/RealNetworks+changes+privacy+policy+under+scrutiny/2100-1040_3-232238.html**

37 Courtney Macavinta, "RealNetworks faced with second privacy suit," C/Net, November 10, 1999 **http://news.com. com/2100-1001-232766.html?legacy=cnet&tag=st.cn.1**

bugs" in their marketing email messages that report back when and how often the message was viewed, by whom, and what actions or links were followed. Very few people are aware of this now common online marketing technique; it is ripe for a privacy backlash or strong privacy self-defence techniques.

In sum, the overzealous or irresponsible deployment of invasive information and communication technologies can undermine the credibility of privacy promises and, in some instances, trigger strong consumer and legislative responses.

5.4 Possible solutions

The ONE must carefully consider the legal, public relations and economic risks of adopting any technology enabled data collection strategy.

To start, it is important to recognize that much of the information that is collected is, in fact, personal in nature, meaning that it may lead to identifiability. Even if the information itself, such as a computer IP address, software unique ID, or shopper's card movements in a store is not personally identifiable per se, what matters is whether the data can be linked to an individual. In this context, firms should recognize and address the possibility that, if they can collect this data, others may be able to do so too. For example, an RFID tag embedded in a loyalty card could also be read by competitors.

It is important to limit collection to what is strictly necessary. Too often firms collect data simply because they can or because it has *potential* value.

It is very important to have clear privacy policies that are brought to the attention of the customer at the time of data collection. Firms should be very careful not to assume they know their customers' expectations and that "implied consent" has been given. If there are residual privacy and security risks, these should be noted and addressed.

Successful companies will always offer meaningful choices and controls to consumers, and invite their participation and feedback. For example, customers should be able to disable or control features or easily decline or uninstall unwanted software. And new technological deployments may be more readily accepted by consumers if there are clear, direct and demonstrable benefits, rather than general promises of improved administrative efficiency, personalized service, better choices and special offers.

Firms should make, and keep, their privacy promises. Doing so establishes credibility and trust over time, and helps to build the customer goodwill that will be necessary in the event of a privacy breach.

Lastly, firms should have a realistic crisis-management plan. The successful ONE lives on the "bleeding edge" and must be ready for hard to quantify risks. Too often, ICTs are adopted and deployed without an adequate appreciation of the possibility of a privacy breach and the ensuing backlash.

6.0 Conclusions

The overarching theme relating to privacy in response to the Open Networked Enterprise is *accountability*. The successful ONE of the future may very well be global, decentralized, open, borderless, modular, flexible, empowering and so forth characteristics that seem to reflect the Internet itself but these same qualities challenge the responsible management of vast storehouses of customer information necessary for the ONE to succeed.

Remember to keep your focus on the customer. Taking a customer centric view of information will highlight the distinction between person ally identifiable information versus non person al information. The difference between how firms treat each is critical.

Dr. Ann Cavoukian is Ontario's first Information and Privacy Commissioner to be reappointed for a second term. Initially appointed in 1997, her role in overseeing the operations of the freedom of information and privacy laws in Canada's most populous province was extended to 2009. Like the provincial auditor, she serves as an officer of the legislature, independent of the government of the day.

She is recognized as one of the leading privacy experts in the world and is frequently called upon to speak at major forums around the globe. Her published works include a book entitled *Who Knows: Safeguarding Your Privacy in a Networked World* (McGraw-Hill, 1997), written with Don Tapscott, and, most recently, *The Privacy Payoff* (McGraw-Hill Ryerson, 2002), in which she and the book's co-author, journalist Tyler Hamilton, address how successful businesses build customer trust.

Dr. Cavoukian joined the Office of the Information and Privacy Commissioner in 1987, during its startup phase, as its first Director of Compliance. In 1990, she was appointed Assistant Commissioner. Prior to joining the IPC, she headed the Research Services Branch for the provincial Attorney General. She received her M.A. and Ph.D. in Psychology from the University of Toronto, where she specialized in criminology and law, and lectured on psychology and the criminal justice system.