Privacy by Design by Regulation: The Case Study of Ontario

Avner Levin*

This article presents the findings of a case study examining the role of the regulator in facilitating Privacy by Design ("PbD") solutions. With the introduction of PbD into the new European Union General Data Protection Regulation, *it is important to understand the conditions under which PbD can succeed and the role which regulators can play (if at all) in promoting such success. Two initiatives with similar technology are examined: first, a PbD success, the introduction of facial recognition technology into existing cameras in casinos in Ontario, and second, a PbD failure, the expanded deployment of cameras within the public transit system of Toronto. The findings are organized into three overarching themes: PbD-focused findings, leadership and organizational findings, and regulator-focused findings. The article argues that privacy continues to persist as an engineering problem despite PbD, that (related to that) there is growing recognition of privacy as an issue of organizational change and leadership, and consequently, that the role of the regulator must evolve if PbD is to become a meaningful regulatory tool, an evolution that carries with it both risks and opportunities for privacy.*

* Professor, Law & Business Department, Ted Rogers School of Management, Ryerson University. This paper was supported by a research grant from the Blavtanik Interdisciplinary Cyber Research Center, Tel Aviv University. Many thanks to Professor Michael Birnhack of the Buchmann Faculty of Law, Tel Aviv University for leading this research project and for the fruitful discussions we had on privacy by design and to Michelle Chibba of the Privacy & Big Data Research Institute at Ryerson University for her invaluable research support and her contribution to the many drafts of this paper.

I. Introduction

This paper presents the findings of a case study examining the role of the regulator in facilitating Privacy by Design solutions. PbD is an approach to privacy which urges organizations to design privacy into new initiatives rather than deal with privacy as an after-the-fact "problem". The approach has been embraced by many, but executed by few, for a number of reasons, such as the difficulty in translating the idea of PbD into engineering algorithms. With the introduction of PbD into the new European Union *General Data Protection Regulation*[1] ("*GDPR*"), it is important to understand the conditions under which PbD can succeed, and the role regulators can play (if at all) in promoting such success.

This case study contributes to this understanding by examining the Province of Ontario, Canada, and the role of its Information and Privacy Commissioner in two PbD initiatives. Ontario was not chosen at random. Its Privacy Commissioner at the time the initiatives were taking place, Dr. Ann Cavoukian, was a champion of PbD. Cavoukian tirelessly and passionately promoted PbD both domestically and internationally, and outcomes such as the 2010 Jerusalem Declaration of Privacy Commissioners in support of PbD and the inclusion of PbD in the new *GDPR* can largely be attributed to her advocacy.

This case study wishes to examine the role the Commissioner played as a regulator and whether the conduct of the regulator had any bearing on the success or failure of PbD. The two initiatives that are examined are the introduction of facial recognition technology into existing cameras in casinos in Ontario, an initiative that is generally lauded for the success of PbD, and the expanded deployment of cameras within the public transit system of Toronto, in which PbD did not take hold. Since, in both instances, the potentially intrusive technology and its potential PbD solution were similar, the case study is able to focus on the role of

1. EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1, art 25(1) [*GDPR*].

the regulator and the regulator's impact with greater certainty.

The paper is divided into the following sections. After this first introductory section, it discusses and introduces PbD, its principles, and its evolution, leading in the second section to its incorporation into regulatory frameworks. The second section also reviews engineering challenges to the application of PbD and other relevant criticisms of PbD. The third section provides the methodology and the details of the case study and how the interviews conducted during the case study were analyzed to arrive at the findings of this paper. The fourth section then sets out the findings. Finally, the fifth section draws conclusions from the findings in three main areas: the persistence of privacy as an engineering problem, the growing recognition of privacy as an issue of organizational change and leadership, and consequently, the evolution of the role of the regulator with some thoughts as to how PbD can best flourish when it is part of a regulatory framework.

II. Privacy by Design

The origin of PbD can be found in early efforts to take the intent of the Fair Information Practice Principles ("FIPPs") and translate these principles into the design and operation of information and communication technologies.[2] The concept of Privacy-Enhancing Technologies ("PETs"), as this effort was then known, showed how FIPPs could be reflected in information and communication technologies to achieve strong privacy protection. However, where PETs focused on technology and its potential to protect privacy, PbD prescribed that privacy be built directly and holistically into the design and operation, not only of technology, but also of operations, systems, work processes, management structures, physical spaces, and networked infrastructure. In this sense, PbD was the

2. For an extended treatment of PbD origins, see Ann Cavoukian, "Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era" in George OM Yee, ed, *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (Hershey, PA: IGI Global, 2011) 170; Ann Cavoukian, "Privacy by Design: Leadership, Methods, and Results" in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (New York: Springer, 2013) 175.

next step in the evolution of the privacy dialogue that first led to PETs.[3]

As formulated by Cavoukian, PbD consists of a set of seven "foundational principles". These are:

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

At the time of its initial formulation (the early 1990s), PbD represented a significant shift from traditional approaches to protecting privacy, which focussed on regulation by setting minimum standards for information management practices and providing remedies through legal and regulatory instruments for privacy breaches. The traditional regulatory approach was described by Alexander Dix (former Berlin Commissioner for Data Protection and Freedom of Information) as "[l]ocking the stable door after the horse has bolted".[5] In contrast, PbD allowed for greater regulatory flexibility:

> In the past, FIPPs have largely been discharged through the adoption of policies and processes within the firm: privacy has been the bailiwick of lawyers. Now, under the rubric of "privacy by design," policymakers are calling on the private sector to use the distinct attributes of code to harden privacy's protection.[6]

---

3. See *e.g.* Gerrit Hornung, "Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the Future European Data Protection Framework" (2013) 26:1–2 Innovation: The European Journal of Social Science Research 181 (some still appear to conflate PbD with PETs).
4. Information and Privacy Commissioner, Ontario, Canada, "Privacy by Design: The 7 Foundational Principles", by Ann Cavoukian (Toronto: IPC, August 2009).
5. Alexander Dix, "Built-in Privacy—No Panacea, But a Necessary Condition for Effective Privacy Protection" (2010) 3:2 Identity in the Information Society 257 at 257.
6. Deirdre K Mulligan & Jennifer King, "Bridging the Gap Between Privacy and Design" (2012) 14:4 University of Pennsylvania Journal of Constitutional Law 989 at 992 [Mulligan & King, "Bridging the Gap"].

Since its original formulation by Cavoukian, PbD has steadily gained recognition and acceptance over the last two decades, and while it seemed radical at first, it has come into widespread usage as part of the vocabulary of privacy regulators, advocates, and information technology professionals as well as the subject of flattering media articles.[7] A major milestone in this journey was the Jerusalem 2010 resolution of the International Privacy and Data Protection Commissioners.[8] The resolution recognized PbD as an "essential component of fundamental privacy protection".[9] The resolution further "[encourages] the adoption of Privacy by Design's Foundational Principles" as part of "an organization's default mode of operation"[10] and "[invites] Data Protection and Privacy Commissioners/ Authorities to: promote Privacy by Design …; foster the incorporation of [its] Foundational Principles in the formulation of privacy policy and legislation within their respective jurisdictions …; [and] encourage research on Privacy by Design".[11]

Indeed, research into PbD has flourished following the resolution. From specific projects attempting to demonstrate the success of particular

7. Kashmir Hill, "Why 'Privacy By Design' Is The New Corporate Hotness" *Forbes* (28 July 2011), online: Forbes <https://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/>.
8. 32nd International Conference of Data Protection and Privacy Commissioners, "Resolution on Privacy by Design" *International Conference of Data Protection and Privacy Commissioners* (29 October 2010), online: ICDPPC <www.icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf>.
9. *Ibid* at 2.
10. *Ibid*.
11. *Ibid*.

approaches, such as facial recognition,[12] ubiquitous computing,[13] internet protocols,[14] and other "privacy-invasive technologies"[15] to more general attempts to apply PbD to information and communication technologies,[16] to projects that argue that PbD implementation should be based on an understanding of contemporary privacy practices,[17] the cumulative effect of academic research into PbD has been largely to assist in the ongoing transformation of PbD from a theoretical concept into a regulatory instrument.[18] In 2014, Australia's Commissioner referred to PbD explicitly in its guidelines to Australia's new privacy legislation,[19] and Victoria became the first Australian state privacy office to explicitly

12. Juanita Pedraza et al, "Privacy-by-design rules in face recognition system" (2013) 109:1 Neurocomputing 49.
13. Marc Langheinrich, "Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems" in Gregory D Abowd, Barry Brumitt & Steven Shafer, eds, *Ubicomp 2001: Ubiquitous Computing: International Conference Atlanta, Georgia, USA, September 30–October 2, 2001 Proceedings* (New York: Springer, 2001) 273.
14. Adamantia Rachovitsa, "Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue" (2016) 24:4 International Journal of Law and Information 374.
15. Demetrius Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century* (The Hague: TMC Asser Press, 2014).
16. Marc van Lieshout et al, "Privacy by Design: An Alternative to Existing Practice in Safeguarding Privacy" (2011) 13:6 Info 55; Dag Wiese Schartum, "Making Privacy by Design Operative" (2016) 24:2 International Journal of Law and Information Technology 151.
17. Kenneth A Bamberger & Deirdre K Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, MA: MIT Press, 2015).
18. Mulligan & King, "Bridging the Gap", *supra* note 6; Ira S Rubinstein, "Regulating Privacy by Design" (2011) 26:3 Berkeley Technology Law Journal 1409.
19. Tarryn Ryan & Veronica Scott, "AUSTRAILIA — Australia Legislates for Privacy by Design" *International Association of Privacy Professionals* (11 February 2014), online: IAPP <https://iapp.org/news/a/australia-australia-legislates-for-privacy-by-design/>.

endorse and implement PbD.[20] In the United States, the proposed *Commercial Privacy Bill of Rights Act of 2015* referenced PbD explicitly and would have required it as a business practice.[21] The Congressional Privacy Bill directly followed the release of the White House's proposal for a privacy bill, which also mentioned PbD, suggesting that the US government had a clear policy of incorporating PbD principles into its legislative initiatives.[22]

In Europe, the European Commission ratified the final version of the *GDPR* in 2016.[23] The Regulation will be enforced beginning in 2018, providing organizations with two years to become compliant. Article 25 of the *GDPR* codifies both the concepts of PbD and privacy by default.[24] Under this Article, an organization ("data controller") is required to implement appropriate technical and organizational measures both at the time of determination of the means for processing and at the time of the processing itself in order to ensure that data protection principles are met. In addition, the organization will need to ensure that, by default, only personal information which is necessary for each specific purpose of the data processing is, in fact, processed. Personal information will not be automatically made available to third parties. Social media companies, for example, will no longer be able to offer default settings for their apps in which information is shared or available to the public.

---

20. Hamish Barwik, "Victoria to adopt Privacy by Design: Victorian Commissioner" *Computerworld* (6 May 2014), online: Computerworld <www.computerworld.com.au/article/544416/victoria_adopt_privacy_by_design_victorian_commissioner>; Commissioner for Privacy and Data Protection, "Privacy by Design: How to manage privacy effectively in the Victorian public sector" (20 November 2014), online: CPDP <www.cpdp.vic.gov.au/images/content/pdf/CPDP_Media_Release_Privacy_by_Design_20_November_2014.pdf >.
21. HR 1053, 114th Cong, s 113.
22. Libbie Canter, "White House Privacy Bill: A Deeper Dive" *Inside Privacy* (27 February 2015), online: Inside Privacy <https://www.insideprivacy.com/advertising-marketing/white-house-privacy-bill-a-deeper-dive/>.
23. *GDPR*, *supra* note 1.
24. EC, *Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market* (Brussels: 28 January 2015).

The explicit incorporation of PbD for the first time into a major legislative initiative has placed both the concept and the manner in which it has been incorporated into the *GDPR* under intense scrutiny. Some have hailed the *GDPR* for taking a "flexible approach" to PbD.[25] Organizations implementing PbD, for example, will be able to take into account costs as well as conduct a risk assessment in order to determine the appropriate level of privacy protection and design. Others, however, have criticized the European approach for being too focussed on the notion of privacy as control over personal information, which is a notion favoured by information and privacy commissioners.[26] Mainly, however, questions remain as to how PbD will actually be applied as part of the *GDPR*. How will this norm be understood and enforced? Some attempt to bridge the gap between law and engineering,[27] while others believe it is difficult, if not impossible to bridge this gap, and accordingly see the application of PbD to other dimensions of organizational behaviour.[28]

The purpose of this paper is to contribute to the debate over the success of and future application of PbD through the examination of two initiatives in Ontario using the case study method. The case study method has been used by others with respect to PbD, but somewhat

25. Frederick Leentfaar, "Privacy by design and default" *Taylor Wessing* (November 2016), online: Taylor Wessing <https://www.taylorwessing.com/globaldatahub/article-privacy-by-design-and-default.html>.
26. Deirdre K Mulligan & Kenneth A Bamberger, "What Regulators Can Do to Advance Privacy Through Design" (2013) 56:11 Communications of the ACM 20.
27. Michael Colesky, Jaap-Henk Hoepman & Christiaan Hillen, "A Critical Analysis of Privacy Design Strategies" (Paper delivered at the 2016 IEEE Security and Privacy Workshops in San Jose California, 26 May 2016), Security and Privacy Workshops, 2016 IEEE 33.
28. Bert-Jaap Koops & Ronald Leenes, "Privacy Regulation Cannot be Hardcoded: A Critical Comment on the Privacy by Design Provision in Data-Protection Law" (2014) 28:2 International Review of Law, Computers & Technology 159; see also Michael Birnhack, Eran Toch & Irit Hadar, "Privacy Mindset, Technological Mindset" (2014) 55:1 Jurimetrics 55.

tangentially.[29] In contrast, this paper centres on two initiatives in which potentially intrusive technology was introduced with explicit references to PbD and the findings that can be drawn from them in order to determine the role of regulatory intervention and contribute to the conversation as to how PbD may be applied when it is set as a legal standard. The following section discusses the details of the initiatives and the case-study methodology used in their exploration.

III. The Case Study

A. The Legal and Regulatory Background

The Province of Ontario (Canada) has specific privacy legislation for organizations operating in the public sector. The *Freedom of Information and Protection of Privacy Act*[30] ("*FIPPA*") and the *Municipal Freedom of Information and Protection of Privacy Act*[31] ("*MFIPPA*") govern the public sector at the provincial and municipal levels, respectively. However, Ontario has no specific privacy legislation for organizations operating in the private sector. Instead, the federal *Personal Information Protection and Electronic Documents Act*[32] ("*PIPEDA*") applies to the private sector. Ontario also has specific privacy legislation for health service providers, the *Personal Health Information Protection Act*[33] ("*PHIPA*"). Private sector operators in the health sector are governed by *PHIPA* as well, which is considered substantially similar to *PIPEDA*.

The Information and Privacy Commissioner of Ontario ("IPC") is the regulator that enforces *FIPPA*, *MFIPPA*, and *PHIPA*. The Commissioner

29. Inga Kroener & David Wright, "A Strategy for Operationalizing Privacy by Design" (2014) 30:5 Information Society 355.
30. *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31 [*FIPPA*].
31. *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56 [*MFIPPA*].
32. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].
33. *Personal Health Information Protection Act*, SO 2004, c 3, Schedule A [*PHIPA*].

is appointed by and reports to the Legislative Assembly of Ontario and is independent of the executive branch. Under the three acts and statutory mandate, the Commissioner is responsible for:

- Resolving access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction;
- Investigating privacy complaints with respect to personal information held by government or health care practitioners and organizations;
- Ensuring that the government organizations and health information custodians comply with the provisions of the Acts;
- Educating the public about Ontario's access and privacy laws; and
- Conducting research on access and privacy issues and providing advice and comment on proposed government legislation and programs.[34]

During Cavoukian's fifteen-year tenure as Commissioner, her office carried out its mandate under what became known as the "3C" approach — Consultation, Co-operation, and Collaboration. Co-operation was emphasized over confrontation to resolve complaints. Collaboration was sought proactively by seeking partnerships to find joint solutions to emerging privacy and access issues.[35] Internally, her 3C approach led Cavoukian to create a research, policy, and special projects department that was separate and distinct from the Office's compliance, enforcement, investigations, and complaints responsibilities. This department had a

34. Information and Privacy Commissioner of Ontario, "Role and Mandate", online: IPC <www.ipc.on.ca/about-us/role-and-mandate/>.

35. This approach led, for example, to positive results in the area of privacy breaches. Public institutions covered under *FIPPA* and *MFIPPA* voluntarily self-reported data breaches to the IPC despite the *Acts* having no breach notification requirements. Hundreds of data breaches were reported voluntarily in this way, allowing the office to play a vital role at critical breach management stages.

diverse set of skills and competency with a focus on policy, legal, and technology expertise and played a significant role with respect to the two initiatives discussed here.

B. The Two Initiatives

The focus of this paper is on two organizations that are covered by Ontario's privacy legislation and for which the IPC has oversight responsibilities. Brief background information on each of the institutions is provided below.

1. The Toronto Transit Commission ("TTC")

The TTC is an agency of the City of Toronto and is overseen by a Board.[36] The TTC is responsible for public transit within the municipal area of Toronto by means of busses, streetcars, and subway trains. The TTC is regulated by the IPC under *MFIPPA*, but unlike the Ontario Lottery and Gaming Corporation ("OLG") (discussed below), there is no formal regulator that provides oversight for the core activity of the TTC (transportation). The TTC is governed by general legislation applicable to other public sector agencies and by the City of Toronto by-laws.

2. The Ontario Lottery and Gaming Corporation ("OLG")

The OLG is an "Operational Enterprise Agency" of Ontario. Its purpose is to provide gaming and lottery entertainment (casinos, lotteries, horse-racing etc.) while maximizing benefits in a "socially responsible manner".[37] As an operational enterprise agency, the OLG has a single shareholder, the Government of Ontario, and it reports through its Board of Directors to Ontario's Minister of Finance. Board appointments are not full-time, and

---

36. Toronto Transit Commission, "The Board" *Toronto Transit Commission*, online: TTC <www.ttc.ca/About_the_TTC/Commission_reports_and_information/index.jsp>.
37. Ontario Lottery and Gaming Corporation, "ABOUT OLG" *Ontario Lottery and Gaming Corporation*, online: OLG <about.olg.ca/who-we-are/>.

Directors do not manage the OLG directly.[38] The OLG is an institution governed by *FIPPA*, but its main regulator, for the purposes of gaming, is the Alcohol and Gaming Commission of Ontario[39] ("AGCO"). The AGCO operates under the *Alcohol and Gaming Regulation and Public Protection Act*, 1996.[40] Unlike the IPC, the AGCO is not independent of the government and reports to the Ministry of the Attorney General.[41]

3. The TTC Initiative

The TTC initiative began with a complaint to the IPC in the fall of 2007. Privacy International, an organization based in England, complained about the TTC's plan to expand its CCTV surveillance systems by adding more video surveillance cameras in the subway system. It is noteworthy to mention that the TTC already had in place a robust CCTV surveillance program (with policies and procedures) and an extensive systems network that included older analog and newer digital CCTV technology.[42] According to the letter, the TTC was in violation of *MFIPPA*.[43] The IPC launched an investigation into the TTC's practices in response to the letter of complaint. The investigation did not proceed in a traditional manner given the heightened public interest in video surveillance systems at the time and the impact of these systems on privacy. Cavoukian decided that alongside the formal investigation of the complaint, her office would expand the investigation to examine "the role that privacy-enhancing technologies can play in mitigating the privacy-

38. Ontario Lottery and Gaming Corporation, "Our Reporting Structure" *Ontario Lottery and Gaming Corporation*, online: OLG <about.olg.ca/corporate-governance/>.
39. Alcohol and Gaming Commission of Ontario, online: AGCO <www.agco.on.ca/en/whatwedo/index_commercial.aspx> [AGCO].
40. *Alcohol and Gaming Regulation and Public Protection Act*, SO 1996, c 26, Schedule.
41. AGCO, *supra* note 39.
42. Information and Privacy Commissioner of Ontario, "Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report", by Ann Cavoukian, Privacy Investigation Report MC07-68 (Toronto: IPC, 3 March 2008) at 16 [IPCO, "Privacy and Video Surveillance"].
43. *Ibid*.

invasive nature of video surveillance cameras".[44] In the introduction to the section of the report discussing PETs, Cavoukian further stated: "it is essential that privacy protections be built directly into [the] design and implementation [of technology], right from the outset. This view is captured in my mantra of 'privacy by design'".[45] The report then discussed a specific form of image and object detection and encryption developed by research engineers at the University of Toronto ("U of T").[46]

The investigative report found that the TTC was in compliance with *MFIPPA*.[47] Still, the report outlined twelve recommendations for the TTC of which two related to the software solution and PbD:

> 11. That the TTC should keep abreast of research on emerging privacy-enhancing technologies and adopt these technologies, whenever possible.
>
> 12. That the TTC should select a location to evaluate the privacy-enhancing video surveillance technology developed by the University of Toronto researchers[48]

The final recommendation required the TTC to provide "proof of compliance or an update on the status of its compliance with each of the recommendations" within three months of the date of the Report.[49] Unlike other investigation reports often handled exclusively by the Office's compliance, enforcement, investigations, and complaints unit, the research, policy, and special projects department was brought in to collaborate with the TTC on this technology recommendation.

The exploration by the TTC of privacy-enhancing video surveillance was a direct result of the recommendation to do so by the regulator in the investigation report. The TTC responded by providing the U of

---

44. *Ibid* at 1.
45. *Ibid* at 12.
46. Karl Martin & Konstantinos N Plataniotis, "Secure Visual Object Based Coding for Privacy Protected Surveillance" (2007), Draft Submitted to IEEE Transactions on Circuits and Systems for Video Technology, online: IEEE <www.comm.toronto.edu/~kostas/Publications2008/pub/submitted/2007-submitted-Martin-ieee_csvt_secure_stspiht.pdf>.
47. IPCO, "Privacy and Video Surveillance", *supra* note 42 at 43.
48. *Ibid* at 44.
49. *Ibid*.

T researchers access to a test environment and its subway monitoring room to allow the researchers to evaluate the feasibility of the technology in a subway platform context over a few months. After the researchers completed the testing and evaluation of the technology, the TTC determined that it would not be possible to incorporate the software technology into its CCTV systems.

4. The OLG Initiative

Unlike the TTC initiative, the OLG Privacy by Design project did not arise out of an official complaint and investigation report. Instead, also in 2007, the OLG approached the IPC to discuss whether it would be legally permissible for the OLG to adopt facial recognition technology for its voluntary "self-exclusion" program. The "self-exclusion" program allows persons that are addicted to gambling to ask the OLG to remove them from gambling premises that they wish to enter. The approach used until then by the OLG was paper-based, requiring security officers to review photos and related identification information on the program registrants and then manually attempt to recognize registrants and pick them out of the casino crowds.[50] The OLG sought to modernize its monitoring of individuals entering gambling facilities after several incidents in which individuals were not recognized and, therefore, not removed from gambling facilities even though they were enrolled in the "self-exclusion" program.

The result of the preliminary discussion was a research and pilot project into the development and application of biometric encryption to the OLG's facial recognition system. The project required collaboration between the OLG, the IPC, the U of T, and iView (a video surveillance vendor). The IPC's research policy and special projects department led this initiative, with no involvement from the enforcement, compliance, investigations, and complaints sections of the IPC.

---

50. For more information on the operation of OLG's self-excluded program see: Information and Privacy Commissioner, Ontario, Canada, "Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept", by Ann Cavoukian & Tom Marinelli (Toronto: IPC, November 2010) [IPCO, "Privacy-Protective Facial Recognition"].

At the end of the project, the OLG successfully implemented the technology in twenty-seven of its locations.[51] The IPC and the OLG also published a report in which they reported on the success of the project and the successful integration of the technology developed at the U of T with the OLG's facial recognition system: "This use of BE as a secondary classifier was shown to enhance patron privacy (both for those on the watch list, and regular patrons), system security, and even overall accuracy of the watch list system within the context of the OLG self-exclusion program".[52]

C. Research Methodology

This research project used a case study approach to examine the introduction of PbD into the OLG and the TTC's response to embedding privacy into video surveillance technology and the role that the regulator had in these organizations taking a PbD approach. Semi-structured interviews were conducted with at least three individuals involved in each initiative who had an active and leadership role from both a strategic policy and technical perspective. The questionnaire is included as an appendix to this paper. The interviews were recorded, transcribed, and then read by members of the research team to identify key threads in the conversations and arrive at the findings listed in the following section. It should be noted that individuals were asked to recollect details on an initiative in which they were involved ten years ago and that, as is with any case study, the ability to generalize from it is limited.

Participants are not identified and referred to in the project, and quotations from their interview, according to the table below, include brief, non-identifying information about each participant:

Participant	Role
P1	Strategic decision-maker

51. Sharon Oosthoek, "OLG facial scans to help gambling addicts" *CBC News* (26 November 2010), online: CBC <www.cbc.ca/news/technology/olg-facial-scans-to-help-gambling-addicts-1.929760>.
52. IPCO, "Privacy-Protective Facial Recognition", *supra* note 50 at 14.

P2	Senior project management/ technical
P3	Legal/regulatory
P4	Project implementation/senior technical
P5	Project implementation
P6	Legal/regulatory
P7	Research/technical

IV. Findings

It is worth repeating the cautionary methodological note about generalizing from this case study of PbD in Ontario, Canada to the success or failure of PbD in other jurisdictions. With that caveat in mind, this section presents the main points about the implementation of PbD and the role of the regulator that emerges from the interviews. The findings are organized into three overarching themes. The first theme focuses on PbD — reaction to the concept, working with the principles, engineering challenges, etc. The second theme centers on the organizational and leadership dimensions of the two initiatives. Finally, the third group consists of those findings that focused on the regulator — the ideal regulatory role, the place of legislation, the support given by Cavoukian's office, etc.

A. The PbD Theme

1. PbD and Legacy Systems

The constraint of existing technological and infrastructure systems — "Legacy Systems" is both a conceptual and practical barrier to the implementation of PbD:

> Privacy by design presupposes … a process whereby a new information system is designed or an existing system is redesigned or adjusted. Building systems from scratch opens for more possibilities than does changing existing systems. Comprehensive changes in existing systems will often meet some clear limitations: Basic properties of information systems greatly limit

> improvements.[53]

Such a constraint existed both at the OLG and at the TTC. Yet the search for a privacy-protective solution created an opportunity since there were no "off-the-shelf" solutions for the facial recognition problems that both organizations faced. P2 stated:

> When we talked about using facial recognition, a lot of people said, well that's been tried before, you're going to waste your time. And I would give [to P1] who was the person that said we're going to do this, at the start. Which kind of put the gauntlet out to the technology people – now we've got to step up and see if we can do this.

And P5 added:

> "it was always we were going to be doing biometric encryption with facial recognition to protect privacy". That is of course, in a sense, a precondition for the idea of PbD to begin with. Choosing to design privacy into a solution may have been easier, therefore, because a solution had to be developed "from scratch".

While at the OLG, the search was on for a specific privacy-protective solution to the problem of self-excluded patrons seeking re-entry. At the TTC it appears that the scope was wider. The TTC already had a network of CCTV cameras that were used in the subway, some of which belonged to a legacy system (*e.g.* analog cameras). As noted by P7:

> This system was the existing one including existing cameras and storage/monitoring infrastructure for buses, streetcars and subway station platforms. In other words, this project was looking at [the] existing legacy system – it was not about designing a new system. It was retrofitting. Two options were available: i) put in a new system; or ii) retrofit the existing system to comply with PbD.

The TTC also had to deal with separate policy concerns, ranging from passenger safety and operator safety to national security concerns post 9/11.[54] It seems that it was easier to design and apply an innovative solution to a limited problem than it was to retrofit an existing legacy system meant to address a wide range of policy concerns.

---

53. Schartum, *supra* note 16 at 161; see also Nigel Davies & Marc Langheinrich, "Privacy by Design" (2013) 12:2 IEEE Pervasive Computing 2 [Davies & Langheinrich, "Privacy by Design"].
54. P6, transcript on file.

2. Initial Reaction to PbD

It appears that the OLG staff were not specifically aware of PbD as an idea or of its principles. Staff at different levels reacted to PbD differently. P1 saw the public policy appeal:

> It always starts with an idea of design, if you build in that planning and thoughtfulness at the front end of work, that privacy and protection of information is not something that happens at the end of the story, it happens all the way through and why is that different, than anything else we would design?

But for P2, PbD initially held little value:

> To be honest when I first read the principle I thought so how [is] this going to help us … because it's so conceptual … how are we going to take these principles and actually get down to doing facial recognition to aid in self-exclusion. I would tell you that the technical guys were not convinced that we could do this.

P5 was also lukewarm:

> I thought, well it doesn't really make a lot of sense actually. That's really what I thought. Well my initial thoughts were, I don't see, I don't understand this. Because I'm looking at it purely from a solution point of view. It really was difficult for me at the beginning to understand, why we were putting biometric encryption in. The reason I had a big issue with it, was because what we were calling the biometric, the image, was already public. So it was already out there, and it actually had to be out there in order for the security officers to be able to identify people. So we could not actually hold that secret. We couldn't do it. So it had to be, it actually had to be open, and I'm saying, well if it's already open, then what is biometric encryption doing here.

At the TTC, there were similar concerns about the conflation of PbD with biometric encryption and whether there was any advantage to the U of T research project over existing commercial solutions. Explains P6:

> I don't think that there were any issues with the privacy by design, there were suggestions or recommendations that you go look at technology that U of T was studying. So you were kind of led down a specific kind of path from a privacy by design perspective, and I will tell you the engineers didn't necessarily think what [U of T] had was so different than what already existed in the market.

Against such mixed reaction, it seems that the regulator's role was crucial in both convincing and supporting the OLG in its attempt to design privacy rather than focus on "merely" being in compliance.

3. Working with PbD principles

For the OLG initiative, the search for a solution that would allow for biometric facial recognition and protect the privacy of customers captured in the system evolved and transformed over time. P4 said that initially: "[the Commissioner's] thinking was kind of an interesting concept, in terms of being able to protect biometric in the database, and that was the problem we were trying to solve". However, it seems that the early attempts were not successful. P5 commented on the lack of familiarity with PbD and its principles:

> I didn't have a lot of privacy by design experience … So maybe a few months in, or six months in we started to look at the privacy by design principles, and what I did was an alignment exercise to say, how do we align? You know the stuff that we're planning on doing and going to be doing. How does that align to the seven principles? My question in terms of trying to go through the design process and the solution process is, are those principles there to sort of have you wrestle with them as you try and come up with these solutions and have the conversation with the commissioner, or is that something that you're sort of already advanced in terms of the solution and then you sort of tried to fit what you were doing to these ideas of privacy by design?

Following the alignment exercise, P5 described the process of searching for a privacy solution and how the "problem" was re-defined: "I had an idea of how we could use biometric encryption that I could live with … So I had a conversation in one of our meetings … and the first thing [the Commissioner] said was that's an absolutely good use of biometric encryption". After the approval of the Commissioner for the new manner in which privacy was to be designed into the facial recognition system, P5 concluded: "A lot of weight came off me, because now I could believe in it, and I could actually build something that makes sense".

P4 also shared concerns over the technology of biometric encryption and whether it was compatible with PbD principles, specifically the "full functionality" principle: "That's what the research was all about, if it wasn't going to work, one of the things we would stop, the whole concept of biometric encryption because it wasn't going to be feasible". And more generally P4 added:

> Do I believe that we were on the right page on protecting people's privacy from day one? I think we were, but because we look at the holistic solution around privacy, I think the risk, when you look at the necessity for biometric

> encryption, it's not clear that we had to do that. So I think as a case study, there were some good benefits out of it, but at the end of the day, privacy by design and the principles of privacy by design, are good software engineering design principles regardless. How practical each one of them are, are totally dependable on each individual project.

In addition, the OLG was concerned with fundamental privacy principles such as Purpose Specification and whether their proposal to digitize and store facial images would comply with it. P3 pointed out that:

> What we have to guard against, is having their image … on file so that it could potentially be used for a secondary purpose, if there's a crime in the area and the police come to you, with a warrant, with a lawful court order, and they say we want to access all your biometric that you have on file … that would be a secondary use that even though it is lawful … we wouldn't want that.

P4 also noted that there were other, more protective alternatives that were less attractive from a commercial point of view: "OK Ontario, basically say everybody, anyone who wants to buy a gaming product, needs to have a card, needs to be registered. Ontario doesn't want to go there, right …"

At the TTC, the project never progressed beyond the research phase, seemingly not because of difficulties related to working with PbD and its principles but because of technological obstacles. According to P7:

> The solution could be implemented but remember this was done several years back unlike the advances that have developed recently in the area of CCTV systems … If the TTC invested early on and made a commitment to this privacy enhancing technology, this encoding could be done on the camera which is more secure and easy to implement.

4. PbD and Education

Participants were asked to generalize about PbD on the basis of their experience and their specific project. P2 believes that education of engineers in PbD is absolutely essential if it is to succeed beyond a few examples:

> I think [PbD] principles are just what they are, principles. So they guide you. I think the body of knowledge has to follow after that. So I often thought about the universities, and within some of these information programs that you actually start introducing the concepts of the seven principles into the university so that the students that are coming out are very aware.

P7 added that part of the difficulty is that engineering education is

regulated and largely prescribed by the profession:

> To do [PbD] requires, needs, direction to engineers to do it. Nothing prevents this in technical solutions. It is difficult with undergraduate [education]. Engineers are regulated. It takes a bit more time for engineers to react. 10-20 years ago privacy was not so important … I don't see problems with integrating PbD into curricula or into products.

As to the PbD principles and whether they are detailed enough to provide guidance for engineers, P7 is of the opinion that "what is missing is the educated people who can take the inspirational message [of PbD] and make sense of it". For P7, that is similar to any other engineering design exercise: "customer gives specs the way the customer understands. The designer/builder needs to translate the customer specs. [We] need people to take [the privacy] message and translate it".

5. Legislating PbD

Based on the TTC project, P6 is concerned about any attempt to legislate or impose PbD: "when the organization wants something, and you do it in consultation, then the privacy by design concept gets a much bigger play, and succeeds. When imposed, it has far less opportunity to be successful".

P3 is pleased with the legislation of PbD but concerned about the bureaucratization of PbD:

> First of all here's why I think it's a very positive thing to have it in the legislation. By having it in, the *GDPR* in the statute, it automatically elevates, because companies will now be required to embed privacy as the default, to have privacy by design, data prediction by design, it's no longer just a suggestion, it's required, and that by necessity will raise the bar. You can kind of see it as default. We're talking positive consent that is not the prevailing standard as you know. So that's what raises the bar. My only concern, I don't even want to express this as a concern but a question. I don't want this to get regulated to death.

That may be because other regulators have been slow to embrace PbD, although now it enjoys regulatory consensus. According to P3:

> the whole privacy by design thing, it took three years of presentations at the EU commissioners meeting, before it took off. The first couple of years it received polite applause perhaps. The third year, the UK commissioner she came from the telco world, and then she became commissioner, and she got it like this, and then the EU has commissioner's meetings, the EU commissioners, she

> started propagating it and it just flew after 2004-5.

Therefore, it is notable that PbD has enjoyed the greatest success with regulators that have a non-legal background.

6. Theme Summary

The main findings emerging from the PbD theme, therefore, relate to the gap between the principles of PbD and the concept of PbD on the one hand and the attempts of implementing PbD as an engineering solution on the other. The constraints of having to work with legacy systems, the lack of familiarity with PbD, and its principles necessitating both a learning curve as well as time-consuming mapping exercises in which PbD is mapped against software and hardware design processes with which engineers are more familiar led to a difficult implementation process. In one initiative, this process stalled, while in the other it had to be restructured and rethought in order to arrive ultimately at a successful solution. One suggestion that would assist in bridging this gap was the educational one — the inclusion of PbD and its principles in the contemporary engineering curriculum. Notably, the move to enshrine PbD in legislation was met with concerns.

B. The Organizational Theme

1. Internal Support

Overall, internal support for the project at the OLG was achieved by ensuring that all internal stakeholders were updated. Beyond the support of leadership from a public policy perspective, the design of privacy into the facial recognition system required the support of the technical staff that worked on the project. P2 described the process:

> Our approach was pretty structured … so there was never all of a sudden somebody coming in and [raising concerns]. So at any point in time, when we went through that structure, we educated our stakeholders. We brought them in the room, sat down, and talked to them about what we found, the good the bad and the ugly, because there were a few times that we actually thought that it wasn't going to work.

At that key moment, when the OLG could have decided to stop pursuing

the design of privacy, the support of the regulator and of the technical staff was crucial. Continues P2:

> we actually had a meeting down at [the Commissioner's] office and she was quite clear that she wanted us to move forward with this, so back at the ranch we sat down and we brainstormed. How is this going to work? And I would say a key individual that we actually brought on at that time … who actually took it upon himself to say, look I'm going to try to solve this … I wasn't quite confident that we can actually pull off the design, until this gentleman came in, and he took it upon himself as a challenge.

The success of the solution beyond PbD assisted with the support for privacy in general in the organization in subsequent years. P5 explains:

> we actually came up with examples of how we were actually adhering to the PbD principles and in some cases not, right. So we looked at the one about positive sum and what that means, as an example, and then we looked at what we were doing. Here's a perfect time to tell you about the unexpected benefit of biometric encryption. We had the two classifiers, face recognition whittling down the problem, and then biometric encryption taking over. Just the fact that you're doing two different classifiers, it actually made your accuracy of the system better. What that did is it actually led people to believe in the system more, where they say, yeah we're going to get some false alarms, but we've brought it down from 4% false alarms – which is a lot, down to under 2%. Which is pretty damn good. Like in the biometric field, that's really really good results.

At the TTC, internal support never built up for the biometric encryption PbD initiative and perhaps, consequently, it did not progress beyond the research stage. Apart from the concerns over working specifically with the research team at the U of T (mentioned above), it seems the specific PbD route proposed by the Commissioner was incompatible with existing TTC technology at the time. P6 elaborated:

> If you were doing live monitoring, [the proposed solution] would help to address privacy issues about how much information people were seeing. Where there was a disconnect, [the TTC] did very little monitoring … and the places where it would be monitored, our systems are so old that even [there] they said you couldn't do it.

According to P7, the TTC did not provide funding on a comparable level to that of the OLG:

> The project lasted only a few months which included meetings. No funding from TTC. [The Commissioner] provided 'in kind' resources – staff for project management. TTC provided 'in kind' resources – access to equipment in Bay station. OLG was different because there was funding. OLG, by its nature, has

> significant technical resources. Organizationally, there was a lack of interest as well at the TTC in comparison with OLG. At OLG, there was interest from CEO through to technical staff. TTC had different priorities – I doubt that even with senior management approval [they would have] the expertise. [The TTC had] other major issues, had older generation of trains. It felt that TTC was more exploratory, unlike OLG.

Further, as quoted above, P7 adds that the project at the TTC may not have been, strictly speaking, a PbD project: "In other words, this project was looking at existing legacy system — it was not about designing a new system. It was retrofitting. Two options — put in a new system; or retrofit system to comply with PbD".

Whether or not it was a "true" PbD exercise, the research project failed to elevate the importance of privacy within the TTC. P6 describes the attitude towards privacy:

> Other than regulators and some privacy advocacy groups, most of [the TTC] doesn't [care especially] about privacy. So when you do the regulations, [privacy] becomes a checklist, and organizations who have generally [wanted] to implement a system which has a privacy impact to it, will pay a lip service to [privacy], and say yes, I designed it, I have a retention period that tries to address it … so I think that privacy becomes superficial.

2. The Role of the Internal Privacy Office

Interestingly, at the OLG, the internal access to information and privacy office had an insignificant role during the pilot project. P2 described it as "buried within the organization" and that its importance actually grew as a result of the success of the PbD project:

> I often sit back and say the whole privacy involvement started with this project. I mean people were aware, we had co-ordinators and stuff, but that was more [formal]. So now, right now at OLG if you think about it, in the project management life cycle, the privacy assessment, the central privacy assessment is right up front. It's very grained in the method.

P4 added: "this whole area of privacy by design and this policy was brand new at the time. Like privacy, when we started this program, privacy was, the whole privacy environment didn't have anywhere near the visibility it had today".

According to P5 as well, the importance of the privacy office grew after the success of the project:

> So we probably always had a privacy department at OLG, but I think it probably expanded or had a little more visibility because, I truly believe that was a very important piece. And they were using that as an example of also helping people understand what do you do, do a PIA, do a privacy impact assessment. Do it up front. Understand what you're doing, get it in at design time. Those terms, those little nuanced conversations about, even saying things like do it at design time. Those came from looking at [privacy] early.

3. Theme Summary

The findings related to the organizational theme, therefore, are that PbD initiatives, similar to any other initiative, need internal support in order to succeed. Internal support is required at all levels but, and significantly, even more so at the engineering level. Somewhat counterintuitively, the success or failure of the PbD initiative did not correlate with the existence of an active and visible privacy office within an organization, or even with the existence of a positive privacy culture. However, the success of a PbD initiative bolstered privacy after-the-fact throughout the organization.

C. The Regulator Theme

1. The Regulator's Role in Early Stages

It seems that in this case study, it was difficult, if not impossible, for participants to separate the role of the office of the IPC from the person that held that position for over eighteen years in Ontario. The paper discusses this duality further in the following section, but it was evident to participants that they had to deal not only with formal legalistic regulatory requirements but also with the personal convictions of the Commissioner. P1 put it in the following terms:

> I would say that Ann was really trying to take organizations into the next century … what made her very unique, is she was always looking for ways in which you could actually operationalize [privacy]. She wasn't just interested in reporting on it and investigating it, she wanted to know how to make it easier for people to do.

As P3 observed, the OLG knew that:

> to contemplate doing this without checking in with the regulator would have been death in Ontario. Because [the Commissioner was] very vocal, and always said to government departments "Come and talk to me. I will help you behind

> the scenes quietly".

P4 went further: "You know, the commissioner was not going to let us implement facial recognition without biometric encryption".

For P6, it seemed as well that PbD was more of a personal interest of the Commissioner than of the formal investigation:

> Prior to [the investigation], I don't ever recall the privacy by design aspect of that. So in the policy you're being driven to privacy, but not in a broad perspective, and then when they come out with a report in 2008, you're definitely getting the privacy by design aspects imposed in the recommendations and then in subsequent meetings with the privacy commissioner. You're no doubt getting the privacy by design speech [from the commissioner].

Going forward, P6 added that PbD could simply be viewed as the price that has to be paid in order to avoid greater regulatory scrutiny and obtain regulatory approval:

> When you look at 2007, [the TTC was] already into the investigation and you have the requirements imposed on [the TTC]. And therefore [the TTC doesn't] have a say, [it has to] meet the requirements. When [the TTC], prior to implementation, [goes] back to the regulators to sit with them, and work with them about what [the TTC does] with privacy by design, has much more attractiveness to me and why you get a far greater buy in. And the buy [in] isn't because they necessarily believe in it, the buy in is the price for [the TTC] to be able to do what it wants, and so that is the fundamental difference. So when you look at where [the TTC is] today, about front facing [cameras] or even audio, it is the TTC who has a far greater objective now, will be much happier to do something, will spend the dollars in order to appease everyone, and will implement and take a far greater active approach to privacy by design.

2. Regulatory Support for the Initiatives

In order to convince the OLG to consider PbD, the Commissioner not only raised concerns about the privacy implications of the new technology, but it appears that more importantly, the office offered support that exceeded traditional regulatory involvement. P3 described an initial meeting:

> We had this meeting in the boardroom, and [OLG CEO] laid this all out and she said I know [the Commissioner will] work with us to find a way to make this work. [And the Commissioner said] I have a solution but it has to be tested, a thing called biometric encryption.

And for P2, the regulatory, unconventional support was crucial to

accepting to take on a PbD approach:

> We had the perfect storm. You had an agency of the crown, who was interested in social responsibility. You have a privacy commissioner who had the privacy by design aspect, and had competent people in her organization. You had [the University of Toronto], and we were fortunate enough to get an Ontario company that actually did the facial recognition. With all that together, [PbD] worked.

P4 spoke about the support provided by the Commissioner and meeting the needs of multiple stakeholders:

> We had regular status meetings … we got like OLG, privacy commissioner, U of T, the vendor, and then we had the AGCO, and then we had the site management and gaming management … At this point in time, when you're running with multiple stakeholders, things get complicated. Too many people involved, [too] hard to do this work because you got too many stakeholders. In many cases, it can be really non-productive.

Despite the above lukewarm sentiments about the value of the regulator's support, P4 added:

> My sense is, and again since the privacy commissioner changed, right now we have almost no relationship with [the privacy commissioner]. We, the science guys here, have no relationship with the privacy office downtown at all.

P4's assessment fits the changes taken by the current IPC of Ontario, who has distanced himself and his office from the idea of PbD, for instance, by removing from the official website the numerous PbD resources that were created and promoted during the tenure of Cavoukian.

3. Primary vs Secondary Regulator

It appears that it was important for the success of PbD that the privacy regulator was "not" perceived as the primary regulator of the OLG (the TTC does not have a primary regulator). P4 provided an example: "as we started to move into the casino environment, to be able to do anything in the casino, you need the gaming regulator to be there … the regulator was there anytime you do anything in a casino".

And P5 stated more generally:

> There are big differences because the AGCO is the regulator of OLG. The privacy commissioner, yes, is a regulator as well, that's a part of the commissioner's office, but it's different, because we are like, that's a regulator of gambling, and we have massive amounts of gambling controls. It's done purely for protection and for control. The privacy commissioner is conceptual …

> Where at the AGCO, it's very direct, 'you will do this'.

4. Collaboration or Enforcement

Notably, following up on the previous theme, it seems that it was possible for the OLG to collaborate with the Privacy Commissioner as the secondary regulator and not be overly concerned about enforcement. In addition, Cavoukian's 3C approach played an important role in creating collaboration not only between the OLG and the Privacy Commissioner but between the TTC and the Commissioner as well. Noted P3: "Cavoukian always favoured the carrot to the stick, … from a privacy perspective. She would rather address things up front, rather than after a breach has happened".

Indeed, it seems that at least at the OLG, it was realized early on at the conceptual stage of the project that privacy issues would need to be addressed during the development of facial recognition for video surveillance technology (P1, P2 interviews). It was clear at the senior level that the privacy regulator would likely raise concerns with combining surveillance and biometric technologies that would involve collecting sensitive information on all casino patrons, not just the target (self-excluding) population (P1 interviews). Thus, there was an impetus to be proactive by reaching out to the Commissioner at the conceptual stage rather than after the design of the proposed system. At that point, it seemed that PbD would be an opportunity for collaboration with the regulator and that the PbD route would avoid the enforcement-style regulatory relationship. According to P4:

> OLG brought this forward to try and you know, talk to the privacy commissioner about using facial recognition … and I believe the privacy commissioner said no way … The privacy commissioner had published, or was getting ready to publish privacy by design … and was looking for use cases, or some experimental deployment to see if it would work. So [everyone] sort of put two and two together and said, OLG if you want to do this, we've got this privacy by design scenario, so would that work, would that be an opportunity.

At the TTC, the initial circumstances were different since there was already a complaint in front of the regulator about the use of CCTV within the TTC system. The complaint created a formal relationship of an investigation between the regulator and the TTC that did not

exist with the OLG. Prior to the complaint, it appears that an informal relationship did exist. States P6:

> The TTC had made public statements looking at cameras on the bus. So that adds a phone conversation and meetings with the Ontario Privacy Commissioner's office saying we want to help you, we want to see the policy, we will work with you on the policy.

The complaint, in other words, forced the regulator and regulated into an enforcement-style relationship where collaboration would have been preferable and, indeed, had been attempted. The focus was on the formal investigation led by the compliance, enforcement, complaints, and investigations department. Only later did the more collaborative research, policy, and special projects department become involved when looking at the potential privacy protective technology solution. Indeed, P6 did not recall PbD being front and centre in the initial conversations of the TTC with the Commissioner: "I did not recall that notion ever directly coming up, but it comes up indirectly. During the investigation, the answer is no". The TTC's focus was on the complaint and the investigation: "When you look at 2007, [the TTC was] already into the investigation and you have the requirements imposed on [the TTC]. And therefore [the TTC doesn't] have a say, [it has to] meet the requirements". However, at the later stage, with the involvement of the research, policy, and special projects department, the TTC was more receptive to PbD. According to P6: "When [the TTC], prior to implementation, [went] back to the regulators to sit with them, and work with them about what [the TTC will do] with privacy by design, [it] has much more attractiveness and why you get a far greater buy in".

5. The Overall Role of the Regulator

It was easier for the TTC and the OLG to approach the Privacy Commissioner given that the Commissioner at the time was Dr. Cavoukian who had (and continues to have) an unusually high public profile and a reputation for both forcefully advocating for privacy and strongly supporting organizations as they seek privacy-friendly solutions. P1 described the former Commissioner in the following terms: "It was Ann's openness to new solutions, and not immediately saying you

can't do that. And our openness to, you might have to do it differently, but we can get there". And P2 was impressed by the Commissioner's advocacy: "nobody would have thought that the information and privacy commissioner would be giving a talk at a gaming conference. And she did". Still P2 noted that the OLG approached the Commissioner with some trepidation: "there was a fear … because you're actually exposing the organization to the privacy commissioner … internally people were concerned".

P3 described the Commissioner's approach as follows:

> [The commissioner] developed the policy with 3 c's which was communication, co-operation, consultation. If you talked to [the commissioner] before the fact of whatever may have happened, then [they would] work with you behind the scenes, [not] trying to get any notoriety out of this. [The commissioner] wants solutions that work and wants to help you. You take all the credit.

Part of the Commissioner's advocacy was to change the internal thinking about privacy. P3 mentioned that the Commissioner had a presentation which said, "great privacy is a business issue, not a compliance issue, and a competitive advantage. Conflict with the regulator is a zero-sum approach".

P5 also felt that the Commissioner played a positive role:

> I think without Ann's passion for this, this never would have happened. I can guarantee you that. I would not have thought of even doing this. So, I would say that her passion for that, and the fact that she really you know, was adamant that we look at these things from a privacy lens very strongly, I think that that really helped. I think that the privacy commissioner's office really kept us on track. Kept the entire project, the program on track. OLG was a willing participant in it for sure, we all, we all wanted to make sure we did what was best for the public good, but I think that you needed that guidance for sure, it was key.

At the TTC, the overall relationship with the Privacy Commissioner had a different tone since the attempt to design privacy into the TTC's cameras was done alongside a formal investigation of a complaint about the TTC and its practices. While little was said by participants about the investigation itself, it seems that there were several barriers to adopting a PbD solution into TTC's video surveillance expansion, including the fact that the TTC did not come willingly to PbD adoption but that it was imposed through the investigation (P6 interview).

Still, the interaction with the regulator caused the TTC to formulate its need for surveillance cameras that would not have come about otherwise. States P6:

> The TTC said we want the regulator on board, we want to make sure what we're saying is perfect, and we want to work with [the regulator]. [The regulator] said, well you know, what we really want to know is have you looked at other less intrusive technologies, and what's the primary purpose, which is a problem to answer because every group has a different answer. So [the regulator] really just sent [the TTC] back, saying, this is what we want to see in the business case, show us that you've looked at all the other privacy [more protective options], and show me why they're not [possible], and then tell me how your system [will comply].

Finally, for P1, the role of the privacy regulator in contemporary society is different from the role of other regulators:

> Here's the thing though, where I think privacy is unique right now, there's such a proliferation of tools, to get into somebody's information. I think by virtue of the environment, there is a stronger need for the regulator to have much more proactive foresight on where to get ahead of this, and also to be working collaboratively with insight on how to design. I don't think any legislative regulator in the area of privacy and information in what is now, basically, a data-driven analytics age, can be resting on their historical way.

To that P3 added:

> [The commissioner's role is] not a traditional role. Perhaps because [Cavoukian was] not a lawyer, it was easy for her to look at it as not a lawyer. [Cavoukian] loved the design aspect, let's design things in a way that can avoid the need to engage the regulators wrath, which is usually what you're getting at the end.

6. Theme Summary

The sum of the findings related to the regulator theme is that the personal role that Ann Cavoukian played in the implementation of PbD is inseparable from the formal regulatory role that her office played. It is clear that regulatory support early-on was crucial for the success of PbD and also that the formal regulatory relationship, in the form of an investigation, was, in fact, counter-productive and did not lead to the success of PbD. Broadly speaking, it seems that a collaborative regulatory model is preferable to a model which focuses on the enforcement of the relevant privacy law and that an informal relationship, such as the one that is created when the Privacy Commissioner is perceived not to be the

main regulator, is preferable to a more formal one for such initiatives to succeed.

V. Conclusions

Three conclusions can be drawn from the findings of this research project with respect to engineering privacy, privacy as an organizational function, and finally with respect to regulating PbD.

A. Privacy as an Engineering Problem

Privacy continues to be an engineering problem. Ten years ago, in both initiatives, the first and foremost challenge was to engineer a technological solution that would reflect in a meaningful way the principles of PbD. In both initiatives, engineers at all levels of the project noted their inability to use the principles of PbD in a way that would help them in their work.

At the TTC, the initiative did not proceed beyond some preliminary testing. The findings show that the TTC did not find the biometric encryption technology useful. This was a straightforward conclusion that, in fact, had little to do with PbD. Simply put, the technology did not work in the manner that the TTC had hoped for, or in a manner that at least would garner support for the continuation of the initiative. During the limited pilot, PbD and its principles were of limited use to the researchers and engineers as they attempted to incorporate the privacy enhancing technology into the TTC's systems. PbD could not offer, therefore, professional guidance, the equivalent of an engineering manual, to the researchers working on the initiative and could not point them in the direction of a successful solution. PbD was of little practical use and due to the overwhelming lack of organizational support for the initiative within the TTC, could not even play a motivational, inspirational, or ideological role.

At the OLG, with all of the senior leadership support and with all of the regulatory support, the initiative came close to failure because of the difficulty of engineering PbD. In a sense, as revealed in the findings, the original initiative did fail, and it became apparent that it was necessary to reconfigure the project to allow for some form of integration of biometric encryption into the facial recognition systems that the OLG was preparing

to deploy. From the initial hope (and perhaps, to this day, widespread public misperception) that PbD would protect the information of all visitors to the OLG gambling sites by encrypting their images,[55] and in so doing would mitigate the risks of such information being shared with others for a variety of secondary, unapproved purposes, the OLG initiative changed to deploy biometric encryption in order to enhance the security of its self-excluded patron database. The images of such patrons are used, in other words, as an encryption key that unlocks the database upon the entry of a self-excluded patron into an OLG gambling site.

The OLG initiative can hardly be said, therefore, to diminish surveillance or the use of CCTV or the use of facial recognition technology. However, the OLG initiative does demonstrate the successful incorporation of privacy enhancing technology into its image processing and databases. The question remains whether the initiative was an example of the successful application of PbD principles to a technological problem and whether we can conclude that PbD principles provided guidance to the OLG's engineers as they attempted to incorporate biometric encryption into their systems. The findings unfortunately indicate that we cannot and that the PbD principles were mapped onto the work done by engineers after the fact and with some difficulty. At best, PbD inspired all those working on the initiative to indeed find a way to design privacy protection into it. The importance of PbD as a motivating factor and driving force is, therefore, an important conclusion, yet at the same time it underscores the important realization that the principles of PbD offer little practical guidance to engineers.

---

55. One of the very first paragraphs of the report on the OLG initiative, IPCO, "Privacy-Protective Facial Recognition", *supra* note 50 states "the increased use of facial recognition technology raises a number of privacy and security concerns. Given their mutual interest in respecting the privacy of all casino patrons, the IPC and OLG agreed that the application of an emerging Privacy-Enhancing Technology — Biometric Encryption (BE) — to a facial recognition system at an OLG casino would be an ideal 'win-win' project" at 1. See also IPCO, "Privacy-Protective Facial Recognition", *supra* note 50 at 14.

B. Privacy, Organizational Change, and Leadership

Against the backdrop of difficulty in implementing PbD in a technical, engineering sense, there is a growing sense that the value of PbD lies more in its ability to bring about organizational change and serve as an effective leadership tool. The findings allow for a discussion of the importance of regulatory leadership as well, which is discussed in the following section.

The two initiatives present radically different, almost diametrically opposed, organizational approaches.[56] At the TTC, it is clear that there was little appetite for organizational change. Leadership viewed the PbD initiative as a regulatory imposition that was foisted upon the organization as a result of an external complaint. Indeed, it seems that the organization was at a loss understanding why a formal investigation against it was launched when, from an organizational perspective, existing systems and policies were reviewed and vetted by the IPC. From the outset, therefore, the TTC appeared to be in organizational opposition to any attempt to enhance or design privacy into its systems, possibly because that would be tantamount to admitting that the systems needed to be enhanced and were, therefore, lacking in some way and that the complaint against it would somehow, as a result, be perceived as justified.

Adding to the organizational reticence was the formal complaint process and the formal relationship that it created between the TTC and the IPC. As an organization, the TTC appeared content to remain within the confines of the complaint process and not venture beyond. Since the exploration of privacy enhancing technology was formally one of the recommendations of the IPC's investigatory report, the TTC dealt with it formally, and perhaps with minimal effort, in order to ensure it was in compliance with the report but not really out of a compelling interest in privacy. PbD was perceived not as a motivating ideology but as an imposition.

---

56. This point is strengthened by the recognition that both initiatives appeared to benefit from similar organizational resources. The TTC, for instance, provided access to its subway stations and other facilities in order to provide researchers the ability to evaluate their PbD technology for the duration of the initiative.

At the TTC, there was no push at the time to introduce new, potentially invasive, potentially surveilling, technology. The organization had its priorities set out in terms of improving service levels, increasing and maintaining ridership levels, improving customer experiences, maintaining costs, etc. It was focused on its core mandate of providing transit services, and as a result, leadership viewed the investigation, report, and pilot project as unwelcome distractions. In this organizational environment, there was little room for PbD to take hold, let alone serve as a useful tool for leadership.

In contrast, the approach of the OLG to PbD was strategic and calculated in order to ensure regulatory support for the organization's initiative to modernize its self-exclusion program. Leadership of the OLG, at its most senior levels, was committed to support the integration of privacy with the facial recognition technology it was interested in. The findings indicate that the OLG leadership recognized the value of privacy not only strategically, in its dealing with the IPC, but also as a genuine value of public policy. As such, the protection of privacy fitted other values that the OLG aspired to associate with, such as organizational social responsibility in the context of responsible gaming.

The organizational adoption of PbD was easier at the OLG for two additional reasons. First, the OLG was not caught up in an investigation and was not the subject of a complaint to the IPC. The OLG was, therefore, not constrained by a formal relationship or concerned with the implications any of its actions may have with respect to an ongoing investigation. Second, the IPC was not the primary regulator of the OLG, allowing for a free and more informal relationship between the two entities. It is clear from the findings that the OLG is very careful in its relationship with its primary regulator, the AGCO, and that the regulatory guidance of the AGCO is quite detailed at times. It is telling that the OLG perceived the IPC and PbD as the opposite, and this further supports the conclusion that the power of PbD is not to be found in detailed technical guidance but rather in its ability to increase awareness and motivate organizations to think about privacy from the outset.

Once the leadership of the OLG endorsed privacy and endorsed PbD as the approach that should be taken with respect to its facial

recognition initiative, it was able to instill within its engineers working on the project the necessity of taking privacy into consideration and of collaborating openly with the IPC on a privacy enhancing solution. The IPC was perceived not so much as a dreaded regulator but rather as a subject-matter expert brought in to assist on the incorporation of privacy and on the understanding of PbD. This open relationship enabled close collaboration (of which adherents of a more formal regulatory role may be critical — see the following section) and ultimately allowed for the OLG to change the manner in which biometric encryption was integrated into its systems with the approval of the IPC.

The internal organizational result, as evidenced by the findings, has been an increase in the role and significance of privacy throughout the OLG from a more formal, limited, compliance role to a more pervasive, cultural, strategic role. Participants became more familiar and comfortable with PbD and its principles (such as purpose specification), the privacy office has increased in its resources and organizational importance, and privacy impact assessments are no longer a novelty. All of this occurred, notwithstanding the difficulties that the OLG's engineers had with the actual implementation of PbD's principles into their processes. This result strengthens the overall conclusion that the importance of PbD can be found in its ability to effect change, to inspire and to motivate, rather than in its ability to provide detailed guidance on how privacy is to be designed into a specific, given project. Of course, such conclusions have implications with respect to the ideal regulatory role in enforcing PbD once it becomes legally required.

C. PbD as a Regulatory Tool

As noted in the second section of this paper, Article 25 of the *GDPR* (that section of the new EU legislation where PbD is introduced into law) states that organizations will have to "implement appropriate technical and organisational measures … which are designed to implement data-protection principles … , in an effective manner and to integrate the necessary safeguards into [data] processing".[57] The Article also states that

57. *GDPR*, *supra* note 1, art 25(1).

in so doing, organizations must take several factors into account:

> the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[58]

Finally, the Article states that organizations will be able to demonstrate compliance through certification. As envisioned in the *GDPR*, certification will be a voluntary process undertaken by organizations, and certificates and seals will be issued by certifying bodies that are, in turn, accredited by the relevant data protection authorities.[59]

Several important points emerge from the language used in the *GDPR* with respect to PbD. First, PbD is not understood exclusively as a technical or engineering tool. It is just as equally an organizational tool that can be used to bring about organizational measures and changes that will better protect privacy. The findings discussed above, and in particular the immediate conclusion above with respect to the ability of PbD to bring about organizational change, support Article 25 to that extent.

Second, Article 25 recognizes that PbD is an exercise that will vary greatly from one set of circumstances to the next and that in order to succeed as a regulatory instrument, PbD will have to take into account the factors listed in Article 25. This language indicates that a heavy-handed, one-size-fits-all regulatory approach is not to be expected in the EU with respect to PbD and that organizations will be given considerable flexibility. Unfettered flexibility does raise concerns, of course, as to whether PbD will end up as a watered-down idea that will not bring about meaningful regulatory change. Yet, at the same time, this case study does indicate that flexibility, and in particular regulatory flexibility with respect to the implementation of PbD, is necessary if the idea is at all to succeed.

This flexibility is discussed further immediately below, but even prior to that discussion, it is worth noting how different the regulatory paths of the two initiatives were, despite apparent similarities. The OLG and the TTC both explored very similar intrusive technology, and both were

58. *Ibid*.
59. *Ibid*, art 42–43.

subject to the same legal framework surrounding personal information in Ontario. However, these similarities only serve to emphasize the different outcomes of each initiative. As discussed above, the initiatives ended differently largely due to the degree of internal organizational support each initiative enjoyed but (and perhaps more importantly for the present discussion and for the more general discussion attempting to determine how PbD will fare when it is mandated by law) also due to the role of the regulator in each initiative.

Throughout the TTC initiative, the regulator was constrained by the formal investigation and could not collaborate with the TTC to push for the success of PbD. With the OLG, however, due to the combination of not being the main regulator of the OLG as well as not formally investigating the OLG, the IPC was able to actively collaborate and demonstrate considerable flexibility. From a PbD initiative, which was presented to the public and perceived as an initiative in which privacy would be designed into surveillance cameras using innovative bio-encryption technology so that all individuals walking into an OLG gambling facility would have their privacy protected (through the encryption of their image), the project changed in scope to provide, in the end, for the protection of the personal information of self-excluded patrons in the OLG database by encrypting it with their image. While a noteworthy and laudable achievement, the final outcome of the OLG initiative is a far cry from its original formulation. It is clear from the findings that it would not have developed in such a manner were it not for the approval of the IPC and (then) Commissioner Cavoukian specifically.

Information gathered during the interviews conducted for this project was not sufficient to determine conclusively why such a change took place. Was it so that the OLG could simply proceed uninterrupted in the modernization of its self-exclusion program? Was it so that the OLG and the IPC could showcase a model of regulated-regulator interaction? Was it so that the IPC could tout PbD as a workable and not only aspirational idea? Was it to demonstrate the benefits of bio-encryption as a specific form of privacy enhancing technology? In all likelihood, the answer is a mix of all of the above. Does that indicate that Cavoukian cared more

about demonstrating the success of bio-encryption and of PbD than she did about the protection of everyone that would walk into a casino? Although Cavoukian has been forcefully criticized for her 3C approach and her pragmatism in the past,[60] such a conclusion seems unduly harsh.

A more positive evaluation of Cavoukian and the IPC's role would take into account her creation of a research, policy, and special projects department, the substantial support her office gave to the two initiatives through this special department, and her regulatory flexibility, all as much-desired regulatory traits. The findings can be further used to argue the point that neither initiative would have enjoyed the same level of support under another commissioner. Indeed, no other regulatory office in Canada has supported PbD initiatives in a similar manner, and the research, policy, and special projects department no longer exists at the IPC.

Regulatory determination, even rigidity, is no doubt quite often necessary and required, and the IPC, including under Cavoukian, certainly has shown its ability to enforce the law and exercise its order-making powers under Ontario's provincial legislation. The question of this case study is, however, whether PbD will be better achieved through a rigid or flexible approach. In the United States, for example, the introduction of PbD led scholars to call on the Federal Trade Commission ("FTC") to combine some regulatory firmness ("enforcement threats") with the cultivation of "entrepreneurial privacy [advocacy]" and in so doing to "[avoid] both the shortcomings of static, top-down, command-and-control regulatory approaches and the ways in which reliance on bottom-up self-regulation alone can subvert public goals by private interests".[61] It is certainly understandable why the IPC and Cavoukian would want to demonstrate flexibility with respect to PbD at a time that it was not explicitly part of the governing law but rather an approach that the IPC

60. Ian Kerr, "Dreamin Man: The Role of Idealism and Pragmatisms in Privacy Advocacy" *Ian Kerr* (23 July 2008), online: Ian Kerr <www.iankerr.ca/blog/2016/6/21/dreamin-man-the-role-of-idealism-and-pragmatisms-in-privacy-advocacy>.

61. Kenneth Bamberger & Deirdre Mulligan, "Privacy on the Books and on the Ground" (2011) 63:2 Stanford Law Review 247 at 313.

encouraged organizations to take with respect to compliance.

More generally (and to the extent that the case study can be generalized), it appears that a rigid approach to the implementation of PbD would be counter-productive given the ambiguity surrounding many of the operational details that have been developed, or have been attempted to develop, with respect to PbD over the years. PbD has always been most impactful as a guiding principle, emphasizing the importance of privacy and elevating privacy to the level of other organizational goals by stressing that it should be included in every organizational initiative related to personal information. The TTC and the OLG initiatives show us (in addition to academic literature on this point) that mapping PbD onto engineering, solution, and design algorithms is incredibly difficult. Some flexibility is, therefore, almost essential given the present state of PbD.

It may be that, somewhat intuitively, Cavoukian adopted a flexible regulatory approach that both fits PbD and appears to be advocated for increasingly by scholars studying the data protection authority model and its efficacy over the years. Researchers that examine information systems have argued that PbD will only succeed if it is applied as part of a contextual approach rather than by attempting to quantify privacy.[62] Scholars have called, for example (and specifically with respect to PbD), for an innovative regulatory framework that will allow, if not encourage, experimentation with new technological and engineering solutions and that will facilitate agreements between organizations and regulators that are the product of discussion and negotiation.[63] On both counts, that is very similar to the conduct of the IPC in this case study.

D. The Future of PbD

How will PbD flourish now that it is about to become law in one of the largest jurisdictions in the world? This case study instructs us that it is probably not possible to develop a uniform mapping of PbD principles onto engineering and solution design. The two initiatives demonstrate just

62. Davies & Langheinrich, "Privacy by Design", *supra* note 53.
63. Rubinstein, "Regulating Privacy by Design", *supra* note 18.

how difficult it was to achieve even partial success in the implementation of PbD under what could be seen as almost ideal circumstances, of an encouraging and supportive regulator and enthusiastic (at least in the case of the OLG) organizational response. The difficulties, if not outright failure, of coherently engineering PbD point not only at the weakness of the concept but at its strength. PbD is best realized as a rallying call for privacy, as a change and leadership tool that can be used internally in an organization but also externally by the regulator.

How should European and other regulators approach PbD therefore? It seems from the case study that a mix of rigidity and flexibility is required. Rigidity is required with respect to insistence on the principle itself — that privacy must be and become a priority, that initiatives are not to proceed without privacy in mind, that privacy must be the default (in the language of Article 25). All of these should not be subject to compromise and negotiation between the regulator and regulated. Yet at the same time, the case study instructs us that regulatory flexibility with respect to the implementation of PbD in specific initiatives is absolutely required. PbD will fail if regulators develop and insist upon a uniform approach to its application.

It is likely that certification will play a significant role in the creation of this regulatory flexibility, not because of the substantive standards of certification, which could be quite detailed and quantitative, but simply by virtue of introducing intermediaries in between the regulator and the regulated. In a sense, regulatory rigidity as it relates to the details of what it means, organizationally to design privacy, will be outsourced to the certifying bodies, allowing the supervising (data protection) authorities leeway in the determination of whether specific organizations and initiatives are in compliance with Article 25. Interestingly, Cavoukian, through her PbD Centre of Excellence at Ryerson University, and in partnership with the accounting firm Deloitte, is one of the first bodies

to offer such certification.[64]

Certification, and indeed the idea of PbD itself, can also be seen as carrots offered to organizations by law instead of a heavy regulatory stick. The regulator, according to this understanding, will step back and not micro-manage the protection of privacy by organizations, but in exchange, organizations must respond by changing internally and turning privacy into one of their leading values. And that, learning from the case study, is what appears to have happened at the OLG. The IPC let the OLG facial recognition proceed at a cost to the privacy of the many visitors to the OLG's gambling sites but received the benefit of a changed organization that now has greater awareness to privacy and that willingly accepts the design of privacy into any future initiative.

The risks of such a regulatory "bargain" are clear yet may be unavoidable due to the limitations of PbD. Is the Ontario case study a red flag, a signal cautioning against determined regulatory flexibility at the expense of privacy protection? Or is it a demonstration, well ahead of its time, of a bold, new, and unconventional regulatory approach? Time will tell if this regulatory flexibility, this compromise of individual protection in consideration for organizational awareness and change, is the approach that regulators should take and whether designing privacy in such a manner will lead to the desired outcome that the *GDPR*, and similar regulatory frameworks, are intended to deliver: Privacy.

64. For some instructive details as to how Cavoukian certifies organizations, see Sylvia Kingsmill, "Privacy by Design Assessment and Certification" *Deloitte* (October 2017), online: Deloitte <www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology.pdf>.

Appendix: Interview Questions

1. What is your professional background?

2. What is your current role, and what was your role in connection with the policy of "privacy by design" that we will discuss today?

3. Please tell me about this policy:

    a. Who initiated the policy?

    b. What was the motivation for the new policy?

    c. What inspired this policy? (*e.g.* Ontario's Privacy Commissioner; the "Jerusalem declaration" of the Privacy Commissioners from 2010). What were the considerations underlying the policy and what is its purpose?

    d. What was the decision-making process concerning the implementation of the policy? (who decided, who was consulted, what preliminary steps were taken, etc.)

    e. What interaction did you have with the regulators? Was it direct (*e.g.* meetings, correspondence) or indirect? (*e.g.* reading reports)

    f. Were the implications of the policy examined? How?

4. What was the underlying concept of privacy that this policy addressed? How was the policy intended to meet the privacy needs?

5. What was the concept that founded the regulation of technological activities by legal means? Did the ability to implement the policy depend on the technology you were addressing?

6. What was the role of engineers (*e.g.* computer), and were they part of the public or private sector in the implementation of the policy? How did engineers influence the outcome?

7. What role did having or being dictated a policy have in the internal

organizational discussion about privacy?

8. How is the policy implemented in practice? Are there difficulties in its implementation? What are they? Is the policy achieving its privacy and more general objectives?