Abandon Zero-Sum, Simplistic either/or Solutions –

Positive-Sum is Paramount: Achieving Public Safety *and* Privacy

November 2012

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

Information and Privacy Commissioner,
Ontario, Canada

TABLE OF CONTENTS

Foreword

Too often, the state's traditional model for protecting privacy and safeguarding information has led to a zero-sum game – an increase in privacy is often seen as leading to less security. Of course, protecting public safety and a nation's security are necessary and important functions of a civilized society. Government and law enforcement agencies frequently require personal information for national security and to protect public safety. However, privacy, liberty and freedom of choice are also essential to the functioning of prosperous and democratic free societies. Technological advances in the collection and processing of information over the last few decades have positioned these fundamental human rights as vital to the health, well-being and freedom of individuals. Abuses of personal information can cause untold harm, wasted resources, and generally lead to the detriment of freedom and liberty. For example, a society of individuals perpetually anxious about "big brother" surveillance, misuses of their information, or unwarranted search and seizure, cannot function at optimum levels.

Following the attacks of 9/11, I issued our Office's position, saying: "Public safety is paramount – but balanced against privacy."[1] Today, if I could change one thing, it would be the notion of "balance" in that statement. In this paper, as reflected in the title "Abandon Zero-Sum, Simplistic either/or Solutions – Positive-Sum is Paramount: Achieving Public Safety *and* Privacy," we have shifted our focus on the importance of taking a positive-sum (win/win) approach, instead of a zero-sum (win/lose) approach in tackling public safety issues. By adopting such a viewpoint, one can easily see that people can have multiple interests that may indeed co-exist, including areas such as law enforcement, national security and human rights. This is the perspective offered by *Privacy by Design*, which was recently cited by the European Counter Terrorism Coordinator in a report presented to EU Ministers of the Interior.[2] For some time in Europe, there have been calls to bridge the gap between data protection and law enforcement's access to personal information.[3] I hope the information in this paper will contribute to the discussion that our European colleagues and other interested parties internationally are now undertaking. Protecting privacy need not stand in the way of public safety.[4] Providing for public safety must not undermine privacy – let us strive to preserve both of these vital interests.

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

1 Information and Privacy Commissioner of Ontario. (September 21, 2001). Public safety is paramount – but balanced against privacy.

2 EU Counter-Terrorism Coordinator. (2012). *9990/12 EU Counter-Terrorism Strategy - Discussion paper.*

3 The Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group"). "Freedom, Security, Privacy – European Home Affairs in an Open World." 2008, p. 50.

4 For example, my Office has issued guidance on the disclosure of information in emergency or other urgent circumstances. See, Office of the Information and Privacy Commissioner of Ontario. "Fact Sheet #7 - Disclosure of Information Permitted in Emergency or Other Urgent Circumstances." (2005).

Introduction

There is great interest in how the Office of the Information and Privacy Commissioner of Ontario, Canada (IPC) has approached privacy and public safety issues, by bringing them together in a positive-sum manner. In this paper, the IPC shares its approach to applying *Privacy by Design* (*PbD*) which is relevant in the context of public safety and law enforcement, including the application of *PbD* to surveillance programs and the use of associated technologies. The hallmarks of this approach include an emphasis on communication, understanding divergent points of view, and focusing on protecting, preserving and enhancing individuals' privacy.

In recognizing the importance of public safety and law enforcement, the Commissioner has emphasized that multiple interests in this area can co-exist. An essential part of this approach is the concept of *PbD*. In addition to describing this concept, examples will be provided of the IPC's approach to its implementation in the area of video surveillance, biometric technology, and advanced data analytics. Implementing *PbD* means working proactively with law enforcement in order to maximize privacy protections within public safety programs, for example, by the use of cutting edge technology. It also leads to improved privacy governance.

The paper also offers examples of when a failure to adopt a *PbD* approach has led to an erosion of public confidence in law enforcement initiatives, for example in the mandatory collection of personal information in the context of second-hand goods and telecommunications. These "Privacy by Disaster" scenarios remind us that it is critical to bake privacy into a program, policy, or legislative initiative right from the start.

Consultation, Co-operation, Collaboration (3 Cs) and How They Intersect with *Privacy by Design*

Since January 1, 1988, IPC has acted independently of government to uphold and promote open government and the protection of personal privacy in Ontario, Canada. The Commissioner is appointed by and reports to the Legislative Assembly of Ontario and remains independent of the government of the day to ensure impartiality. Under statutory mandate, the IPC is responsible for investigating complaints, ensuring that organizations comply with the provisions of Ontario's access and privacy Acts, educating the public, conducting research on emerging access and privacy issues, and providing advice and comments on proposed government legislation and programs.[5]

The Commissioner carries out the Office's mandate with three key words in mind — consultation, co-operation, and collaboration. In this regard, the IPC keeps

5 The Commissioner oversees the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) and the *Personal Health Information Protection Act* (*PHIPA*).

the lines of communication open with the institutions it oversees. Co-operation is emphasized over confrontation to resolve complaints. Collaboration is sought proactively by seeking partnerships to find joint solutions to emerging privacy and access issues. Emphasizing communication, consultation and understanding assists in facilitating a focus on the privacy rights of the individual and the achievement of user-centric results.

The IPC's approach has, for example, led to positive results in the area of privacy breaches. Public institutions covered under Ontario's two freedom of information and privacy protection Acts (*FIPPA* and *MFIPPA*) voluntarily self-report data breaches to the IPC despite the Acts having no breach notification requirements. Hundreds of data breaches have been reported voluntarily in this way which has allowed the IPC to play a vital role at critical breach management stages.[6]

Taking a proactive problem-solving approach lies at the heart of *PbD*. *PbD* makes privacy a foundational requirement, anticipating and preventing privacy-invasive events before they happen. *PbD* was developed back in the 1990s, when the notion of embedding privacy into the design of technology was far less popular. At that time, taking a strong regulatory approach was the preferred course of action. With advanced digitization of data, networked infrastructure, social networking, etc., it is now clear that the future of privacy cannot be assured solely by compliance with regulatory frameworks.[7] Rather, privacy assurance must ideally become an organization's default mode of operation over three areas of application: (1) information technology; (2) accountable business practices; and (3) physical design and networked infrastructures.

Based on a set of 7 Foundational Principles, *PbD* offers a flexible and technology-neutral vehicle for engaging with privacy issues, and for resolving them in ways

6 Cavoukian, Ann. "A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight." In *The Eighth Workshop on the Economics of Information Security*. University College, London, England, 2009.

7 This perspective is acknowledged internationally. Privacy leaders from around the world have endorsed the importance of *PbD*. At the 32nd International Conference of Data Protection and Privacy Commissioners in 2010, *PbD* was unanimously passed and adopted as an International framework for protecting privacy. International Conference of Data Protection and Privacy Commissioners (2010). *Privacy by Design* Resolution, adopted at Jerusalem, Israel, October 27-29, 2010. At http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf.

that support multiple outcomes in a positive-sum, win-win scenario as opposed to a zero-sum, either/or scenario. The Principles are as follows:

The 7 Foundational Principles of *Privacy by Design*

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

Privacy by Design - The 7 Foundational Principles: *http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf*

The aim of this proactive approach is to reduce the risk of privacy harm from arising in the first place, ideally preventing it entirely, while preserving a commitment to functionality. Privacy is often viewed as an individual right that must be sacrificed in order to attain other socially desirable, but competing goals. The right to privacy is often traded off to achieve national security, for example. However, it is our belief that the security model in current use must change from a zero-sum to a positive-sum paradigm, where both the need for privacy protection of personal information and the need for security can be satisfied. We also must ensure that any security measures undertaken are real and not illusory, meaning, they must be necessary and effective.

Unlike some critics, who see technology as necessarily eroding privacy, we have long taken the view that technology is inherently neutral. As much as it can be used to chip away at privacy, its support can also be enlisted to protect privacy.[8] In this way one can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive. This approach serves to minimize the unnecessary collection, use and disclosure of personal data, and to promote public confidence and trust in data governance.[9]

8 Cavoukian, Ann. *Privacy by Design ... Take the Challenge*. Office of the Information & Privacy Commissioner of Ontario, 2009.

9 Cavoukian, Ann. "Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum Not Zero-Sum." Office of the Information & Privacy Commissioner of Ontario, 2008.

Our Approach in Action

Video Surveillance and CCTV Cameras

There exists a broad range of perspectives regarding video surveillance. On one side of the spectrum, some civil society groups assert that public video surveillance systems threaten privacy, especially when used in combination with other technologies (e.g., data mining, GPS tracking, RFID, Internet, facial recognition). The concern is that, in combination, these technologies have a real potential to change the relationship between the citizen and the state. At the other side of the spectrum, various law enforcement and security officials assert the need for broad use of video surveillance as a key tool to deter criminals; support apprehension and investigation; increase perceptions of safety; promote commerce; and aid in prosecutions.[10]

At present, it is difficult to find unequivocal evidence that video surveillance deters or prevents crime. A more viable role for video surveillance may be as a source of evidence in the investigation and prosecution of crime associated with, for example, critical infrastructure. For example, video surveillance footage released to the public led to early identification of suspects and played an important role in their subsequent prosecution in the case of the Brixton nail bomber in 1999 and in the failed bombing of London's subway system on July 21, 2005. In Ontario, images collected from video surveillance cameras located in a hospital in Sudbury, Ontario, were highly instrumental in identifying and locating a woman who pleaded guilty to having kidnapped a newborn infant from the hospital. Images collected from the camera were also very helpful in the return of the infant to his family.[11]

The IPC created *Guidelines for the Use of Video Surveillance Cameras in Public Places* (*Guidelines*) to assist organizations in deciding whether the collection of personal information by means of a video surveillance system is lawful and justifiable as a policy choice, and if so, how privacy protective measures can be built into the system.[12] The *Guidelines* recommend that organizations take mitigating steps, e.g. encrypt wireless transmission to prevent viewing by unintended persons. The collection of personal information must also be kept to a strict minimum by, for example, limiting the number of cameras, limiting the time the cameras are recording, and considering early automatic overwriting of recorded images. Also, organizations are advised to ensure that reasonable safeguards are established to protect recorded images, appropriate to the sensitivity of the information. Importantly, there should be strong governance and accountability mechanisms. These include a comprehensive privacy policy for the program and detailed procedures relating to the video surveillance program. Organizations must be open

10 Information and Privacy Commissioner of Ontario. (2008). Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report MC07-68.

11 Ibid.

12 Information and Privacy Commissioner of Ontario. (2007). Guidelines for the Use of Video Surveillance Cameras in Public Places.

and transparent by consulting with relevant stakeholders in advance of initiating a surveillance program, and by using prominent signs to notify the public of video surveillance equipment locations and contact information. Also, evaluation and auditing of the surveillance program must be carried out regularly.

Acknowledging that in limited and specific circumstances video surveillance cameras may be appropriate to protect public safety, the IPC has worked collaboratively with law enforcement to apply the *Guidelines* to a number of initiatives. For example, one of Canada's largest police agencies, the Toronto Police Service, approached the IPC regarding a proposed program to conduct video surveillance in specific high-crime areas as an added tool for the reduction and detection of crime. The Police were already aware of the *Guidelines* and committed to apply them to the program (e.g., images for the video surveillance program should not be monitored from a central video surveillance system, are overridden automatically every 72 hours, and are not accessed unless an incident prompts an investigation).[13] The Toronto Police Service also applied the *Guidelines* to an in-car video surveillance program meant to reaffirm the commitment to professional and unbiased policing, enhance officer safety and improving the quality of evidence for police vehicles. The program was prompted from a recommendation by a Race Relations Joint Working Group following a series of media articles alleging racial profiling within the criminal justice system.[14]

These and other examples of working closely with law enforcement have led to praise for *PbD* from law enforcement. Chief of the Toronto Police Service, William Blair, has said that the IPC's method ensures "a positive-sum approach to the use of public space cameras in Toronto, one that enables the use of this additional tool to support policing while concurrently mitigating privacy concerns through technological and operational design."[15]

In the context of formal investigations into the use of video surveillance prompted by complaints, the IPC has also sought to understand and be responsive to the broad range of perspectives on video surveillance. After Privacy International, a U.K. based advocacy group, filed a privacy complaint with the IPC regarding the Toronto Transit Commission's (TTC) plans to expand video surveillance within the subway system, the Commissioner expanded her investigation to include a review of literature, as well as an examination of the role that privacy-enhancing technologies can play in mitigating the privacy-invasive nature of video surveillance cameras. The Commissioner concluded that the TTC's expansion of its video surveillance system, for the purposes of public safety and security, was in compliance with Ontario privacy laws. She also called on the TTC to undertake a number of specific steps to enhance privacy protection.[16]

13 Ibid.

14 Toronto Police Services Board, & Toronto Police Service. (2003). Report of the Board / Service Race Relations Joint Working Group.

15 Information and Privacy Commissioner of Ontario. (November 10, 2009). *SmartPrivacy for Smart Public Safety*. Presented at the Toronto Forum for Global Cities Conference, Toronto, Ontario.

16 Information and Privacy Commissioner of Ontario. (2008). Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report MC07-68.

The Commissioner's ultimate goal was to consider the issue of video surveillance broadly in the TTC report given the enormous public support for the use of video surveillance cameras in mass transit systems and by the law enforcement community. Despite the wide spectrum of views on video surveillance, one of the areas in which there is general agreement and acceptance of video surveillance is in the area of mass public transit. For example, the U.S. Department of Homeland Security held a workshop seeking input into best practices for states that receive funding for video surveillance installations that would assist the government in ensuring the protection of privacy and civil liberties.[17] The common view expressed in the workshop was that in light of the extensive areas involved (tunnels, platforms, stairways), the high numbers of passengers (especially during rush hours) and the around the clock operating hours of the system, the ability to deal with security issues could not feasibly be limited to increasing the number of security personnel. Consequently, the views of both privacy advocates and those in emergency management and law enforcement converged on the need for video surveillance in urban mass transit systems – all agreed that the use of video surveillance cameras in this context was justifiable.

Nevertheless, the Commissioner has said it is incumbent upon those who wish to deploy surveillance systems to be aware of and adopt privacy-enhancing technologies whenever possible, especially as they become commercially available. The TTC report describes research that has shown that it is possible to design surveillance systems in a manner that may successfully address issues of public safety while, at the same time, protecting the privacy of law-abiding citizens. As an example of the research being conducted into privacy-enhancing technologies, the Commissioner cited the work of researchers Karl Martin and Kostas Plataniotis at the University of Toronto, who used cryptographic techniques to develop a secure object-based coding approach.[18]

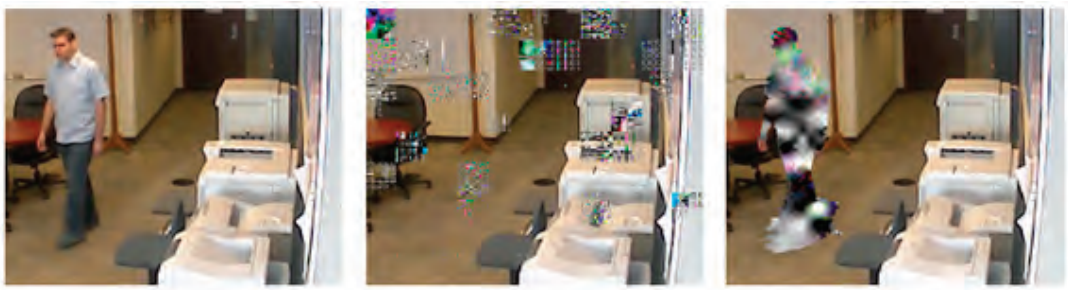

Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.

17 U.S. Department of Homeland Security. DHS Privacy Office Public Workshop CCTV: Developing Privacy Best Practices (December 17-18, 2007), http://www.dhs.gov/privacy-workshops#7 ; Information and Privacy Commissioner of Ontario. (2008). Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report MC07-68, p. 1.

18 This technology is now available commercially at www.bionym.com

The Use of Privacy-Protective Biometrics

Identification and authentication requirements are steadily increasing in both the online and off-line worlds. Both public and private sector entities assert a need to "know" who they are dealing with. Tokens used for the verification of identity, protection of information, and authorization to access premises or services may be 1) a password or shared secret (something you know), 2) an identity card (something you have), or 3) a biometric (something you are). In all of these cases, the details of the token are held by a third party whose function is to authorize and, at times, allow the transaction to proceed if the details of an individual's token match those stored in a database.

Biometric information is increasingly viewed as the ultimate form of authentication or identification, supplying the third and final element of proof of identity (described above). Accordingly, it is being applied in a variety of security applications. However, privacy advocates have long held that surveillance and biometric systems raise significant privacy concerns. As biometric uses and databases grow, so do concerns that the personal data collected will not be used in reasonable and accountable ways. The threat to privacy and human rights arises not simply from the identification that biometrics provide, but from ethical issues related to informational privacy rights that include potential data misuse, function creep, and linkage of databases via biometric templates, which make surveillance, profiling, and discrimination, often without the knowledge of the individual, all possible. Moreover, unlike passwords, biometric data are unique, permanent, and, therefore, irrevocable.[19] Since this particularly sensitive data may be transmitted across networks and stored in various databases can also be stolen, copied, or otherwise misused, the risks to the individual are very significant. For example, affected individuals may be exposed to biometric identity theft or fraud.

Biometric Encryption (BE) uses *PbD* to directly address the privacy and security concerns associated with biometric systems. BE is a process that securely binds a key to, or extracts a key from, a biometric, such that neither the key nor the biometric can be retrieved. The key is recreated only if the correct live biometric sample is presented on verification. In other words, the biometric serves as a decryption key. At the end of verification, the biometric sample is discarded once again. With BE, the user is always in control of his or her biometric — it is not stored (in either raw or template form) and therefore, cannot be compromised. Further, the original biometric cannot be recreated (ideally) from the information that has been stored — it is untraceable.

BE has been incorporated into watch list scenarios such as the Ontario Lottery and Gaming Corporation (OLG) self-exclusion program.[20] In the summer of 2007, the OLG approached the IPC to discuss the use of facial biometrics to enhance their ability to identify individuals entering gaming sites who had enrolled in

19 Cavoukian, A., Chibba, M., & Stoianov, A. (2012). Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment. *Review of Policy Research, 29*, 37–61.

20 Information and Privacy Commissioner of Ontario, & Tom Marinelli. (2010). Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept.

OLG's voluntary 'self-exclusion' program. Canadian casinos offer self-exclusion programs which allow individuals the opportunity to opt for a self-imposed ban from one or more gaming sites as part of their efforts to mitigate the harms associated with compulsive gambling. Enrollees in the OLG program who enter OLG gaming sites and are identified by security staff will be escorted from the premises and issued a trespass notice.

OLG's process of detecting self-excluded individuals was largely manual. Enrollees were voluntarily photographed and personal information about them was collected, at their request, to be used in subsequent identification. These photos and associated information were then distributed to OLG gaming sites where they were printed and stored in secure binders accessible by security personnel who, among other responsibilities, would undertake the arduous task of trying to match faces in the casino with photos in the binders. Such a process of manual facial recognition suffers many obvious challenges, due to the limits of staff (and human) capability. As there are thousands of self-identified problem gamblers enrolled in the program, OLG wanted to examine whether technological tools could aid them in more efficiently and effectively meeting their objectives for the self-exclusion program. An automated facial recognition system in combination with a watch list was thought to be an attractive tool to enhance and support the manual inspection process.

Although the program is entirely voluntary (opt-in), seeking to recognize only those individuals who have provided positive consent, the use of facial recognition technology by the OLG raised a number of privacy and security concerns.[21] Given their mutual interest in respecting the privacy of all casino patrons, the IPC and OLG agreed that the application of an emerging BE to a facial recognition system at an OLG casino would be an ideal "win-win" project. A collaborative team was formed consisting of OLG, IPC, members of the University of Toronto's Electrical and Computer Engineering Department, and a video surveillance/tracking and biometrics firm. The team researched and developed an innovative proof of concept to integrate a "Made in Ontario" BE algorithm developed by University of Toronto researchers Kostas Plataniotis and Karl Martin into a commercially-available facial recognition system. The end goal of this collaboration was to develop a technology that could function in a real-world environment, and would offer dramatically improved privacy protection over simple facial recognition, without compromising functionality, security or performance — the hallmarks of a positive-sum *PbD* application.

University of Toronto researchers studied a range of issues with regard to the application of BE to a facial recognition system, including image pre-processing, feature extraction, cryptography, error correcting, and key binding, among others. Results of their simulation testing showed that BE could, in theory, be effectively integrated into a watch list facial recognition system. Proof of concept testing allowed OLG, in collaboration with a vendor, University of Toronto and the IPC, to show that a facial recognition application with BE is viable for

21 See Cavoukian, A., Chibba, M., & Stoianov, A. (2012). Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment. *Review of Policy Research, 29*(1).

development and deployment in a casino environment. The system architecture was successfully created to integrate BE into a commercial facial recognition product while maintaining OLG's core requirements. This architecture treated BE as an important component in a multi-layered approach to privacy and security of the overall system. Live field test at Woodbine facilities resulted in a Correct Identification Rate (CIR) of 91 percent without BE, and 90 percent with BE, thus showing negligible accuracy impact. Also, BE reduced the False Acceptance Rate (FAR) by up to 50 percent – a huge improvement in accuracy and exceeding state-of-the-art for facial recognition. This resulted in a triple-win: privacy, security, and accuracy (unexpected) – all improved.

By the end of 2011, the system was successfully deployed and is fully operational in most of Ontario's 27 gaming sites. To the best of our knowledge, this is by far the largest installation of a BE system and the first ever application of BE in a watch list scenario. The overall identification accuracy of self-excluded people has already improved by more than one order of magnitude compared to the previous manual system.

Advanced Data Analytics

Historically, advanced data analytics have been used, among other things, to analyze large data sets to find patterns and build predictive models for decision-making. Companies use advanced analytics with data mining to optimize their customer relationships, and law enforcement agencies use advanced analytics to combat criminal activity from terrorism to tax evasion to identify theft. Naturally, these methods have their limits. For example, traditional data mining techniques to find patterns useful for counter-terrorism have yielded little value. While these efforts may be welcomed from a public safety perspective, they have significant ramifications for privacy. In his report on Government Data Mining, Professor Fred Cate, Director of the Center for applied Cybersecurity Research, cautions against the widespread appeal of data mining techniques, which have resulted in the misidentification of innocent individuals and the failure to catch the "bad guys."[22]

The term "Big Data technologies" describes a new generation of technologies and architectures designed to economically extract value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery, and/or analysis. For example, the use of Big Data analytics has allowed MoneyGram International to lower its incident of moneygram fraud by 72 percent. The technology is a context accumulation program owned by IBM and developed by IBM Entity Analytics chief scientist Jeff Jonas.[23]

The IPC and Jeff Jonas worked together on the paper *Privacy by Design in the Age of Big Data* to address how today's Big Data will provide the raw material

22 Cate, F. (2008). Government data mining: The need for a legal framework. *Harvard Civil Rights-Civil Liberties Law Review (CR-CL), 43*(2).

23 Rosenberg, D. (April 21, 2012). IBM Fellow Jeff Jonas on the evolution of Big Data, *CNET*.

for tomorrow's innovations in a privacy protective manner.[24] It describes Jeff Jonas' remarkable and ambitious journey to create a sensemaking style system. This new technology evaluates new data observations in relation to previous observations – much in the same way that one evaluates a jigsaw puzzle to locate its companion pieces on the table – and use this context-accumulating process to improve understanding about what is happening in real-time.

Whenever Big Data contains personally identifiable information, increased responsibility and care is required to manage this information. The bigger the pile of data, the greater the value – the value to legitimate business users as well as those with interests in its misuse. Jeff Jonas believes it is imperative that with game-changing advances in analytics one should step back and ponder design decisions that will enhance overall security and privacy. Over the first year of this project, while drafting and redrafting these blueprints, his team worked to embed properties that would enhance, rather than erode, the privacy and civil liberties of data subjects. To engineer for privacy, his team weighed performance consequences, default settings, and which *PbD* features should be so hard wired into the system that they literally cannot be disabled. Over the year that spanned the preliminary and detailed design, the team created a robust suite of baked-in *PbD* features.

Jeff Jonas and his team believe this sensemaking system has engineered more privacy and civil liberties-enhancing qualities than any predecessor. For example, the system is expected to more strongly favour false negatives thereby minimizing decisions that adversely affect innocent individuals. Thus, in the age of Big Data, we are strongly encouraging technologists engaged in the design and deployment of advanced analytics to embrace *PbD* as a way to deliver responsible innovation. In fact, the IPC envisions a future where technologists will increasingly be called upon to bake-in, from conception, more privacy features directly into their products and services.

Privacy by Disaster – What Happens When Privacy is not Built-In Proactively

When organizations have a "Privacy by Disaster" mindset, privacy protections are only built, or practices explained, after a significant incident or development. The fallout from Privacy by Disaster approaches can be damaging and very public. Consider the significant media and public scrutiny generated as a result of a study showing that Apple's iPhones, iPads and Google's Android phones record location information. This resulted in several companies appearing before a U.S. House of Representatives Committee Hearing having to explain their data collection and usage practices.[25]

24 Information and Privacy Commissioner of Ontario, & Jeff Jonas. (2012). *Privacy by Design* in the Age of Big Data.

25 Information and Privacy Commissioner of Ontario, & Kim Cameron. (2011). Wi-Fi Positioning Systems: Beware of Unintended Consequences.

Similar scenarios have occurred with the roll-out of smart meters, which are a component in updating aging electricity grids in North America, Europe and elsewhere. Smart meters measure electricity consumption on an hourly basis. As a result, analysis of consumption information could reveal information about behavioural patterns within the home. According to a 2010 Market Strategies International Study 79 percent of people knew little or nothing about the smart grid, and 76 percent did not know anything about smart meters.[26] As a result, consumers were wary, and at times, hostile regarding smart meters in some jurisdictions. For example, residents of Marin County, California, created a prominent road blockade to prevent PG&E trucks from going into their town to install smart meters.[27] In the Netherlands, similar concerns led the Dutch Minister of Economic Affairs to suspend smart meter deployment.[28] Concerns also led to a privacy investigation in the province of British Columbia, Canada.[29] By contrast, in Ontario, where *PbD* was built into the smart metering system from the outset,[30] there has not been the same concern on the part of the public.

Law enforcement's approach to access to personal information can raise significant concerns for the public and regulators, particularly if privacy is not addressed from the outset. It is acknowledged that there are two very important values at play regarding law enforcement access to personal information. Individuals should be free from government tracking unless necessary for public safety, and law enforcement should have sufficient access to personal information when it is necessary to protect public safety. Detailed next are examples where privacy was not incorporated at the beginning, which resulted in a high level of scrutiny from the IPC.

Second-Hand (Used) Goods

In 2007, and for the very first time, Commissioner Cavoukian invoked a provision in Ontario privacy law that allows her to order an institution to cease a collection practice and destroy a collection of personal information that contravene Ontario's public sector privacy statutes.[31] As a result, the City of Ottawa and the Ottawa Police were ordered to stop collecting extensive personal information from individuals selling used goods to second-hand goods stores. All personal information already collected also had to be securely destroyed. This cease and desist Order followed from an investigation into a privacy complaint the Commissioner received regarding a municipal bylaw that had required second-hand goods stores to collect extensive

26 Information and Privacy Commissioner of Ontario. (May 9, 2012). *Get Smart About Privacy on the Smart Grid – Embed Privacy, by Design.* Chartwell Smart Grid Webinar.

27 Ibid.

28 Information and Privacy Commissioner of Ontario. (2012). Smart Meters in Europe: *Privacy by Design* at its Best.

29 Office of the Information and Privacy Commissioner for British Columbia. (2011). Investigation Report F11-03.

30 See, for example, Information and Privacy Commissioner of Ontario, Hydro One, & Toronto Hydro Corporation. (2010). Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid.

31 Information and Privacy Commissioner of Ontario. (2007). Municipal Order MO-2225.

personal information from all customers seeking to sell their second-hand goods. In the Order, the Commissioner cites representations made by the Ottawa Police regarding Business Watch International (BWI), a company that developed software that used goods stores can use to send detailed personal information of sellers directly to BWI. The company maintained a large electronic database on behalf of the Ottawa Police that included more than a quarter-of-a-million used good transactions, involving more than 44,000 identifiable individuals.

The creation and maintenance of such a database constituted a grave infringement to the privacy rights of individuals. Under the bylaw, the police were not required to obtain a warrant or demonstrate any suspicion of wrongdoing in order to access this database. Meanwhile, every individual who sold an item to a second-hand goods store could become subject to scrutiny by the police, even though it was clear that the vast majority are innocent, law-abiding citizens who have committed no offence.

In an effort to provide assistance to all municipalities and police services in the province, the IPC also published a set of guidelines with respect to the regulation of used goods titled *Privacy Guidelines for Municipalities Regulating Businesses Dealing in Second-hand Goods*.[32] In this context, municipalities have been advised that, as a general rule, the collection of personal information of individuals must be necessary rather than merely helpful. Where the collection of personal information is found to be necessary, municipalities should conduct a privacy impact assessment with a view to minimizing the personal information collected. Second-hand goods consumers must be provided with a notice of the collection, and their information should not be disclosed to third parties such as police without specific justification.

"Surveillance by Design"

In 2011, Canadian federal surveillance bills were introduced in Parliament to require telecommunication service providers to build and maintain intercept capability into their networks. If passed in their original form, these bills would also provide the police with a much greater ability to access and track information, via the communications technologies that we now take for granted, including in some circumstances, without a warrant or any judicial oversight. In the Commissioner's view, this represents a looming system of "surveillance by design," that should concern us all in a free and democratic society.[33]

The Commissioner strongly urged the government to re-draft these bills, in recognition of the sensitivity of the Internet data being collected. Through open letters and newspaper articles, the Commissioner raised awareness about the

32 Information and Privacy Commissioner of Ontario. (2007). Privacy Guidelines for Municipalities Regulating Businesses Dealing in Second-hand Goods.

33 Cavoukian, A. (2011, December 14). Beware of 'Surveillance by Design', Op-Ed, *Financial Post*; Cavoukian, A. (2011). An Open Letter from Commissioner Cavoukian to Minister of Public Safety Vic Toews and Minister of Justice and Attorney General of Canada Rob Nicholson., http://www.ipc.on.ca/site_documents/2011-10-31-Letter-to-Ministers-Toews-and-Nicholson-Surveillance.htm

privacy issues with the government's proposed program.[34] In consideration of the gravity of the issue, the Commissioner held a symposium on January 27, 2012 on International Privacy Day called Beware of "Surveillance by Design:" The Threat of Looming "Lawful Access" Legislation.[35] For more information, visit www.realprivacy.ca.

Conclusions

As outlined, when *PbD* is not adopted, Privacy by Disaster can and does occur. This kind of miscue is not only regretable from a privacy perspective, but it also represents a disservice to laudable public safety goals. Moreover, it can result in intense scrutiny from the public, media, lawmakers, courts and regulators concerned about protecting personal privacy. Examples of these in Ontario include the police collecting and accessing personal information of individuals selling used goods to second-hand goods stores, and requiring the building and maintaining of "surveillance by design" in electronic communications. In these cases, despite having to critically examine these initiatives, the IPC nonetheless approached the issues with an emphasis on a high level of communication, cooperation and collaboration. As always, the aim is to understand and be responsive to all the perspectives involved by adopting the approaches described in this paper. This approach mirrors the proactive/preventative nature of *PbD* which is designed to address the risk of harm to individuals before privacy intrusions or breaches can take place. In this paper, the IPC has outlined examples of applying *PbD* in the area of video surveillance, biometrics, and data analytics. In these cases, the outcomes demonstrate that it is possible to bring together divergent views and to achieve public safety objectives, while at the same time, minimizing the impact on privacy.

Law enforcement officials have significant public safety-related duties. Privacy is not meant to stand in the way of the proper fulfilment of these responsibilities. At the same time, taking a zero-sum approach, where privacy is sacrificed in the interests of security, should not and cannot be the default option. The protection of society through public safety initiatives can and must be done in a manner that also protects society's most cherished rights and values: privacy, liberty and freedom of choice. Law enforcement and public safety officials should lead with *Privacy by Design* – our safety and our freedom may indeed depend on it.

34 Cavoukian, A. (2011, October 31). Privacy invasion shouldn't be 'lawful', *The National Post*.

35 Information and Privacy Commissioner of Ontario. (2012). Beware of "Surveillance by Design" Symposium Archive, from http://www.realprivacy.ca/speakers

Bibliography

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter F.31.

Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M.56.

Personal Health Information Protection Act, S.O. 2004, Chapter 3, Schedule A.

Cate, F. "Government Data Mining: The Need for a Legal Framework." *Harvard Civil Rights-Civil Liberties Law Review (CR-CL)* 43, no. 2 (2008).

Cavoukian, Ann. "Beware of 'Surveillance by Design'." *Financial Post*, December 14 2011.

———. "An Open Letter from Commissioner Cavoukian to Minister of Public Safety Vic Toews and Minister of Justice and Attorney General of Canada Rob Nicholson." http://www.ipc.on.ca/site_documents/2011-10-31-Letter-to-Ministers-Toews-and-Nicholson-Surveillance.htm.

Cavoukian, A. "Privacy Invasion Shouldn't Be 'Lawful'." *The National Post*, October 31 2011.

Cavoukian, A., M. Chibba, and A. Stoianov. "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment." *Review of Policy Research* 29 (2012): 37–61.

Cavoukian, Ann, Michelle Chibba, and Alex Stoianov. "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment." *Review of Policy Research* 29, no. 1 (2012).

Green College University of British Columbia, and Information and Privacy Commissioner of Ontario. "National Security in a Post-9/11 World: The Rise of Surveillance ... the Demise of Privacy?", 2003.

Information and Privacy Commissioner of Ontario. "Beware of "Surveillance by Design" Symposium Archive." http://www.realprivacy.ca/speakers.

———. "A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight." In *The Eighth Workshop on the Economics of Information Security*. University College, London, England, 2009.

———. "Fact Sheet #7 - Disclosure of Information Permitted in Emergency or Other Urgent Circumstances." 2005.

———. "Get Smart About Privacy on the Smart Grid – Embed Privacy, by Design." Presented at the Chartwell Smart Grid Webinar, May 9, 2012.

———. “Guidelines for the Use of Video Surveillance Cameras in Public Places.” 2007.

———. “Municipal Order Mo-2225.” 2007.

———. “Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report Mc07-68 “, 2008.

———. “*Privacy by Design*.” 2009.

———. *Privacy by Design ... Take the Challenge*. 2009.

———. “Privacy by Design: The 7 Foundational Principles.” 2009.

———. “Privacy Guidelines for Municipalities Regulating Businesses Dealing in Second-Hand Goods.” 2007.

———. “Public Safety Is Paramount – but Balanced against Privacy.” September 21, 2001.

———. “Smart Meters in Europe: *Privacy by Design* at Its Best.” 2012.

———. “SmartPrivacy for Smart Public Safety.” Presented at the Toronto Forum for Global Cities Conference, Toronto, Ontario, November 10, 2009.

———. “Transformative Technologies Deliver Both Security *and* Privacy: Think Positive-Sum Not Zero-Sum.” 2008.

Information and Privacy Commissioner of Ontario, Hydro One, and Toronto Hydro Corporation. “*Privacy by Design*: Achieving the Gold Standard in Data Protection for the Smart Grid.” 2010.

Information and Privacy Commissioner of Ontario, and Jeff Jonas. “*Privacy by Design* in the Age of Big Data.” 2012.

Information and Privacy Commissioner of Ontario, and Kim Cameron. “Wi-Fi Positioning Systems: Beware of Unintended Consequences.” 2011.

Information and Privacy Commissioner of Ontario, and Tom Marinelli. “Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept.” 2010.

International Conference of Data Protection and Privacy Commissioners. “Privacy by Design Resolution.” Jerusalem, Israel, 2010.

Office of the Information and Privacy Commissioner for British Columbia. “Investigation Report F11-03.” 2011.

Rosenberg, Dave. “IBM Fellow Jeff Jonas on the Evolution of Big Data.” *CNET*, April 21, 2012.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York City: Springer, 2003.

The Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group"). "Freedom, Security, Privacy – European Home Affairs in an Open World." 2008.

Toronto Police Services Board, and Toronto Police Service. "Report of the Board / Service Race Relations Joint Working Group." 2003.

U.S. Department of Homeland Security. "DHS Privacy Office Public Workshop CCTV: Developing Privacy Best Practices (December 17-18, 2007)." http://www.dhs.gov/privacy-workshops#7.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

November 2012

http://www.privacybydesign.ca

Information and
Privacy Commissioner,
Ontario, Canada