The Roadmap for *Privacy by Design* in Mobile Communications:

A Practical Tool for Developers, Service Providers, and Users

www.privacybydesign.ca

December 2010

PRIVACY BY DESIGN RESEARCH LAB

Information and Privacy Commissioner,
Ontario, Canada

Acknowledgements

The authors, Drs. Ann Cavoukian and Marilyn Prosch, wish to acknowledge Vance Lockton and Michelle Chibba, Policy Department Staff, and Ken Anderson, Assistant Commissioner (Privacy), at the Office of the Information and Privacy Commissioner, Ontario, Canada, for their input on this paper.

The authors further recognize the members of the expert industry panel convened for the Arizona State University (ASU) *Privacy by Design* Lab's study on mobile technologies, and their contributions to that project. This panel consisted of Frank Dawson (Nokia), William H. Demaine (Mayo Clinic), Marissa Hambleton (MH2 LLC), Janet Price (MCC), Walt Tamminen (Nokia), Mark Williams (SRP), and American Institute of CPAs (AICPA) task force members Ken Askelson, Sagi Leizerov (Ernst & Young), Doron Rotman (KPMG) and Don Sheehy (Deloitte).

The authors also acknowledge The Privacy Projects, which provided funding for the initial research project at the ASU *Privacy by Design* Lab. The Privacy Projects is an independent, non-profit corporation established in 2008, and dedicated to investigating and recommending enhancements to current privacy policies, practices and technologies through research, collaboration and education.[1] In particular, the authors would like to acknowledge the leadership of Richard Purcell and Joseph Alhadeff.

[1] See http://theprivacyprojects.org/

Information and Privacy Commissioner,
Ontario, Canada

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

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

Table of Contents

Commissioner's Foreword

In the decade and a half since my Office first developed the concept of *Privacy by Design* (*PbD*), we have watched it grow from an idea that was often dismissed as being 'impossible' to being refined into a conceptual framework that has now reached global acceptance. This can be seen in two key moments that have recently occurred. First, in late-October 2010, an International Resolution was unanimously passed at the International Data Protection and Privacy Commissioners' Conference recognizing *PbD* as, "an essential component of fundamental privacy protection." Second, in December 2010, the U.S. Federal Trade Commission made adopting the *PbD* approach the first component of their framework for addressing the commercial use of consumer data.[2] The power of the 'design it in' approach to privacy is truly without borders. Now, as this concept spreads, the only questions that remain are along the lines of, "We believe in *PbD* … but how do we do it?"

This operationalization is the next challenge for *PbD*. Thus, when a chance was presented to create a Roadmap for *Privacy by Design* in the mobile communications industry, I gladly undertook the task. This opportunity arose from a study at Arizona State University (ASU). The study, run under the auspices of ASU's newly launched *Privacy by Design* Research Lab, looked to capture the insights and expertise of a panel of industry insiders, who each had on-the-ground, real world experience with embedding privacy into their organizations and industry. Convened by head researchers Drs. Marilyn Prosch and Julie Smith David, the expert panel consisted of top executives from a number of facets of the mobile communications industry, representing device manufacturers, service providers, and major technology consulting firms.[3] I was happy that the authors of this study asked the experts to stretch their ideas in considering what was achievable. Too often, we are constrained by the present in considering the very possible future. While a number of the solutions presented will take work and time to implement, I believe that none are beyond our reach, and that they provide useful and implementable guidance on the future direction of *PbD* in the mobile space.

The Roadmap for *Privacy by Design* in the mobile communications industry presented in this document expands on this initial ASU research, and reflects the high-quality, innovative contributions of the industry leaders comprising the expert panel, who have shown their commitment to ensuring the ongoing protection of, and respect for the privacy of the individuals to whom they provide an important service. We were able to identify solutions for which the panel had come to a clear consensus, both with regard to relevance to a given problem and operationalization characteristics, and use these solutions as the key elements of our Roadmap. In creating this guidance document, we are striving to demonstrate that *Privacy by Design* is not an ivory tower concept or theoretical distraction; it is, instead, an on-the-ground reality based on *practical* tools and solutions. As previously discussed by my office, though, *Privacy by Design* is a holistic concept that should be applied throughout an organization, end-to-end, including its information technology, business practices, processes, physical design and networked infrastructure. Thus, while many of the solutions presented herein focus on technology, this document should be used as a step towards a holistic *PbD* process in the mobile industry.

[2] Federal Trade Commission (Dec. 2010). Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers. Available at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[3] A full description of the methodology and results of this panel will be presented by the ASU researchers at the IAPP Global Privacy Summit in March 2011.

Over time, it has become increasingly clear to me that in order to fully realize the privacy protections required for mobile devices and communications, practical tools are needed to help inform each of the players in that industry how to embed privacy into their practices according to their role. Some initial work is being done in this area – the International Working Group on Data Protection in Telecommunications will, for instance, soon be releasing its recommendations to suppliers and users of mobile devices in its document, “Mobile Processing of Personal Data and Security.” To these efforts we now add this Roadmap – the result of an innovative, highly collaborative effort of a number of excellent minds. I would like to acknowledge all of the individuals and organizations who have added their considerable expertise to this project, and in particular, I must thank Richard Purcell, President and Executive Director, and Joseph Alhadeff, Chairman, of The Privacy Projects, without whose funding the ASU study could not have been undertaken.

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario, Canada

1 Introduction

Privacy by Design is a concept that is virally spreading around the globe. The powerful concept of engineering privacy directly into the design of new technologies, business practices and networked infrastructure, in order to achieve the doubly-enabled pairing of functionality and privacy, has gained significant adoption by governments, researchers and industry, in any number of sectors. Now that the *PbD* paradigm has achieved this high level of acceptance, the next major question to be addressed is – how can *PbD* best be operationalized?

In the first half of 2010, Arizona State University's *Privacy by Design* Research Lab set out to develop a set of practical tools to answer this question, by focusing on a particular case study: the mobile communications industry. To achieve this, the researchers convened an expert panel of top executives in the leading organizations in this industry, with the goal of identifying and rating the privacy and security challenges in their growing field – as well as proposing potential solutions – based on their real world, on-the-ground experiences. Participants based their discussions around the 7 Foundational Principles of *Privacy by Design*,[4] and eventually reached a consensus on 15 challenges (ranked 'medium' to 'critical'), and 70 associated potential solutions.

In this guidance document, we focus on the solutions presented by the panellists – in particular, the parties to which responsibility for the implementation of each were assigned. Distinct trends were noted in the types of solution associated with each party, and it became clear that the panellists' responses could be collected into a practical tool for developers, service providers and users – a Roadmap for *Privacy by Design*.

Here, we begin by describing the necessity for such a tool in the mobile industry, and then detail the Roadmap, which begins with the Device Manufacturer, travels through the OS/Platform Developer, Service Provider, and Application Developer, and ends with the responsibilities assigned to Users themselves.

2 The Widespread Adoption of Mobile Communications Technology

Addressing the privacy and security of mobile communications has become critical, as these devices have reached penetration levels unlike any other major communications technology (see Figure 1). By the International Telecommunication Union's estimates, there are approximately five billion cell phone subscriptions globally.[5] In North America, it is estimated that there are 94 cell phone subscriptions for every 100 individuals, while in Europe, there are 120 subscriptions per 100 people. Access to mobile networks is available to 90% of the world's population, including 80% of the rural population. Usage rates are also staggering – for instance, over 6.1 trillion SMS messages (i.e. 'texts') are sent annually, or approximately 200,000 per second.

[4] Available at: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

[5] All estimates and usage statistics in this section are from: International Telecommunications Union (ITU), "The World in 2010." http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf

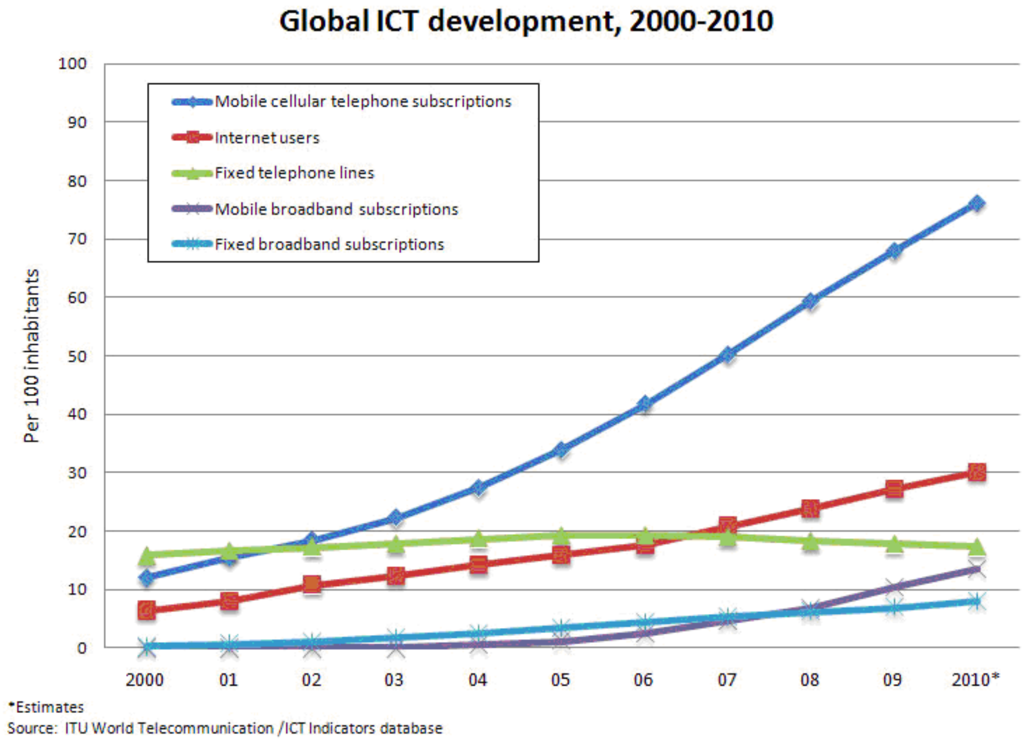

Figure 1: Global ICT Development (Source: International Telecommunications Union, "The World in 2010")

In addition to this spread, mobile devices are becoming more advanced, as they are increasingly engineered to be capable of performing most of the same types of actions as laptop or desktop computers (with the primary exception of applications that require very high processing power). Internet access, email, data storage and processing, and the use of first or third party applications, are now commonplace on any number of mobile devices. On top of the benefits for any time communication and connection, these advances are making information truly mobile – wherever they are, users can quickly find, or be provided with, information related to their immediate interest, location or problem, and can keep vast quantities of digital resources available at all times. Where the Internet can be said to have sparked an 'information revolution', the lesser infrastructure required for deployment and use of mobile technologies has sparked an 'access revolution'.

2.1 Privacy and Mobile Communications

Of course, information passing to and from a single, powerful mobile device raises potential privacy and security issues. Any concerns that one may have had with personal computing can now be said to apply to mobile communications technology – and any concerns about ISPs quickly translate to the central hub for all phone calls made, text messages sent, and data transferred: the network provider. In addition to this, a host of current and future issues are raised by the combination of significant computing power and a portable form factor. Communications to and from the device will be wireless, by and large – signal interception[6] is thus a concern that must be addressed.

[6] This includes both criminal and legitimate purpose (e.g. law enforcement) signal interceptions, the latter of which requires consideration of appropriateness, due process, proportionality, and user notification / control.

Legitimate data transactions also raise privacy concerns, particularly as location data is increasingly being associated with mobile communications. Unlike laptop or other portable computers with which users generally engage on an ‘as-needed’ basis, mobile devices are likely to be ‘always-on’ (to allow for reception of incoming phone calls, text messages, etc.) – as such, tracking the location of a mobile device will often give a highly accurate impression of its owner’s movements throughout the day. Finally, the small, portable nature and high value of mobile devices makes them prone to loss or theft – a significant issue when such devices are assigned increasingly more functionalities, and store increasingly more personal or otherwise sensitive data.

The increasing ubiquity and power of mobile devices is beginning to both clarify and magnify their associated privacy concerns. However, rather than waiting for issues to arise, academics and industry professionals are looking to get out ahead of the curve, taking a proactive (rather than reactive) approach to building privacy into the industry – without losing the significant benefits associated with fully realized functionalities. This is the heart of *Privacy by Design* – anticipating and addressing privacy issues before they become problems, in a positive-sum manner.

3 A Roadmap for *Privacy by Design* in the Mobile Communications Industry

Acceptance of the *PbD* paradigm, and adoption of the 7 Foundational Principles provides a strong foundation to building privacy into any industry (see Table 1). However, various players, including industry, government, and even users, are asking how these principles can be put into practice. They need a roadmap for privacy – a practical tool that can aid in outlining the steps required to fully embrace the *PbD* doctrine. This operationalization is the challenge facing privacy professionals today – and the one we chose to address for the mobile communications industry below.

Table 1 – The 7 Foundational Principles of Privacy by Design

Principle	Description
1. ***Proactive*** not Reactive; ***Preventative*** not Remedial	The *Privacy by Design* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default Setting***	We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, *by default*.
3. Privacy ***Embedded*** into Design	*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
4. Full Functionality – ***Positive-Sum***, not Zero-Sum	*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretence of false dichotomies, such as privacy ***vs.*** security, demonstrating that it ***is*** possible to have both.
5. End-to-End Security – ***Full Lifecycle Protection***	*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.
6. ***Visibility*** and ***Transparency*** – Keep it ***Open***	*Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify.
7. ***Respect*** for User Privacy – Keep it ***User-Centric***	Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

As noted, a panel of experts strongly versed in both privacy and mobile communications developed 70 solutions to 15 challenges facing the industry. Importantly, the panellists also identified which one or more parties had, in their view, primary responsibility for each solution. Analyzing their responses, it became clear that themes could be identified in the solutions assigned to each party;

the industry representatives were, in effect, laying out a roadmap of responsibilities that should be met in order to address the privacy and security challenges of mobile communications.

Even in this laying out of these responsibilities, one of the key insights arising from the expert panel was the confirmation that "*Privacy by Design* is a team sport."[7] No single designer can achieve privacy within an organization, and no single organization can achieve privacy within an industry. Concurrent with traditional, internal considerations such as the Privacy Impact Assessment, privacy/security Gap Analysis, and the Threat Risk Assessment, each of which is becoming common practice within numerous industries, privacy must be considered in a holistic, ecosystem-wide manner if it is to be both effective and lasting. It is notable, then, that while the expert panel in some cases heavily weighted responsibility for a solution towards a single party, there was no solution for which all of the expert panellists agreed that responsibility could be assigned *exclusively* to a single party. Thus, while this Roadmap identifies key messages for each player individually, the hallmark for success of *Privacy by Design* will be collaborative efforts across various parties.

In short, allocating responsibility for any aspect of this Roadmap to a particular party does not remove the requirement for collaborative efforts across the ecosystem. In addition, this Roadmap, and the solutions identified by the industry panellists, is not necessarily comprehensive – the absence of a particular solution does not imply that it may be discarded, or should not be implemented. Instead, this Roadmap describes the focal points for each group, as identified by the industry panel. They should be taken as an insight into the innovative thinking that will be required to fully realise the promise of *PbD*.

With the above considerations in mind, we present the Roadmap for *Privacy by Design* in the Mobile Communications Industry.

[7] A term developed by Oracle Corporation's Vice President for Global Public Policy, Joseph Alhadeff. http://www.privacybydesign.ca/content/uploads/2010/03/Going_for_the_gold.ppt.PbD.pdf

Table 2 – Roadmap for *PbD* in the Mobile Communications Industry: A Snapshot

Player	Roadmap Features
Device Manufacturer *Ensure that the requisite privacy tools are built-in, embedded in design*	**Sample Solutions Discussed** **DM1** – Build privacy protections into the device form factor **DM2** – Allow users to differentiate between roles **DM3** – Consider thin-client mobile devices **DM4** – Develop a privacy wizard to allow protections to be set quickly and easily **DM5** – Develop at-a-glance feedback mechanisms for data being collected **DM6** – Create safe disposal and secure destruction mechanisms
	Key *PbD* Principles[8] Principle 2 - Privacy as the default setting Principle 3 - Privacy embedded into design Principle 5 - End-to-end security – full lifecycle protection
OS / Platform Developer *Work with device manufacturers to integrate controls and reporting mechanisms*	**Sample Solutions Discussed** **OS/PD1** – Collaborate with the Device Manufacturer **OS/PD2** – Integrate fine-grained, cross-application privacy controls **OS/PD3** – Regulate applications' access to device data **OS/PD4** – To the extent practicable, define privacy requirements and security standards for services provided on the platform **OS/PD5** – Develop reporting mechanisms
	Key *PbD* Principles Principle 2 - Privacy as the default setting Principle 3 - Privacy embedded into design Principle 4 - Full functionality – positive-sum, not zero-sum

[8] The identified 'Key *PbD* Principles' represent focal points inferred from the responses of an expert industry panel. They are not, importantly, an indication that players can *solely* focus on the listed Principles; the *Privacy by Design* paradigm should be understood, and implemented, as a cohesive whole.

Player	Roadmap Features
Network Providers *Educate your users, keep the data safe*	**Sample Solutions Discussed** **NP1 –** Use the direct relationship with users to promote privacy education **NP2 –** Protect data travelling through the network **NP3 –** Consider the creation of an identity infrastructure for users
	Key *PbD* Principles Principle 5 - End-to-end security – full lifecycle protection Principle 6 - Visibility and transparency
Application Developers / Data Processors *Integrate privacy into the development cycle, and practice data minimization techniques*	**Sample Solutions Discussed** **AD/DP1 –** Abide by the protections of the Global Privacy Standard **AD/DP2 –** Employ notice and *informed* consent **AD/DP3 –** Utilize and document appropriate security practices **AD/DP4 –** Use privacy-protective default settings **AD/DP5 –** Ensure end-to-end protection of data **AD/DP6 –** Design applications with privacy in mind
	Key *PbD* Principles Principle 2 - Privacy as the default setting Principle 4 - Full functionality – positive-sum, not zero-sum Principle 5 - End-to-end security – full lifecycle protection
All Parties *Develop standards and privacy frameworks, as well as consumer-facing privacy icons*	Sample Solutions Discussed AP1 – Develop privacy standards for the mobile industry AP2 – Develop privacy 'seals' AP3 – Develop and utilize consumer-facing privacy icons AP4 – Recognize that transparency, education and awareness are the keys to trust
	Key *PbD* Principles Principle 1 - Proactive not reactive; preventative not remedial Principle 6 - Visibility and transparency Principle 7 - Respect for user privacy

Player	Roadmap Features
Users / Consumers *Control your data, and use the settings available to you*	**Sample Solutions Discussed** **U/C1** – Use the protections provided **U/C2** – Be receptive to privacy messages from service providers or developers
	Key *PbD* Principles Principle 1 - Proactive not reactive; preventative not remedial Principle 7 - Respect for user privacy

3.1 Device Manufacturers

Ensure that the requisite privacy tools are built in, embedded in design

Key Messages:

- Build in any protections that can be made OS/Platform/Application independent (e.g. automatic encryption of stored data);
- Build in privacy/security tools required by other developer levels (e.g. multi-factor authentication);
- Build in simple data wipe mechanisms for end-of-life or phone loss/theft scenarios;
- Determine a means of digitally marking or separating roles (e.g. youth vs. adult, home vs. work); and
- Ship phones with potentially privacy-invasive features (e.g. geolocation information accessible by applications) turned **off**.[9]

From its infancy, *Privacy by Design* has had a close relationship with Privacy-Enhancing Technologies (PETs), and, more recently, Transformative Technologies.[10] PETs pioneered the notion that technologies may be used to *enhance* privacy by building in safeguards – protecting data before it ever reaches a third party. Transformative technologies extend this notion, designing a PET into a privacy-invasive system to minimize the unnecessary collection, use and disclosure of personal data, and to promote public confidence and trust in data governance structures. Through the years, the IPC has profiled

[9] If, for regulatory (e.g. emergency services must have access to geolocation information) or technical reasons, the geolocation capability or other functionality of the device cannot be turned entirely off, the default condition should be that such information is inaccessible to applications not covered by the regulation. This difference should be made clear to the user, however.

[10] See http://www.ipc.on.ca/images/Resources/trans-tech.pdf

a number of such Transformative Technologies, including Biometric Encryption,[11] Secure Visual Object Coding,[12] and a host of other transformative solutions for technologies involved in the Smart Grid,[13] IP Geolocation and Online Targeted Advertising,[14] and In-Home Health Monitoring.[15] Each of these solutions has a common element – they recognize that reliance on policy and regulation alone is not sufficient, and as such, privacy protections must be directly built into the technology itself. It is notable, then, that a 'major-medium' challenge identified by the panellists was, "a lack of responsibility by device makers [that] point to service providers as the responsible party." The industry experts agreed that the device itself could play a significant role in the protection of privacy – by building it into the system, by default (*PbD* Principle 2), embedding privacy into the design of mobile devices (*PbD* Principle 3), and providing end-to-end data lifecycle protections (*PbD* Principle 5). The panellists' responses fell into two primary categories: those built into the operation of the device, and those that engage the user. Again, we note that these – and most other – solutions may not be solely addressed by a single industry player (here, the Device Manufacturer). *Privacy by Design* is a collaborative process in which all parties must come together to identify and develop privacy solutions.

3.1.1 Expert Panel Sample Solutions for Device Manufacturers – Device Operation

DM1 – Build privacy protections into the device form factor: The first category of Device Manufacturer responsibility notes that the capacities of the device form the foundation upon which any other privacy protections must be built. Device hardware is the most difficult aspect of a mobile technology to update – if at all possible. If a problem occurs, or a feature is lacking, in either the operating system or an individual application, an update can be pushed out; mistakes can be corrected. However, if a feature is absent from the form factor of a device, it will likely remain so – only those individuals purchasing a redesigned model will get the update, not existing customers. As such, significant planning must be put into the privacy tools that are built into the device, and made available to the operating system and applications. In this light, the expert panel has recommended two tools be designed-in to mobile devices: 1) automatic, seamless encryption of data stored on the device,[16] and 2) meaningful, usable multi-factor authentication capabilities. These protections, in combination with measures such as an enforced access PIN and/or password, will serve as a reliable base that the user can expect always to be present, regardless of the platform, applications or network that he or she engages.

DM2 – Allow users to differentiate between roles: In the same category, at the device level (in combination with the OS/Platform Developer) an opportunity exists to build in features which strongly differentiate between different types of users, or the various roles of single users. Two potential areas of research are presented by the expert panel on this topic. First, it is recommended

[11] See http://www.ipc.on.ca/images/Resources/bio-encryp.pdf

[12] See http://www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf (pg. 12-14)

[13] See http://www.privacybydesign.ca/content/uploads/2010/03/achieve-goldstnd.pdf

[14] See http://www.privacybydesign.ca/content/uploads/2010/10/pbd-ip-geo1.pdf

[15] See http://www.ipc.on.ca/images/Resources/pbd-sensor-in-home.pdf

[16] The IPC has again ordered that any Personal Health Information (PHI) carried on a portable device must be encrypted. See the January 2010 PHIPA Order HO-OO7, "Encrypt Your Mobile Devices: Do It Now," available at: http://www.ipc.on.ca/images/Findings/ho-007.pdf. See also PHIPA Order HO-004, issued in March 2007, available at: http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf.

that mobile devices might include a mechanism by which certain interactions could be flagged and prevented based on various user profiles or preferences – allowing, for instance, a parent to specify that the primary user of the phone is a youth, and thus certain data collection or processing should not be permitted. Care must be taken, however, to prevent future categorization or identification of the user, should elements of these profiles be discoverable outside of the device (e.g. a service provider inferring that the device belongs to a youth because an interaction is blocked). A second area of potential research is the design of devices with multiple, distinctly separate memory devices (and, potentially, CPUs) that can be toggled by users – to separate, for instance, home from work computing. For both of these solutions, deep integration of protection into the device (at the hardware or OS/Platform level) will allow for additional certainty that user choice, with regards to his or her identity characteristics when using the device, will be respected across all applications.

DM3 – Consider thin-client mobile devices: A further area of research raised is the development of thin-client mobile devices, which would store little or no PI on the device itself – instead, storing this information on remote servers. Such devices would allow for a refocusing of security, moving away from device-based protections to focus on the security of remote servers, whether wholly controlled by a provider or existing 'in the Cloud.' Of course, collecting the PI of multiple users in a single location brings with it its own privacy challenges, including the fact that such a collection might prove a tempting target for criminals (or advertisers), and could have serious consequences if breached, leaked or inappropriately reused. Cryptographic protocols would also likely need to be supported for the transfer of data to and from the device. However, such an arrangement might be of significant benefit for situations in which the data is already centrally protected, but mobile access is required (or where the user opts for this method of remotely storing their data).

3.1.2 Expert Panel Sample Solutions for Device Manufacturers – Engaging Users

In a second category of panellist solutions assigned to the Device Manufacturer, it should be noted that the expert panel did not feel the device manufacturer should consider itself to be disconnected from its end-user. Throughout the lifespan of a device, opportunities exist for the mobile device maker to engage with the consumer with respect to privacy provisions. The expert panel suggested, for instance, three primary points at which privacy options could be made clear to the user.

DM4 – Develop a privacy wizard to allow protections to be set quickly and easily: First, the panellists suggested that a privacy wizard be developed, that would help parents and responsible minors set defaults on a device when it was first taken out of the box. While this solution was initially proposed as a means of differentiating adult users from children, it could easily be extended to include all privacy options on the device. An example of this is found in the geolocation feature of many modern mobile devices. The expert panel recommended that devices be shipped with this capability turned **off;**[17] a privacy wizard displayed at the first startup of the device could inform users of the geolocation capability of the device, describe the potential privacy implications thereof, and allow users to turn it on, if desired, as well as set any initial 'location-blocking' conditions (during particular times of the day, for instance). The usefulness of the privacy wizard could further be extended by making it a persistent privacy tool, available to the user throughout the lifespan of the device. This would allow

[17] See footnote 9.

individuals to easily edit their privacy settings based on their changing circumstances or experiences. Finally, this privacy wizard might also be driven through the set up of the mobile sync client on the user's laptop/desktop computer, should that be the more appropriate form factor.

DM5 – Develop at-a-glance feedback mechanisms for data being collected: Next, users should be made aware of when personal information is being collected. Of course, some information arising from the technical operation of a phone, such as its broadcast signature, could potentially be used (in combination with other information) to identify a user. The user should be aware of this possibility, but does not necessarily need to be constantly notified of its transmission. However, notifications are a useful tool for those data elements that can be controlled by the user. For instance, an icon, light or other 'at-a-glance' feedback mechanism could be displayed when the geolocation capability of the device is active, or the data it is generating is accessible to installed applications. A simple means of switching between open (e.g. location-enabled) and private (e.g. location-blocked) modes might also be provided, such as a button or switch (alternatively, this easy switch feature could be integrated into the operating system of the device).

DM6 – Create safe disposal and secure destruction mechanisms: Finally, with the current focus on safe disposal or recycling of electronic devices,[18] and in keeping with *PbD* Foundational Principle 5 (End-to-end security – lifecycle protections, including secure destruction), it is important that both end-of-life and loss-of-use (should the phone be lost/stolen) protections be built in to allow users the option of securely deleting any personal or sensitive information on the device. BlackBerry, for instance, offers this in multiple ways: a device wipe based on multiple incorrect password entries, an on-device wipe command, and even a remote data wipe option (after installation of the free BlackBerry Protect program), should the user not be in possession of the device when the data wipe is required. Each of these wipes can be customized to include part, or all, of the data on the device, including that stored in removable memory cards.[19]

[18] See, for instance, www.recycleyourelectronics.ca

[19] See the IPC's publication BlackBerry Cleaning: Tips on How to Wipe Your Device Clean on Personal Data - http://www.ipc.on.ca/images/Resources/blackberry-cleaning.pdf

3.2 OS/Platform Developers

Work with device manufacturers to integrate controls and reporting mechanisms

Key Messages:

- With Device Manufacturers, build in cross-application privacy protections and security controls;
- Provide a simple, easy-to-understand user interface for such controls;
- Control data passing from device to applications; and
- Design reporting features that allow the user to be notified of how data is being collected, by what applications, and whether any exceptions to his/her privacy preferences have occurred.

The Operating System and Platform of a mobile device are key enablers of privacy and security protections, due to their central position in virtually all device interactions. While the OS/Platform may not create or collect significant amounts of data (particularly if we consider the device, and not the OS/Platform, to be the location of stored user data), it provides the interface with which other parties must engage in order to access data, set preferences, or utilize many of the protections built-in by the Device Manufacturer. As such, the panellists' focus for OS/Platform Developers was the building in of tools that could assist other mobile industry players in achieving their privacy and security goals. They focused on embedding privacy into the design of technologies (*PbD* Principle 3) and ensuring that privacy was the default condition (*PbD* Principle 2), while maintaining the positive-sum of full functionality alongside strongly protected privacy (*PbD* Principle 4).

OS/PD1 – Collaborate with the Device Manufacturer: First, it must be recognized that the Device Manufacturer alone cannot instantiate a number of the privacy and security protections that they may desire – the OS/Platform Developer must provide support for many hardware factors, in order for them to be effective. As such, the OS/Platform Developer should engage with Device Manufacturers to determine what privacy measures are in development, and how they can best be integrated into system functionality. The expert panel in particular noted that the OS/Platform should ensure that the goal of built-in encryption of device data is fully supported, without negatively affecting functionality.

OS/PD2 – Integrate fine-grained, cross-application privacy controls: Second, it should be understood that the OS/Platform is the primary point of connection between the device and the user (in combination with the physical form factor). In particular, the OS/Platform's user interface is likely to be an individual's point of most frequent engagement with the device. It is also the primary point at which the vast majority of fine-grained, cross-application privacy and security controls may be instantiated, as the device hardware will provide the user only limited, and most likely binary, options (a switch to turn geolocation on/off, for example). Thus, it is critical that these controls are both effective and available to *all* users, regardless of technical expertise or comfort level. Being the primary point of contact with the user (and thus his or her privacy experience), these controls must be easily accessible (as close to the home screen as possible), understandable (explanations of features should be made available), and comprehensive (wherever a privacy feature can be instantiated at the OS/Platform level – rather than the application level – it should be). Of course, in consideration of the diverse development environments and complexity of functions across applications, it may not always be possible to enable such cooperative development of granular cross-application protections. In those situations, OS/Platform providers should, to the extent practicable, provide application developers with application programming interfaces (APIs) to privacy functions that can be used to enable more centralized and seamless preference selection and management.

OS/PD3 – Regulate applications' access to device data: Third, by allowing varied levels of access to device information, the OS/Platform can also aid the Application Developer to realise its goal of data minimization. An application developer could specify, for instance, the level of granularity needed when accessing the device's geolocation feature – accessing or collecting only the data required for the specified purposes, rather than gathering (in this example) the exact location – transforming it to the lesser level of precision required for a certain functionality to be provided. This rule could be applied to any data being collected by an application directly from the device, rather than needing to be entered by the user.

OS/PD4 – To the extent practicable, define privacy requirements and security standards for services provided on the platform: While in many instances it will not be possible to engage with all applications installed by all users, where the opportunity arises OS/Platform developers should define privacy requirements and security standards that application developers or other service providers should meet, and work with relevant service providers to implement these standards in a timely fashion. Such a system might best be deployed by the provider of any central, official means by which applications are distributed for a particular platform (e.g. the Apple iPhone App Store, or BlackBerry's App World). This data protection should extend throughout the lifecycle of the data (see *PbD* Principle 5: End-to-End Security – Lifecycle Protection).

OS/PD5 – Develop reporting mechanisms: Finally, the expert panel noted that, as the central interface through which on-device data transactions will take place, the OS/Platform is in a prime position to assist in the monitoring of privacy controls and practices, to ensure that they are working as intended. A reporting mechanism for data accesses and/or exceptions should thus be created, results from which would be relayed to the user or the service provider for review, as appropriate.

3.3 Network Providers

Educate your users, keep the data safe

Key Messages:

- Educate users about the risks associated with personal information;
- Complete a threat risk assessment and conduct annual, independent third party privacy audits; and
- Work to create a federated identity management subsystem.

NP1 – Use the direct relationship with users to promote privacy education: The relationship between the Network Provider and the consumer is different than that between consumers and the Device Manufacturer or OS/Platform developer. The latter two parties create products that will be used by an unknown user; they may understand a likely demographic, but have no real sense of the properties of any individual consumer. Network Providers, on the other hand, are in the position of having a more 'personal' relationship with their customers (at the very least, due to the ongoing payment arrangement). This relationship may also extend beyond the device - for instance, pamphlets may be included with bill mailings (or electronic bills) in order to engage the consumer with advice or educational moments with regard to his or her privacy, during a free moment in his or her day (as opposed to bringing up messages while he or she is looking to accomplish a task on the device). Thus, in addition to any 'in-the-moment' or 'how-to' messages (which might be handled on the device), the Network Provider may have the opportunity to engage with the consumer in an ongoing reflection of the 'why' of privacy protection.

NP2 – Protect data travelling through the network: In addition to a possible role as "educator," the Network Provider plays a central, infrastructure role in the mobile communications space. As such, it also has a responsibility for protection of the data that comes across the network. Traditional privacy measurements, such as the Threat Risk Assessment, Privacy Impact Assessment, and independent third party privacy audits (along with the implementation of any necessary protections identified during these processes), are suggested as key tools to ensure that potential risks and exposures of personal information have been addressed and demonstrate good privacy practices and controls. Such evaluations look to ensure that the 6th *PbD* Foundational Principle – Visibility and Transparency of business practices and technologies, with relation to PII – is met.

NP3 – Consider the creation of an identity infrastructure for users: Finally, it was suggested by the panellists that Network Providers consider developing a Federated Identity Management system, including privacy broker service elements, for use by a defined community of services. Such a system would extend the notion of the thin-client device suggested for Device Manufacturers, by centralizing the management of users' identity credentials in an off-device location. The user would then be able to participate in the network with the understanding that any applications or services in this community wishing to access identity credentials would have to do so through a defined privacy broker – an alternative means of instantiating cross-application protections.

3.4 Application Developers / Data Processors

Integrate privacy into the development cycle, and practice data minimization techniques

Key Messages:

- Practice data minimization;
- Use privacy-protective default settings; and
- Maintain user awareness, and control of, data collection and use.

AD/DP1 – Abide by the protections of the Global Privacy Standard: For most users of mobile technologies, there will come a point at which on-device privacy protections will not suffice to protect their data: when he or she chooses to engage with an application, and sends it, or allows it to access, his or her personal information. At this point (for many applications), data will be transferred off the device for processing – and the full range of protections offered by Fair Information Practices as contained in the Global Privacy Standard (GPS),[20] must be engaged by the Application Developer and/or Data Processor. Permission from the user to access data does not remove responsibility from the Application Developer (or the associated Data Processor) for its proper, and limited, handling – a fact noted by the industry panel. The panel focused, in particular, on the principles of Collection Limitation and Data Minimization – keeping the collection of personal information to that which is fair, lawful, and limited to that which is necessary to collect for specified purposes. Of course, this should be done without sacrificing the application's functionality, or user experience. The IPC has recently described this as the "Min/Max Principle" – using the minimum amount of personal information to achieve the maximum functionality – positive-sum at its best.

AD/DP2 – Employ notice and *informed* consent: When applications require (minimally necessary) personal information in order to provide a function or service, protections must be applied to that data throughout its entire lifecycle – from collection, to use/storage, to destruction. This begins with the principles of Notice and Consent. At a minimum, the user should be made aware of how PII will be used, how long it will be retained, how it will be deleted or anonymized, and when and under what circumstances it will be transferred to other data processors or service providers. Users should also be able to view, review and control personal information, when it has not been anonymized. However, the solutions proposed by the expert panel go further, suggesting that application developers work to ensure that users are able to exercise *informed* consent. At the application level, direct engagement with users allows for a number of opportunities for raising levels of user education and awareness with regard to privacy. Ideally, these will be targeted at the user who is cognizant of privacy concerns, but who may not have the time or opportunity to read lengthy policies, nor explore advanced settings in applications. As such, application developers may wish to consider quick, simple ways to engage users in the control of their data - for instance, developing and using universal privacy icons (discussed further in the next section), building parental settings into applications, or developing online games to teach children about being 'safe' on mobile devices.

[20] http://www.privacybydesign.ca/content/uploads/2010/06/gps.pdf

AD/DP3 – Utilize and document appropriate security practices: Once personal information has been collected, data processors should consider themselves to be custodians of that information, which brings with it a duty of care. Security practices should be both implemented and clearly documented to restrict access to PII to only those applications or individuals with a business need to have such access, protect it from loss, and allow users to revoke access, if needed.

AD/DP4 – Use privacy-protective default settings: In addition, as users are learning to safeguard their data, the initial conditions that they encounter must be privacy-protective. We know (see *PbD* Principle 2: Privacy as the Default Setting) that "the default rules" – in 80% of cases, the default setting is the condition that will prevail. User privacy can thus be greatly affected simply by designing a privacy-friendly default case. For instance, a 'push' model of data collection – in which the user chooses when and what data is distributed to applications – will always be a more privacy-friendly default option than a 'pull' model, involving automatic collection (which may be overlooked by the user). Again, this Roadmap does not seek to limit mobile functionality (we aim for a win-win scenario; see *PbD* Principle 4: Full Functionality – Positive-Sum, not Zero-Sum) – if necessary, the latter choice can be offered to the user, once he or she has been made aware of any potential risks. It is critical though, that users be given the ability to exercise control over their data.

AD/DP5 – Ensure end-to-end protection of data: Finally, as with the mobile devices themselves, the end-of-life condition of data collected through mobile communications must be defined (see *PbD* Principle 5: End-to-End Security – Lifecycle Protection). There are two complimentary means of doing this, as presented by the panel. First, organizations should instantiate a process by which all data held should be periodically assessed to determine the necessity of retaining each data element in consideration of the purposes for which it was collected, with destruction or anonymization occurring as necessary. This step will help inform application developers of requirements and functions related to data retention and allow data processers to be constantly mindful of their data usage and collection practices, and adjust them, when required, to obtain the maximal level of data minimization. Secondly, it is recommended (as the top solution for two separate challenges) that research be conducted into an appropriate means of tagging or otherwise embedding into data one or more expiry conditions. These conditions may include a defined use, or a specified time limit, and once the condition is met, the data would no longer be accessible to the data processor. Such a mechanism would both assist processors in their data management practices (by allowing for automatic recognition of data in need of deletion), as well as providing data subjects with an assurance that data use would be limited to that provided in the collection notice.

AD/DP6 – Design applications with privacy in mind: To achieve *Privacy by Design*, however, the above protections cannot be 'bolted-on' after an application is developed. Instead, privacy should be considered a core functionality, and addressed throughout the development process. In fact, the overarching theme behind *Privacy by Design* is captured in the solution ranked most important, for the only challenge rated as critical: Application Developers should "design new applications with privacy in mind right from the outset, and throughout the process and prototyping."

3.5 All Parties

Develop standards and privacy frameworks, as well as consumer-facing privacy icons

Key Messages:

- Develop universal, user-facing privacy symbols or icons that indicate how data will be collected and/or used;
- Develop/reach a consensus on industry standards or frameworks, indicating that all services meeting the standard will treat personal information in the same manner;
- Publish privacy guidelines for mobile development; and
- Treat user awareness as a marketing tool.

AP1 – Develop privacy standards for the mobile industry: Within any industry, one of the most effective means of ensuring that a core functionality is met at an agreed upon level is the development of standards. Achieving *Privacy by Design* in the mobile communications industry, then, will involve the development of industry-wide standards and privacy frameworks for the collection and use of data in mobile technologies and applications. This development cannot be accomplished by any single party – it requires collaboration between all involved partners, including Device Manufacturers, OS/Platform Developers, Network Providers, Application Developers, and representatives for User groups, as applicable. Already, numerous standards for security in various aspects of mobile communications either exist or are under development. To name just one example, the SEPIA (Secure Embedded Platform with Process Isolation and Anonymity) Initiative in the EU is looking to develop standards (and a certification process) for smartphones and tablets worldwide, which would build trust that mobile products can be as secure as PCs[21] when it comes to storing, transmitting and processing sensitive (e.g. financial/medical) information. Thus, the expert panel saw little reason that similar standards could not be developed with regard to both the on- and off-device protection, and appropriate use of personal information in mobile technologies and applications. Such standards speak to the proactive and preventative measures required by *PbD* Foundational Principle 1 (Proactive not Reactive; Preventative not Remedial).

AP2 – Develop privacy 'seals': Once these privacy standards are defined, then certainty may exist, from the developer, to the advertiser, to the user, that any technology or application which conforms to a standard will collect, use and/or protect data in a consistent manner. This would then allow for the creation of 'seals' which could be attached to various technologies or applications[22] – and lift significant burden from the user. Rather than being forced to evaluate every piece of software and hardware individually, users could define a level of privacy with which they were comfortable,

[21] See: http://bit.ly/gqrj9g

[22] The IPC, for instance, is currently growing its Privacy by Design Ambassadors program, which provides a means of labelling those groups, businesses or developers that have applied the PbD Principles within their organizations. See http://www.privacybydesign.ca/ambassadors/

determine what standard matched that level, and look for products conforming to it. Research could also be undertaken on whether some of these comparative and evaluative functions could be automated in the form of discovery, reputation and policy matching/negotiation services.

AP3 – Develop and utilize consumer-facing privacy icons: In addition, joint responsibility should be shared in the development of, "a set of easily understood universal privacy symbols that are displayed when PII is collected by, used by, or transferred from the mobile device," as well as policies regarding, "when, how and the duration [for which] these symbols are to be displayed," with the goal of creating visibility and transparency for data collection, usage and disclosure practices (*PbD* Principle 6). This notion of 'at-a-glance' privacy notifications is not without precedent. In this area, the IPC received the IAPP's *Privacy Innovation Award* for its work in the field of 'Privacy Short Notices' – concise and easily understood notices informing individuals of how their personal information is being used.[23] Similar efforts exist across numerous fields; the Platform for Privacy Preferences (P3P) Project, for example, was an effort to allow websites to express their privacy practices in standard, human and machine-readable formats. These practices could be interpreted by browsers or other software to provide the user with information about the site's data collection and usage policies, or automatically make decisions, when appropriate. Researchers such as Lorrie Faith Cranor at Carnegie Mellon University have also been investigating the notion of a "privacy nutrition label" for websites, which they have found improves both users' abilities to comprehend privacy policies and improves their satisfaction in engaging with the information.[24]

The behavioural advertising industry has also been examining the potential of a privacy icon to raise awareness of its practices and use of personal data – a process that may be worthy of examination by the mobile communications industry. Facing significant scrutiny from privacy advocates, federal regulators and customers who feel uncomfortable with their online behaviours being 'tracked' for advertising purposes, a range of parties associated with behavioural targeting have looked to develop an icon to represent, or link to, additional information about advertising practices. It is felt that greater transparency will lead to greater consumer trust – a hypothesis that is supported by a 2010 Future of Privacy Forum study that found that adding transparency and choice to targeted advertising nearly doubled the proportion of survey respondents who stated that they felt comfortable with the practice, raising it from 23% (without transparency and choice) to 40%.[25] The icon currently adopted is shown in Figure 2.

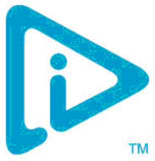

Figure 2: Evidon's Advertising Option Icon, or Forward I

[23] See: http://www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=728

[24] Gage Kelley, P., Cesca, L, Bresee, J., and Cranor, L.F. (2010) Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach.

[25] Future of Privacy Forum Online Behavioural Advertising "Icon" Study. January 25, 2010. http://futureofprivacy.org/final_report.pdf

Formally called the "Advertising Option Icon,"[26] but colloquially known as the "Forward I," this icon is displayed in the upper-right corner of online advertisements from participating companies that are targeted based on "third party, interest-based data." Clicking the icon brings up an advertiser-branded window with additional information and links with descriptions of targeted advertising, FAQs and/or an opt-out screen for specific interest-based advertising providers.

AP4 – Recognize that transparency, education and awareness are the keys to trust: The key factor of the two above approaches – the short notice/privacy nutrition label, and the Forward I, is that they are able to engage the user at very precise moments in the use of their personal information: the nutrition label, prior to, or at the time of collection, and the Forward I at the time of use. Transparency in these actions, and user education and awareness, are key to trust – which, in turn, is key to a lasting and productive business relationship between a technology/service provider and the user. Security and the protection of privacy is a key business enabler – this is what we call the Privacy Payoff.[27]

3.6 Users / Consumers

Control your data, and use the settings available to you

Key Messages:

- Take responsibility for your data – don't share it blindly;
- Engage the privacy protections provided to you;
- Determine your privacy preferences, and only engage with applications and technologies that respect them; and
- Respect the privacy of others.

U/C1 – Use the protections provided: While users may not have a direct connection with the design and creation of their mobile technology, they do retain some level of responsibility for appropriate use and control of their data stream. As much as developers, users should be proactive and use available preventative measures (*PbD* Principle 1), as protections are only as good as their use. Where privacy-protective defaults are in place, they must remain in place to provide protections. Where advice is given with respect to potential risks, it must be heeded to be effective. Where multiple privacy 'personas', parental settings or end-of-life protections are available, they must be used.

U/C2 – Be receptive to privacy messages from service providers or developers: In this roadmap, Device Manufacturers, Network Providers, OS/Platform Developers and Applications Developers are instructed to give users tools to protect privacy, and to assist users in the best possible manner by turning on privacy defaults, providing privacy wizards and explanations of the risks associated

[26] http://www.evidon.com/solutions/overview

[27] Cavoukian, A. and Hamilton, T. (2002) The Privacy Payoff: How Successful Businesses Build Consumer Trust. McGraw-Hill.

with personal information, and protecting that information upstream once it has left the user's direct control (*PbD* Principle 7: Respect the privacy of other users). Users, though, must ensure that they remain receptive to these messages, and make educated choices before changing privacy-protective defaults or releasing data to applications.[28] Developers and service providers are asked to return control, to the greatest extent possible, to the user – he or she must then exercise it.

4 Concluding Remarks

The future of privacy will be ensured by the adoption of *Privacy by Design*. Technology is advancing far too fast for compliance with regulatory schemes alone to be sufficient – strong legislative protections are necessary for the protection of privacy, but will not be enough. Digital information, once breached, is nearly impossible to recover. Thus, it is critical that protections be built directly, not only into technologies, but into the culture of entire industries – so that groups come to recognize privacy as a core functionality, and not just a problem to be overcome.

Above, we have presented a Roadmap for *Privacy by Design* in the mobile communications industry. To conclude, a few key messages should be reinforced. First, *PbD* is a collaborative effort. All parties have a role to play – both on their own, and in partnership with other developers. If a device does not allow for a given functionality, an OS/platform does not support it, or the user does not know about it, it will not be effective. Next, *Privacy by Design* is about the **initial** conditions of a given technology. This means that users should not have to set up new privacy features – privacy-protective defaults should already be in place and built in. But it also means that to the greatest possible extent, developers (of applications or platforms) should have access to built-in, on-device privacy features or interface elements. Embedding privacy into the 'building blocks' of a technology is as critical as offering privacy in the final, user-facing device.

Finally, we must remind all groups of the *7th PbD Foundational Principle* – respect for the privacy of users, and their right to control their personal information. Keeping the system user-centric, maintaining individuals' awareness, and allowing them to exercise choices over their data, will be the key to developing enduring trust – and ensuring that the mobile communications industry, or any other, is able to thrive well into the future, with privacy embedded into their devices.

[28] This includes data (photos, video, location, etc.) about other individuals that may be captured by a mobile device. Respect the privacy of others, and think before you post – seek consent before uploading personal information about them. See: http://www.ipc.on.ca/images/Resources/youthonline-madrid.pdf

About the Authors

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

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to proactively embed privacy into the design specifications of information technology and accountable business practices, thereby achieving the strongest protection possible. In October, 2010, regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark Resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection. This was followed by the U.S. Federal Trade Commission's inclusion of *Privacy by Design* as one of its three recommended practices for protecting online privacy – a major validation of its significance.

An avowed believer in the role that technology can play in the protection of privacy, Dr. Cavoukian's leadership has seen her Office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in numerous international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening consumer confidence and trust in emerging technology applications.

Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada, and is a member of several Boards including, the *European Biometrics Forum, Future of Privacy Forum,* RIM Council, and the *Ponemon Institute*. In 2009, Dr Cavoukian was reappointed as Commissioner for an unprecedented third term.

Marilyn Prosch, Ph.D., Associate Professor, Arizona State University, Co-Founder, ASU *Privacy by Design* Research Lab

Dr. Marilyn Prosch is a faculty member at Arizona State Univeristy, teaching principally in Accounting Information Systems and Data Protection. Prior to joining the ASU faculty, she was a faculty member at Lehigh University for 10 years. She serves on the AICPA/CICA Privacy Task Force which developed GAPP (Generally Accepted Privacy Principles). Her areas of interest include internal controls, accounting information systems, and data protection. Dr. Prosch holds the CIPP (Certified Information Privacy Professional) certification. She has met with, or spoken to, the U.S. Department of Commerce, U.S. Federal Trade Commission, National Association of Secretaries of State, and the Arizona Auditor General's Office on the subject of GAPP, as well as conducted various research studies on privacy breaches and GAPP.

www.privacybydesign.ca

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

***Privacy by Desig*n Research Lab**
Center for Advancing Business through IT
W.P. Carey School of Business
Arizona State University
P.O. Box 874606
Temple, Arizona
USA 85287-4606
Telephone: (480) 965-2280
Fax: (480) 956-5277
E-mail: CABIT@asu.edu

The information contained herein is subject to change without notice. The IPC, Arizona State University and the Privacy by Design Research Lab shall not be liable for technical or editorial errors or omissions contained herein.

December 2010

http://www.privacybydesign.ca

PRIVACY BY DESIGN RESEARCH LAB

Information and Privacy Commissioner,
Ontario, Canada