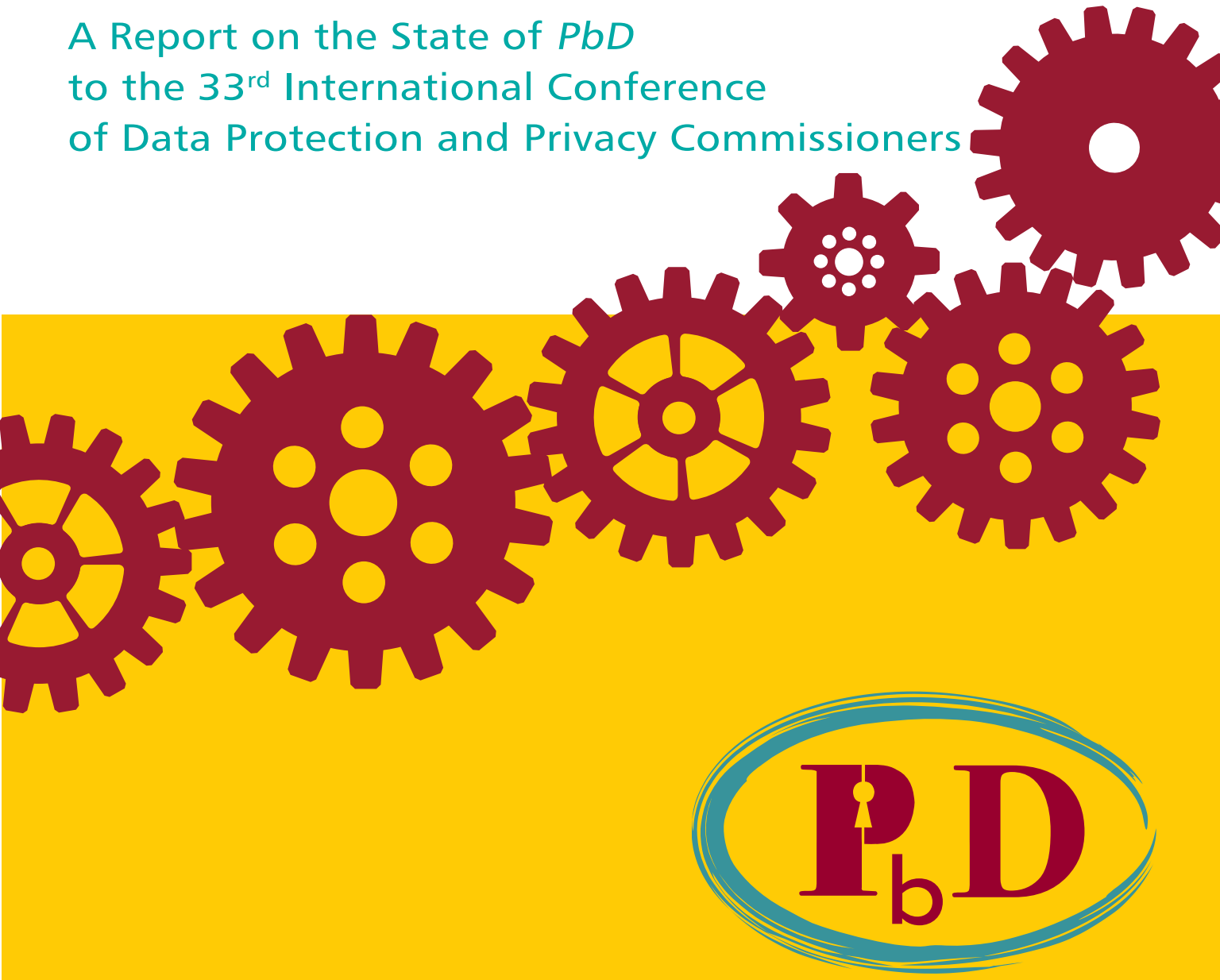
Privacy by Design

Strong Privacy Protection – Now, and Well into the Future

A Report on the State of *PbD*
to the 33rd International Conference
of Data Protection and Privacy Commissioners



Welcome...

In October 2010, International Privacy Commissioners and Data Protection Authorities unanimously passed a landmark resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection and encouraging its widespread adoption. As part of that resolution, we were invited to report back to the 33rd International Conference of Data Protection and Privacy Commissioners in 2011.

Privacy by Design: Strong Privacy Protection Now, and Well into the Future, is the Ontario Information & Privacy Commissioner's report on the developments that have transpired on the *PbD* front since the passage of the Resolution last year.

Those wishing to explore the milestones more fully are invited to consult the electronic version of this report, which contains links to additional information. It is available at www.privacybydesign.ca.

Table of Contents

Commissioner's Message

On the heels of last year's Resolution, *Privacy by Design* has now made it into the mainstream media. An article in Forbes magazine carried a remarkable headline announcing: "*Privacy by Design* is the New Corporate Hotness."

Clearly, despite the plaintive cries of the pundits, privacy is not dead – not by a long shot. We need look no further than consumer reactions to the growing number of privacy breaches. Privacy is, and remains, a social norm. Social networks facilitate the need to connect, but they change nothing with respect to our equally important need for privacy. Forbes, therefore, captures a critical sensibility – organizations that succeed in delivering their core functionality and protecting privacy will become the ones that consumers trust and seek out – the very essence of what they call "corporate hotness."

Today, we recognize that *Privacy by Design* is the key to meeting this goal and delivering this level of service. It is the gold standard in privacy protection, focusing, as it does, on taking a proactive approach, in an effort to prevent the privacy harm from arising. From a societal perspective, it is doubly-enabling in nature, satisfying the needs of business and consumers, governments and citizens. Little wonder then, that as privacy concerns increasingly take centre stage, application of the 7 Foundational Principles of *Privacy by Design* has become widespread. In fact, they have been translated into 23 different languages!

This year, more than any other, we have seen organizations operationalize the Principles of *Privacy by Design*. And this puts to rest another frequently-reported myth: that a focus on privacy will somehow stifle innovation. Nothing could be farther from the truth. In fact, if anything, the reverse is true – delivering on the promise of fully functional systems (including

strong privacy protection), demands the highest levels of innovation imaginable. And the good news is that early adopters reap significant advantages, giving them a desirable edge over their competitors.

As we move forward in the second decade of the 21st century, let us not limit ourselves by viewing the protection of personal information as solely a compliance issue. Rather, let us acknowledge that privacy has become, in and of itself, a foundational requirement – one co-mingled in the successful day-to-day operations of organizations.

The widespread accommodation of privacy as a core system requirement is poised to become one of the key trends of our time – and justifiably so. In the pursuit of freedom and liberty, as individuals and at a societal level, we deserve nothing less.

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

2011

Privacy by Design

Privacy by Design (*PbD*) represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches, after-the-fact. Alexander Dix, Berlin Commissioner for Data Protection and Freedom of Information, has, quite rightly, described such approaches as being akin to "locking the stable door after the horse has bolted."

By contrast, *PbD* is a *proactive* approach to privacy protection. It seeks to avoid data breaches and their attendant harm, instead of simply offering mechanisms for redress. This approach, based on 7 Foundational Principles, with its emphasis on positive-sum, win-win outcomes, continues to attract attention and gain support from around the world.

The 7 Foundational Principles

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 pretense 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 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.

Privacy by ReDesign: Extending the Principles

In 2011, *Privacy by Design* was extended to provide a framework for improving privacy protection in existing and legacy systems, where the opportunity to embed privacy from the outset had long passed. *Privacy by ReDesign* (*PbRD*) was introduced in a white paper co-authored with Dr. Marilyn Prosch, a professor at Arizona State University[1], and is expected to have a significant impact on the privacy landscape.

PbRD: A 3-Step Process

Rethink: review existing risk mitigation strategies and systems, and consider alternatives that will be privacy-protective. 1

ReDesign: develop and enable improvements in the system that will deliver the original functionalities intended, along with privacy, in a doubly-enabling, positive-sum strategy. 2

Revive: launch the newly improved, privacy-protective system, having effectively transformed the earlier one. 3

PbRD is a transformative process which offers a framework for undertaking a proactive assessment of existing gaps in how an organization manages personal information and addresses those gaps systematically. The 7 Foundational Principles are applied, not as goals for a nascent system, but as the end result of a *PbRD* transformation.

While both *PbD* and *PbRD* seek to restore control to users, they are, at their core, business-friendly approaches to privacy protection, helping to position privacy as a cost-reducing, business advantage, not a labour-intensive, regulatory burden.

To learn more...

Privacy by ReDesign: Building a Better Legacy, May 2011.

Privacy by Design: From Policy to Practice, September 2011.

Privacy by ReDesign: A Practical Framework for Implementation, November 2011.

1 Arizona State University created the first *Privacy by Design* Research Lab in November, 2009.

Privacy by Design: An International Perspective

Since the unanimous passage of the *Privacy by Design* Resolution at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem, the momentum of *PbD* has grown steadily.

Considerable advocacy for *Privacy by Design* has taken place within the European Union since 2008 – notably by the European Data Protection Supervisor and the U.K. Information Commissioner's Office. *PbD* has especially figured prominently over the course of the past year. Vice President of the European Commission Viviane Reding observed that *PbD* "will lead to better protection for individuals." As well, in his *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, Peter Hustinx recommended that the European Commission include a general provision on including *Privacy by Design* in the legal framework for data protection. Since then:

- In November 2010, the European Commission released its *Comprehensive approach on personal data protection in the European Union*, which pointed out the important role that *PbD* will play in ensuring data controllers meet their responsibilities.

- The Czech Data Protection Authority endorsed European Union privacy reforms, which they believe will be characterized by "*Privacy by Design*, responsibility and accountability."

- Early in 2011, the Dutch senate, while debating biometrics, identified the need for strong privacy protection to be embedded in appropriate

systems. Max Snijder, the Managing Director of the European Biometrics Group described creating "the first *PbD*-certified consulting method for biometric identity systems" as a key objective.

- Also early in the year, Kirsten Bock and Martin Rost of the Office of the Data Protection and Freedom of Information Commissioner of Schleswig-Holstein, endorsing *PbD*, developed "6 Fundamental Data Protection Goals" which are designed to add additional clarity and rigour to the approach.

- The European Commission recognized that a *PbD*-approach to the European Smart Grid was required. Further, such an approach has also been recommended by a number of other organizations, including: the Article 29 Working Group; the Smart Grid Expert Group 2; the Data Protection Commissioners of the Federation and of the Länder (Germany); and, the Trans-Atlantic Consumer Dialogue.

- In April, the EU RFID Privacy and Data Protection Impact Assessment (PIA) Framework was announced. It is a landmark *Privacy by Design* document that proactively addresses concerns about ubiquitous embedded RFID tags in the emerging "Internet of Things" in a positive-sum, win-win manner. The Framework is notable for being one of the world's first sectoral PIA guidance documents developed by industry and, upon implementation, will be recognized by EU regulatory authorities as evidence of compliance with EU privacy law, with global reach.

Similarly, in the United States, numerous regulatory agencies and legislators have begun to call for a *PbD*-based approach to privacy protection. Notable examples include:

- Last December, the Federal Trade Commission issued a consultation paper on *Protecting Consumer Privacy in an Era of Rapid Change*, which identified *PbD* as one of three key recommendations regarding its proposed privacy framework for online and offline commercial entities.

- Many agencies and regulators associated with the U.S. Smart Grid have also recognized the importance of incorporating *PbD* into this critical architecture, including:

    - the National Institute of Standards and Technology (NIST), in August, 2010
    - the Public Interest Energy Research (PIER) program, (at the University of California, Berkeley), in November, 2010
    - the California Public Utility Commission (CPUC), in July, 2011

- Several pieces of legislation have also been proposed which include the principles of *PbD*, including:

    - the Kerry/McCain *Commercial Privacy Bill of Rights*, proposed in April and which was the first to name *Privacy by Design* within a Bill itself
    - the Franken/Blumenthal *Location Privacy Protection Act*, proposed in June
    - the Wyden/Chaffetz *Geolocation and Privacy Surveillance Act*, also proposed in June

The 7 Foundational Principles have been translated into 23 different languages, including:

1. English
2. French
3. German
4. Italian
5. Spanish
6. Czech
7. Dutch
8. Estonian
9. Hebrew
10. Hindi
11. Chinese
12. Japanese
13. Arabic
14. Armenian
15. Korean
16. Ukranian
17. Russian
18. Romanian
19. Portugese
20. Maltese
21. Greek
22. Macedonian
23. Bulgarian

Other *PbD* developments, from around the world, since the time the Resolution was adopted, include:

- Early in 2010, in its report entitled, *30 Years After: The Impact of the OECD Privacy Guideline*, the OECD wrote that *Privacy by Design* should be introduced into the new

European data protection framework. Further, they wrote that it should be binding not only on data controllers, but also on technology designers and producers.

- In New Zealand, after the Law Commission's review of that country's Privacy Act in August, Commissioner John Burrows noted that, among other things, Privacy Commissioner Marie Shroff's Office would be well-served by instituting several "expert panels" which would advise on technical matters, especially *Privacy by Design*.

- Yoram Hacohen, Head of the Israeli Law, Information and Technology Authority (ILITA) recently authorized Google to operate its Street View cars in public areas and to include the photos in Google Maps. Following the Principles of *PbD* was one of the five conditions that Google was required to follow.

- Seeking reviews of its draft privacy law, in July, the government of Qatar has asked for comment regarding the notion of including *Privacy by Design* as a key legislative principle.

- The GSM Association (GSMA), an international group of mobile operators and related companies, published their Mobile Privacy Principles, which describes a framework intended to foster a *PbD* approach to privacy in the mobile device environment.

Institutions have played an important role in advancing the adoption of *Privacy by Design*. Nonetheless, the work of a cadre of individuals, called *PbD* Ambassadors, is especially worthy of recognition. Among the Ambassadors are many Data Protection Authorities and Privacy Commissioners who have been recognized for their ongoing support of *PbD*. This group includes: Dr. Alexander Dix; Yoram Hacohen; Peter Hustinx; Peter Schaar; and Marie Shroff.

While space prevents acknowledgement of each Regulator's accomplishments, a sample of the work of several Ambassadors from outside of the regulatory community will spotlight some of the types of advances being made every day. These include:

- Malcolm Crompton – the first Australian Privacy Commissioner and now Managing Director of Information Integrity Solutions Pty Ltd. maintains a robust public speaking and consulting pace and consistently advocates for a *PbD* approach across multiple domains, arguing that laws alone cannot solve the current day challenges that face privacy.

- Nicola Fabiano – a noted attorney from Italy and one of the first international *PbD* Ambassadors has undertaken a true "grass roots" approach to advocacy through numerous presentations and by writing extensive articles targeting fellow lawyers.

- Chris King – the Chief Regulatory Officer, eMeter Corporation, is an outspoken advocate of *PbD* within the Smart Grid. Embracing Dr. Cavoukian's exhortation that everyone has a responsibility to identify challenges to privacy, he advocates "constant vigilance" and has begun to identify issues in the broader privacy landscape.

- Dr. Hossein Rhanama and Steven Johns – members of Ryerson University's renowned Digital Media Zone, are staunch advocates of *PbD*, who work tirelessly to ensure that the student entrepreneurs developing high technology solutions within this unique environment understand the commercial importance of building privacy into their work, right from the outset.

- Professors Dimitris Hatzinakos, Kostas Plataniotis and George Tomko – the Chair, Academic Director, and Expert-in-Residence, respectively, of the Identity, Privacy and Security Initiative (IPSI) at the University of Toronto. *PbD* is a core tenet in the organization's goal to develop new approaches to security that maintain the privacy, freedom and safety of the user and the broader community.

- Larry Keating – the President of No Panic Computing, has long practised the principle of building privacy and end-to-end security directly into the technology he has created. He actively shares his privacy experiences with a variety of target audiences in the public, financial, not-for-profit and small business sectors.

- His Highness Prince Fahad bin Faisal Al Saud – who is working to build awareness of *PbD* in Saudi Arabia. He believes that embedding privacy into technology is a critical element of properly serving the needs of users in the Middle East.

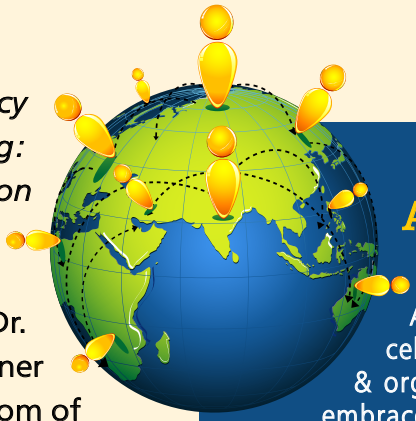
The IPC, as part of its long-standing program of outreach, also works with institutions around the world to advance *Privacy by Design*. Building on its success with Smart Grid stakeholders in Ontario, two international projects are currently underway:

- A joint paper entitled, *Privacy by Design and Smart Metering: Minimize Personal Information to Maximize Privacy – Data Minimization at its Best*, has been undertaken with Dr. Alexander Dix, the Commissioner for Data Protection and Freedom of Information in Berlin, Germany.

- The IPC announced a new partnership with a U.S. utility – San Diego Gas & Electric (a division of Sempra) to embed *Privacy by Design* into their Smart Meter dynamic pricing system

Representatives from many countries and organizations have visited the IPC to learn more about *Privacy by Design*. Over the past year, we have been honoured to host delegations from China, Japan, South Korea, Singapore, and Brazil.

Judging from this overview of *PbD* milestones, it has clearly been a busy year for *Privacy by Design* on the international stage, as it has been in Ontario.



PbD Ambassadors

The *PbD* Ambassador program celebrates individuals & organizations that have embraced *Privacy by Design*.

There are two types of Ambassadors:

Individual Ambassadors are staunch advocates of *PbD*, and reflect a wide variety of accomplishments, skill sets and cultures. Many have led successful implementations within their companies or have architected *PbD* into their firm's product line. Today, there are almost 70 Individual Ambassadors, representing almost a dozen countries. And we are always on the lookout for more!

Organizational Ambassadors are companies or teams that have embedded *PbD* in their day-to-day operations.

If you would like to join the Ambassador program, we want to hear from you!

Please visit www.privacybydesign.ca and follow the nomination instructions.

Privacy by Design: Ontario Activities

This year, the Office of the Information & Privacy Commissioner of Ontario, Canada, has focussed considerable energy on advancing *PbD* in cutting-edge technologies and applications, and on leveraging partnerships to help shape the future of privacy.

Some of the key areas worked on are listed below; for a more complete picture, see www.privacybydesign.ca.

Smart Meters and the Smart Grid

The first IPC paper on privacy in the Smart Grid was written in 2009 with Jules Polonetsky and Christopher Wolf, Co-Chairs of the Future of Privacy Forum. Since then, this area has exploded, and we have been asked to present the *PbD*/Smart Grid story at dozens of utility conferences throughout the United States, Canada and Europe. At the 32nd International Conference of Data Protection and Privacy Commissioners, the IPC hosted a pre-conference session sharing its work on *PbD* in the Smart Grid. We have continued to publish in this area, paving the way for utilities around the world to embed privacy directly into the design of the Smart Grid, from the outset.

To learn more...

SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. November 2009.

Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid. June 2010.

Operationalizing Privacy by Design: The Ontario Smart Grid Case Study. February 2011.

Utilities and regulators have developed a keen awareness of the importance of building privacy directly into the Smart Grid over the past year. Importantly, the US National Institute of Standards and Technology's (NIST) Smart Grid Privacy

Working Group endorsed *Privacy by Design* in their report entitled, "*NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*." The European Commission's Smart Grid Task Force also recommended *Privacy by Design* for the European Smart Grid.

Mobile Devices

This past year, in a joint paper with the Arizona State University *PbD* Research Lab, we considered the roles of different actors in the mobile communications ecosystem with regard to protecting privacy. Working with device manufacturers, operating system/ platform developers, service providers, application developers and end-users, we developed a roadmap for *Privacy by Design* within the mobile communications industry.

To learn more...

The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users. December 2010.

Wi-Fi Positioning Systems: Beware of Unintended Consequences – Issues Involving the Unforeseen Uses of Pre-existing Architecture. June 2011.

Among the important lessons that emerged from that exercise were the recognition that *PbD* is, by necessity, a team sport, and that those early in the value chain (e.g. manufacturers and operating system developers) must embed privacy into mobile devices from the outset to provide the foundation for those later in the chain (e.g. service providers and application developers).

In a joint paper with renowned digital identity expert Kim Cameron, we also examined the unintended consequences for privacy that arise from tracking individuals' geolocation data through their mobile devices. We found that applying *PbD* to the treatment of Media Access Control (MAC) addresses and other mobile device identifiers will ensure greater protection of user privacy, while meeting consumer demand for location-based technologies — truly a win-win strategy.

Health Information

Research based on health information can yield vitally important insights, but traditional methods of de-identification produce zero-sum outcomes, since the techniques that alter or remove potential identifiers also inevitably diminish the quality of the information used for research purposes.

Working with data anonymization expert, Dr. Khaled El Emam, a Canada Research Chair in Electronic Health Information at the University of Ottawa, the IPC documented an approach that combines strong de-identification techniques with re-identification risk measurement approaches to produce high data quality and a high degree of privacy — another win-win!

To learn more...

Sensors and In-Home Collection of Health Data: A Privacy by Design Approach. August 2010.

Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy. June 2011.

Sensors in health-care monitoring devices also hold the potential for enormous social benefit. Their capacity to collect detailed personal health information, however, demands close examination.

Working with the Intelligent Assistive Technology and Systems Lab at the University of Toronto, the IPC discovered that *PbD* provides an ideal foundation for protecting privacy in this area. In particular, focusing on what data collection and disclosure is necessary and acceptable from the individual's perspective, from the outset, results in privacy being protected with minimal effort from the patient. This helps to assure individuals whose health is being monitored that their information will not be put to any inappropriate use, increasing their trust in the application.

Digital Marketing

The use of personal information for targeted marketing communications has been a significant issue this past year. Working with industry partners, the IPC has looked at contextual (based on a user's current action) and geographical (based on the user's location) targeting.

Digital Out of Home (DOOH) represents a fast-growing form of in-store, video-based, digital advertising that employs image sensors to display relevant ads based on the gender and approximate age range of consumers watching the screen. Embedding privacy directly into the system from the outset, Intel's Anonymous Video Analytics system logs non-identifiable data (e.g. number of visitors and ads viewed) and destroys images as soon as the appropriate demographic determination has been made. This positive-sum approach yields useful metrics for advertisers and helps to increase the probability that the messages presented are potentially useful to consumers. No personal data is collected or retained.

Geo-targeting has also benefitted from the application of *PbD* Principles, through the development of an anonymous approach by a Canadian company, Bering Media. Designing privacy in from the outset, Bering Media has developed an architecture that allows Internet Service Providers, who have precise knowledge of user location, to work with ad serving companies, who understand which ads are to be directed to users at particular locations, without either party needing to be aware of the information held by the other. This exceptional outcome — precise targeting of ads without any disclosure of personal information — is a strong affirmation of the *Privacy by Design* approach.

To learn more...

Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising. October 2010.

Anonymous Video Analytics (AVA) Technology and Privacy. April 2011.

Biometric Encryption

Among the various approaches to authenticating identity, biometrics is increasingly being viewed as the ultimate means of verification and identification. Biometric Encryption (BE) uses *Privacy by Design* to directly address the privacy and security concerns associated with biometric systems. It is a process that securely extracts a key from a biometric, such that neither the key nor the biometric can be retrieved from the "helper data" created by the process and stored by the application. In this sense, the key is "encrypted" by the biometric and can only be decrypted upon presentation of the correct live biometric sample for verification. No biometric template or actual representation of the biometric is retained.

In the summer of 2007, the Ontario Lottery and Gaming Corporation (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 OLG's opt-in, voluntary "self-exclusion" program — comprising a "watch list" of approximately 15,000 problem gamblers who wished to be excluded from OLG gambling sites. Although the program was entirely voluntary, the increased use of facial recognition technology raised a number of privacy and security concerns. The OLG and IPC agreed that only the application of BE to the proposed facial recognition system would satisfy the multiple needs of both the self-excluded program *and* privacy.

To learn more...

Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept. November 2010.

Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy. March 2007.

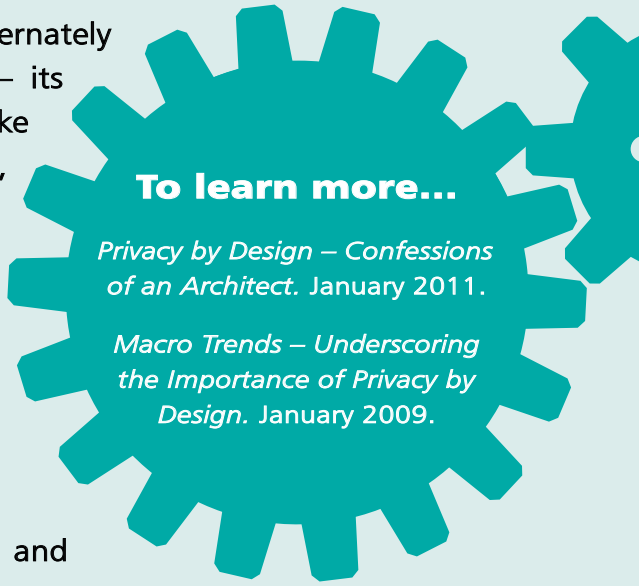
The system was developed by a collaborative team consisting of: OLG; IPC; members of the University of Toronto's Computer Engineering Department; and, incident reporting and biometrics firm, iView Systems. Successfully piloted in late 2010, this use of BE was shown to enhance patron privacy (both those on the watch list and regular patrons), system security and overall accuracy of the watch list system within

the context of the self-exclusion program. The system is currently in place and fully operational in most of the OLG's 27 gaming sites.

"Big Data"

At its best, "big data" promises new opportunities to identify insights by analyzing the mountains of data created every day. At its worst, it raises the spectre of widespread surveillance.

It is an emerging technology and it looms, alternately menacingly and seductively, on the horizon — its widespread adoption rushing toward us like an oncoming train. As privacy professionals, we cannot ignore its implications. It is thus incumbent that we "get in front of it" and introduce privacy solutions. Enter *Privacy by Design*.



"Big data" generally refers to a wide variety of data, including data gathered through:

- The ever-increasing number of sensors and surveillance cameras;
- GPS on mobile applications;
- Tweets, blog posts, and social media updates;
- Images and video on popular sharing sites; and,
- Online purchases, in-store debit and credit transactions and banking history.

The potential benefits of data analytics are far-ranging. Jeff Jonas, IBM Distinguished Engineer and Chief Scientist, IBM Entity Analytics, suggests that it can provide assistance in a number of areas — improved pandemic response,

helping drivers with just-in-time route information for optimized traffic flows, helping optimize online experiences, to name just a few.

So, will big data mean the end of privacy? No. In fact, systems that respect consumers' information, with privacy assured from the outset, could serve to increase user confidence and trust, encouraging higher rates of engagement, in turn, yielding greater benefits for *all* system stakeholders.

A "personal data ecosystem" movement and associated industry, including members such as Michael Fertik, CEO of reputation.com and others, has already emerged to help consumers to benefit directly from the consensual use of their personal information.

Regulatory Innovation

Regulators and policy-makers around the world are starting to talk about *Privacy by Design*, and how its Principles may be incorporated into policy, regulatory frameworks and voluntary codes.

To learn more...

Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers. August 2011.

A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight. November, 2009.

Incorporating *PbD* into policy, law, and practice requires an approach to privacy that is both broader, and yet more flexible than traditional ones. Ultimately, its aim is to have privacy woven directly into business processes in much the same way that other core values such as fairness, transparency, and proportionality, are. This requires embedding privacy at a much deeper level than ever before — at the actual level of code, default settings, and operating systems.

Legislators and policy-makers have a range of vehicles at their disposal to help support the widespread implementation of *Privacy by Design*. What is needed now is substantive dialogue

and innovation within the privacy and regulatory arenas, supporting meaningful privacy protection through these vehicles, while also encouraging creativity and innovation, now, and well into the future.

SmartData

The IPC has also been involved in the development of the next evolution in data protection — "SmartData." Working with its creator Dr. George Tomko, IPSI, and a number of international researchers, this project represents the future of privacy and the ultimate control of personal information. SmartData represents embodied, virtual agents that will act as an individual's proxy online, securely storing one's personal information and intelligently disclosing it based on the context of the data requests, in accordance with instructions authorized by the data subject. This technology surpasses current limited approaches to Artificial Intelligence (AI) through its capacity to respond to unforeseen situations, adapt to novel threats, and provide a nuanced and accurate representation of an individual's privacy and data security preferences — returning control of the data to the data subject, where it belongs!

SmartData is the strongest possible expression of *Privacy by Design*. The individual benefits greatly, by regaining control of his or her personal information without having to assume the burden of constantly exercising that control for each data request. Moreover, unlike many systems which aim to protect data, SmartData enables the data to protect itself. By designing privacy directly into the data, it is necessarily designed into all transactions involving that data!

The major kick-off event for this project will be the IPSI SmartData International Symposium, a 3-day conference that will take place at the University of Toronto, June 4 – 6, 2012. This Symposium received funding and recognition by the Connaught Global Challenge, which focuses on bringing leading researchers from multiple disciplines together with innovators and thought leaders, in an effort to contribute to the advancement of solutions to a "critical issue facing humanity in the 21st century" — a recognition of the vital importance of protecting privacy in the years to come.

A Call to Action

So much has been accomplished, yet so much remains to be done.

Last year, I predicted, "The world has less than a decade to make the protection of personal information and online privacy a priority before the concepts are lost forever…" Surveying what has taken place in the past year, I feel much more optimistic about the future of privacy. We have made tremendous progress.

But we cannot rest — our work has just begun. We must capitalize on the momentum that is building and continue to press for change within each of our countries, jurisdictions and organizations.

To my fellow regulators: so many of you have advanced the promise of *Privacy by Design* within your jurisdictions. I urge you to continue to increase public awareness and encourage leaders to embed its Principles into your legislation, regulations and industry standards.

To business leaders: your active support of privacy within your organizations is invaluable. You create a culture of privacy that provides the fertile ground in which the seeds of *PbD* will take root. Recognize that the protection of personal information is not merely an altruistic exercise — it is one which promises to give you a sustained competitive advantage.

To academics: the future is in your hands. Many of you have begun teaching privacy and *PbD* within your curriculums. Thank you! In practice, the execution of *Privacy by Design* is truly a multi-disciplinary activity — if you have not yet done so, please consider adding it. And urge your institutions to commit to providing resources necessary to begin and maintain critical research within this domain.

To privacy professionals: keep up the good work! Your day-to-day efforts serve as a bridge between users and developers, or customers and providers, yielding the spark of innovation necessary to elicit positive-sum outcomes. I urge you to

make a special effort to reach out to constituencies for whom privacy is not as familiar a concept — developers, engineers, and designers, to name a few.

In fact, I strongly believe that it is critical to reach those who design and build the systems and technology upon which we increasingly rely — so much so, that I have called this "*The Year of the Engineer*." In addition to bringing the *Privacy by Design* message to engineers and developers at dozens of the world's most innovative "tech" firms, I look forward to working with the Canadian Information Processing Society (CIPS) to introduce a level of "engineering precision" to the 7 Foundational Principles of *PbD*. As a group, such professionals play a highly influential role in how personal data is managed. As it has proven beneficial to translate the Principles into a variety of national languages, I think we do ourselves a disservice by failing to speak the language that these individuals use in their respective trades and professions.

Each of us must commit to taking a leadership role to ensure that privacy is considered and embedded from the outset, in virtually any work involving personal information. We cannot sit idly and allow hard-fought privacy rights to disappear through complacency or lack of understanding. To paraphrase an oft-repeated maxim, "All that is necessary for the triumph of unsanctioned disclosure is that good men [and women] do nothing." Let that not be our legacy.

My Office remains committed to advancing the understanding of the application of *Privacy by Design* internationally. With nothing less than freedom at stake, the stakes are very high — too high to ignore.

Sincerely yours,

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

Appendix I: Individual *PbD* Ambassadors

Dr. Parry Aftab		Dr. Khaled El Emam	
Joseph Alhadeff		John Ellingson	
Martin Abrams		Nicola Fabiano	
Prince Fahad bin Faisal Al Saad		Mark Fabro	
Dr. Stefan Brands		Michael Fertik	
Dra. Ana Brian Nougreres		Anita Fineberg	
Dr. Jacques Bus		Natalie Fonseca	
Dr. L. Jean Camp		Victor Garcia	
Malcolm Crompton		Eduard Goodman	
Myles D'Arcey		Robin Gould-Soil	
Michelle Dennedy		Daniel Guagnin	
Dr. Alexander Dix		Yoram Hacohen	

Appendix I: Individual *PbD* Ambassadors (continued)

Dr. Dimitris Hatzinakos		Larry Keating	
Michael Ho		Chris Kelly	
David Hoffman		Chris King	
Jane Horvath		Jeff Kirke	
Peter Hustinx		Stephen Lau	
Pat Jeselon		Hovanes Manucharyan	
Stephen Johns		Thomas Marinelli	
Robert Johnson		Dr. Karl Martin	
Nandini Jolly		Gene McLean	
Jeff Jonas		Terry McQuay	
Krista Jones		David Nicholl	
The Honorable Pamela Jones Harbour		Harriet Pearson	

Appendix I: Individual *PbD* Ambassadors (continued)

Dr. Kostas Plataniotis		Dr. Jean-Pierre Seifert	
Jules Polonetsky		Marie Shroff	
Sharon Polsky		Arthur Smith	
Claudiu Popa		Max Snijder	
Norine Primeau-Menzies		Rick Stephens	
Dr. Marilyn Prosch		Scott Taylor	
Dr. Hossein Rahnama		Dr. Omer Tene	
Dr. Kai Rannenberg		The Honorable Mozelle Thompson	
Doron Rotman		Dr. George Tomko	
Peter Schaar		Michael Winters	
Yosi Schneck			

Appendix II: A *Privacy by Design* Chronology

DATE		EVENT / CITATION / PAPER	SUBJECT AREA
2011	NOV.	 "*Privacy by ReDesign*: A Transformative Process" pre-conference session held at the 33rd International Conference of Data Protection and Privacy Commissioners in Mexico City.	*PbRD*
	OCT.	 San Diego Gas & Electric partners with IPC to embed *PbD* into their Smart Meter dynamic pricing system.	Smart Grid
	SEPT	 IPC teams with Berlin DPA to write: *Privacy by Design and Smart Metering: Minimize Personal Information to Maximize Privacy – Data Minimization at its Best*.	Smart Grid
	AUG.	 Street View is permitted to operate in Israel, but must follow principles of *Privacy by Design*, among other requirements.	International
	AUG.	 New Zealand Law Commissioner recommends the Privacy Commissioner establish an expert panel to advise regarding *Privacy by Design.*	International
	AUG.	 Czech Republic endorses EU reforms which they expect will be characterized by, "*Privacy by Design*, responsibility and accountability."	International
	JUL.	 California Public Utility Commission recognizes *PbD* as a promising approach.	Smart Grid
	JUL.	 Qatar seeks views on whether its draft privacy legislation should inlcude reference to "*Privacy by Design*."	Regulatory

Local International Milestone White Paper Event

Appendix II: A *Privacy by Design* Chronology (continued)

DATE		EVENT / CITATION / PAPER	SUBJECT AREA
2011	JUN.	 White Paper defends use of proper de-identification techniques as a tool in the protection of privacy.	Health
	JUN.	 White Paper warns of "unintended consequences" associated with use of Wi-Fi enabled mobile phones. Highlights *PbD* approach as a technique to identify and avoid unintended uses.	Mobile
	JUN.	 OLG launches Biometrically Encrypted facial recognition system at casinos throughout Ontario.	Biometric Encryption
	MAY	 The concept of "*Privacy by ReDesign*" is introduced.	*PbD*
	APR.	 *PbD* Principles applied in the practice of a targetted advertising approach - Anonymous Video Analytics.	Marketing
	APR.	 Voluntary guidelines adopted in EU addressing the data implications of smart (RFID) tags.	RFID
	APR.	 U.S. Senators Kerry & McCain cite *PbD* in their proposed "Commercial Bill of Rights" legislation.	Regulatory
	FEB.	 The GSM Association (GSMA) publishes Mobile Privacy Principles and identifies *PbD* as a key dimension.	Mobile

Local International Milestone White Paper Event

Appendix II: A *Privacy by Design* Chronology (continued)

DATE		EVENT / CITATION / PAPER	SUBJECT AREA
2011	FEB.	White paper discusses application of *PbD* in the provincial hydro utility's Smart Grid implementation.	Smart Grid
	FEB.	Dutch senate debates data protection and considers need for *PbD*.	Regulatory
	JAN.	IBM announces "IBM InfoSphere Sensemaking - a comprehensive information integration platform incorporating the Principles of *PbD*.	Big Data
	JAN.	Commissioner Cavoukian hosts the third annual celebration of international Data Privacy Day - "*Privacy by Design*: Time to Take Control."	*PbD*
2010	DEC.	A roadmap for *PbD* in the mobile communications space is described, outlining practical steps that can be taken by all players in the industry (Device Manufacturers, Operating System and Platform Developers, Network Providers, Application Developers, and Users) to build-in privacy protections	Mobile
	DEC.	The U.S. FTC issues "Protecting Consumer Privacy in an Era of Rapid Change."	Regulatory
	NOV.	European Commission releases significant proposals for privacy changes.	Regulatory
	NOV.	*PbD* Principles applied to biometric identification of "self-excluded" gamblers.	Biometrics

Local International Milestone White Paper Event

Appendix II: A *Privacy by Design* Chronology (continued)

DATE		EVENT / CITATION / PAPER	SUBJECT AREA
2010	OCT.	*PbD* Resolution is unanimously passed by the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem.	Regulatory
	OCT.	The IPC's work on *Privacy by Design* in the Smart Grid is shared with international colleagues at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem.	Smart Grid
	OCT.	*PbD* employed in a privacy protective approach to IP geolocation-oriented, targeted advertising.	Marketing
	AUG.	*PbD* Principles applied to the sensor-based collection of Personal Health Information.	Health
	AUG.	NIST (National Institute of Standards and Technology - U.S. Department of Commerce) identifies the need to build privacy protections into systems and processes.	Smart Grid
	AUG.	Springer publishes a special *Privacy by Design* issue of "Identity in the Information Society."	*PbD*
	JUN.	Development of a set of "Best Practices" regarding privacy in the Smart Grid. Based on the 7 Foundational Principles of *Privacy by Design.*	Smart Grid
	JUN.	A *Privacy by Design* approach to modelling cloud computing architecture without compromising privacy is described.	Cloud

Local International Milestone White Paper Event

Appendix II: A *Privacy by Design* Chronology (continued)

DATE		EVENT / CITATION / PAPER	SUBJECT AREA
2010	MAY	 The IPC releases a foundational work providing insight into the general application of the 7 Foundational Principles of *Privacy by Design* as well as their relationship to the GPS FIPs.	*PbD*
	MAY	 The European Data Protection Supervisor recommends *PbD* be included in the data protection legal framework.	Regulatory
	APR.	 The Principles of *PbD* are considered in the context of a risk management framework.	Risk Managment
	APR.	 A report on the application of the Principles of *PbD* to the Ontario Health Study Assessment Centres is released.	Health
	MAR.	 A tool to appropriately de-identify Personal Health Information is presented.	Health
	MAR.	 The European Data Protection Supervisor endorses *PbD* as a "key tool" for creating consumer trust in ICT	Regulatory
	JAN.	 Commissioner Cavoukian hosts the second annual celebration of international Data Privacy Day - "*Privacy by Design*: The Gold Standard."	*PbD*
	JAN.	 Vice President Viviane Reding asserts importance of *PbD* in protecting individuals.	*PbD*

Local International Milestone White Paper Event

Appendix II: A *Privacy by Design* Chronology (continued)

DATE		EVENT / CITATION / PAPER	SUBJECT AREA
2009	DEC.	IPC contributes a chapter on Biometric Encryption to the Springer Encyclopedia of Biometrics.	Biometrics
	DEC.	The Center for Democracy and Technology endorses *PbD*	*PbD*
	NOV.	The role of *PbD* with respect to organizational accountability and the creation of strong business practices is discussed.	*PbD*
	NOV.	Announcement of the Arizona State University *Privacy by Design* Research Lab	*PbD*
	NOV.	Initial paper describing potential applications of *Privacy by Design* to emerging Smart Grid architectures is released.	Smart Grid
	NOV.	Use of a commercial risk management tool is described which results in business processes that are consistent with *PbD*.	Risk Managment
	NOV.	*Privacy by Design* is formally shared with international privacy colleagues at the 31st International Conference of Data Protection and Privacy Commissioners in Madrid.	*PbD*
	AUG.	The 7 Foundational Principles of *Privacy by Design* - those forming the basis of the "Jerusalem Resolution" - are set out.	*PbD*

Local International Milestone White Paper Event

Appendix II: A *Privacy by Design* Chronology (continued)

DATE		EVENT / CITATION / PAPER	SUBJECT AREA
2009	JAN.	 Commissioner Cavoukian hosts the first annual celebration of international Data Privacy Day - "The *Privacy by Design* Challenge."	*PbD*
	JAN.	 The Origins of *PbD* are documented.	*PbD*

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

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

416-326-3333
1-800-387-0073
info@ipc.on.ca
IPC: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca