Implementing Privacy by Design through Privacy Impact Assessments

Ameya Avinash Foujdar

517858

Digital Rights and Internet Governance

The University of Turku, Faculty of Law

21/05/2019

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

UNIVERSITY OF TURKU

Faculty of Law

AMEYA FOUJDAR: Implementing Privacy by Design through Privacy Impact Assessments

Master Thesis, x + 70 pages

Master's Degree Programme in Law and Information Society

May 2019

The motivation of this study is the new recognition given to Privacy by Design through the EU General Data Protection Regulation (GDPR) 2016/679, which came into effect in summer 2018. Privacy has come a long way from being a fundamental physical right to being implemented as virtual online privacy under GDPR. One of such requirements is Data protection by Design or Privacy by Design (PbD) in business and technological systems. Aside from defining key elements in safeguarding privacy, GDPR also suggests Privacy Impact Assessment (PIA) for every new use of personal data. Privacy by Design is relatively a new concept initially developed by Ann Cavoukian. She has also developed the PbD Principles, but they by themselves do not ensure holistic implementation of the PbD process. What is lacking in the current model of PbD is an implementation mechanism or process to operationalize the whole process. Starting an informed discussion about PbD and addressing this gap of operationalization by using Privacy Impact Assessments (PIAs) as a tool is the goal of this study. Hence, this thesis brings together the two concepts and shows how PbD, as a process, can be better conducted if complimented with PIA. It aims to develop a framework for such a PIA and constructs a model to address the gaps in its operationalization. It demonstrates the proposed model by applying it to an existing information system: the Föli Mobile Application.

Contents

Table of Figures

Acknowledgments

This submission of the thesis is towards fulfillment of a requirement for the completion of the Master of Information Society and International Comparative law at the University of Turku (UTU). The author has completed a specialization in Digital Rights and Internet Governance, which is overseen by the Faculty of Law. Special thanks to my Supervisor and Responsible Professor, Juha Lavapuro, at the Faculty of Law, for all the brilliant advice he gave, in guiding me towards successful completion of this master thesis.

Ameya A. Foujdar, Finland, 2019

References

Books

- Brandeis, Samuel D. – Warren, Louis D., *The right to privacy*, BoD - Books on Demand, 2018
- Chernow, Barbara - Vallasi, George, *The Columbia Encyclopedia Fifth Edition*, MA Houghton Mifflin, 1993
- Lessig, Lawrence. *Code: And other laws of cyberspace,* second edition, Code Version 2.0, 2009.
- Levi-Faur, David, *Handbook on the Politics of Regulation*. Edward Elgar Publishing, 2011.
- Norman, Donald A., - Stephen W. Draper. *User centered system design: New perspectives on human-computer interaction*. CRC Press, 1986.
- Orwell, George, *Nineteen Eighty-Four. 1949,* The Complete Novels 7, 1990.
- Solove, Daniel J., *A Brief History of Information Privacy Law*, GW Law Faculty Publications & Other Works, 2006
- Team, ITGP Privacy. *EU general data protection regulation (GDPR): an implementation and compliance guide*. IT Governance Ltd, 2017.
- Wright, David - Paul De Hert, *Privacy impact assessment*. Springer Science & Business Media, 6/2011.

Articles

- Antón, Annie I. – Earp, Julia B. – Young, Jessica D., *How internet users' privacy concerns have evolved since 2002,* IEEE Security & Privacy Magazine, 8(1)/2010, 21–27.
- Aquilina, Kevin, *Public security versus privacy in technology law: A balancing act,* Computer Law & Security Review 26(2)/2010, pp. 130-143
- Cannataci, J. A., - Bonnici, J. P. M. *The end of the purpose-specification principle in data protection*, International Review of Law, Computers & Technology, 24(1)/2010, pp. 101–117.
- Cavoukian, Ann. *Privacy by design: the definitive workshop*. A foreword by Ann Cavoukian, Ph.D. Identity in the Information Society, 3(2)/2010, pp. 247–251
- Dinev, Tamara, *Why would we care about privacy,* 23/2014, pp. 97-102.
- Gordon, Sarah - Richard Ford. *On the definition and classification of cybercrime*, Journal in Computer Virology 2(1)/2006, pp. 13-20.

- Grodzinsky, Frances S. – Tavani, Herman T., *Verizon vs the RIAA: implications for privacy and democracy,* International Symposium on Technology and Society 2004, pp. 49-53.
- Gulliksen, J. - Göransson, B. - Boivie, I. - Blomkvist, S. - Persson, J. - Cajander, Å. *Key principles for user-centred systems design.* Behaviour & Information Technology, 22(6)/2003, pp. 397–409.
- Hoepman, Jaap-Henk, *Privacy design strategies*. IFIP International Information Security Conference, 2014, pp. 446–459.
- Kroener, Inga - Wright, David, *A Strategy for Operationalizing Privacy by Design*, The Information Society 30(5)/ 2014, pp. 355–365.
- Lambrecht, A. - Goldfarb, A. - Bonatti, A. - Ghose, A. - Goldstein, D. G. - Lewis, R. - Yao, S., *How do firms make money selling digital goods online?* Marketing Letters: A Journal of Research in Marketing, 25(3)/2014, pp. 331–341
- Lessig, Lawrence, *"The New Chicago School,"* The Journal of Legal Studies 27(S2)/1998, pp. 661-691.
- Mason, Richard, *Four Ethical Issues of the Information Age,* Management Information Systems Quarterly, 1986.
- Post, David, *What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace*, Stanford Law Review, 52/2000, p. 1439.
- Reidenberg, Joel R. *"Lex Informatica: The formulation of information policy rules through technology."* Tex. L. Rev. 76/1997, p. 553.
- Rubinstein, Ira S., *"Regulating privacy by design.",* Berkeley Technology Law Journal 26(3)/2011, p. 1409 - 1453.
- Schwerin, Simon, *Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study,* The Journal of The British Blockchain Association, 1(1)/2018, pp. 1 – 75.
- Tamara, Dinev – Hart, Paul, *An extended privacy calculus model for e-commerce transactions,* Information systems research 17(1)/2006, pp. 61-80.
- van Sinderen, Marten J. - Aart Tijmen van Halteren - Maarten Wegdam, Hendrik B. Meeuwissen - E. Henk Eertink. *"Supporting context-aware mobile applications: an infrastructure approach."* IEEE Communications Magazine 44(9)/2006, pp. 96-104.
- Zeviar-Geese, Gabriole. *"The State of the Law on Cyberjursidiction and Cybercrime on the Internet."* Gonz. J. Int'l L. 1/1997, p. 119.

Conferences and Workshops

- Everson, Eric. *"Privacy by Design: Taking Ctrl of Big Data."* Cleveland State Law Review, 65(1)/2016, pp. 27-44.
- Ibrahim, S. Z. - Blandford, A. - Bianchi-Berthouze, N. *Privacy Settings on Facebook: Their Roles and Importance.* IEEE International Conference on Green Computing and Communications, 2012.
- Kohei, Arai – Rahul, Bhatia – Supriya, Kapoor, *Proceedings of the Future Technologies Conference* (FTC) 1/2018.
- Lawrence, Lessig, *Architecting for Control*, Keynote given at the Internet Political Economy Forum Cambridge Review of International Affairs, 2000. Written Transcript.
- Romanosky, S. - Acquisti, A. - Hong, J. - Cranor, L. F. - Friedman, B. *Privacy patterns for online interactions.* Proceedings of the 2006 Conference on Pattern Languages of Programs – PloP, 2006. Online at: https://dl.acm.org/citation.cfm?id=1415486 Accessed on: 12th May 2019
- Tesfay, W. B. - Hofmann, P. - Nakamura, T. - Kiyomoto, S. - & Serna, J., *Privacy Guide, Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics* – IWSPA, 2018

Laws & Standards

- Act, Data Protection. *Conducting privacy impact assessments code of practice*. Technical Report. Information Commissioners Office (ICO), 2014.
- Article 29 17/EN WP 248 rev.01 of Directive 95/46/EC Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*
- OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* 1918. Online at: https://www.oecd.org/sti/ieconomy/privacy.htm Accessed on: May 14, 2019.
- Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)

Opinions and guidelines

- Cavoukian, Ann, *Privacy by design: The 7 foundational principles*, Information and Privacy Commissioner of Ontario, Canada, 2009.

- Cavoukian, Ann, *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, 2005. Available at: https://www.ipc.on.ca/wp-content/uploads/resources/phipa_pia-e.pdf Accessed on: 12th May 2019
- Nokia, *Privacy Engineering & Assurance: The Emerging Engineering Discipline for implementing Privacy by Design,* Position paper, 2014. Online at: *https://www.w3.org/2014/privacyws/pp/Hirsch.pdf*, Last Accessed: 22.2.2019

Websites

- AUSTRAC, *Australian Transaction Reports and Analysis Centre, Risk management - A tool for small-to-medium sized businesses*, Australian Government, 2014. Online at: http://www.austrac.gov.au/risk-management-tool-small-medium-sized-businesses Accessed on: 12th May 2019
- Byer, Brian, *Internet Users Worry About Online Privacy but Feel Powerless to Do Much About It,* Entrepreneur Europe, 2018 Online at: *https://www.entrepreneur.com/article/314524* Accessed on: 12th May 2019
- *Digital 2019: Global Digital Overview*, 2019, Published on dataportal.com, Online at: *https://datareportal.com/reports/digital-2019-global-digital-overview* Accessed on: 12th May 2019
- Eurostat, *Digital economy and digital society statistics at regional level,* 2018. Available online at: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_digital_society_statistics Accessed on 12th May 2019
- Mander, Jason, *Digital consumers online for average of 6 hours per day*, GlobalWebIndex, 2015. Online at: https://blog.globalwebindex.com/chart-of-the-day/digital-consumers-online-for-average-of-6-hours-per-day/ Accessed on: 12th May 2019
- Net Market share, *April 2019 market share reports, Operating System Market Share*, Market Share Statistics for Internet Technologies, 2019. Online at: *https://netmarketshare.com/operating-system-market-share.aspx* Accessed on: 12th May 2019
- Phan, Kim – DeRitis, Fred G. - Shiroff, Justin A., *Privacy and Data Security and Emerging Technologies – Spotlight on the Internet of Things and Biometrics*, Ballard Spahr LLP, 2018 Available online: *https://www.cyberadviserblog.com/2018/01/pds-emerging-technologies-spotlight-internet-things-biometrics/* Accessed on: 12th May 2019

- Privacy by Design, General Data Protection Regulation (GDPR), Online at: https://gdpr-info.eu/issues/privacy-by-design/ Accessed May 14, 2019.
- Ryerson University, Privacy by Design Centre for Excellence, *Privacy by Design Certification*. Online at: https://www.ryerson.ca/pbdce/certification/ Also, Deloitte LLP, *'Privacy by Design controls framework' developed as a part of 'Privacy by Design Certification Program: Assessment Control Framework',* Available online at: *https://iapp.org/media/pdf/resource_center/Privacy-by-Design-Certification-Program-Assessment-Methodology-20161011.pdf* Accessed on 12th May 2019
- *Turku Region Public Transport System – Payiq, Online at: https://payiq.net/turku-public-transport/ Accessed May 14, 2019*
- Walters, Pennie, *The Risks of Using Portable Devices*, Carnegie Mellon University. Produced for US-CERT, a government organization, 2012, pp. 1-5 Online at: *https://www.us-cert.gov/sites/default/files/* Accessed on: 12th May 2019

Reports

- Cavoukian, Ann, *Privacy by design in law, policy and practice: A white paper for regulators, decision-makers and policymakers*, 2011. Online at: http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf Accessed on: 12th May 2019
- Office of the Privacy Commissioner of New Zealand, *Privacy Impact Assessment Toolkit*, 2015. Part 1 and 2. Online at: https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/ Accessed on: 12th May 2019

Abbreviations

PbD	Privacy by Design
GDPR	General Data Protection Regulation
DPD	Data Protection Directive
PETs	Privacy-Enhancing Technologies
EU	European Union
FIP	Fair Information Practices
PIN	Personal identification number
PrM	Privacy Preserving Measures
UTU	University of Turku

1. Introduction

In the current internet-based society, privacy concerns have risen and taken a completely new form. The EU has taken the lead in harmonizing the phenomenon through the GDPR. Although only time will establish the effectiveness of GDPR, it goes without doubt that this legislation presents something that is much needed today due to major privacy leaks across the world like Facebook and Cambridge Analytica. A lot of these privacy breaches happen because of inherent flaws in their designs that fail to protect the privacy of their users. This event has highlighted the gap between the design of information systems and their effective privacy regulation. This has increased the importance of organizations around the world to embrace the concept of privacy within the design of information systems. This is the concept of Privacy by Design (PbD). GDPR replaced Directive 95/46/EC introducing many changes, one being Privacy by Design. Privacy by Design is a concept initially developed by Dr. Ann Cavoukian while she was the Privacy Commissioner of Ontario, Canada. She has also developed the various elements of PbD, also known as the Privacy by Design Principles. Considering the important nature of the principles they by themselves do not ensure holistic implementation of the PbD process. What is currently lacking to operationalize PbD is an implementation mechanism or process. There is an acute lack of a framework to implement PbD within information systems, and currently, there exists no model to achieve this. This thesis aims to formulate a framework and develop a way to operationalize the PbD Process.

Firstly, this thesis aims to study how Privacy by Design (PbD) is a necessary process, how it has a strong theoretical basis under Lessig's Theory of Regulation and how this process can be operationalized. As GDPR or any other legislation does not provide any operationalizing process regarding implementing the PbD process within information systems, this paper will create a *'PbD process model'(hereinafter 'model')* to operationalize the said process. This model will, as proposed by Kroener and Wright[1], comprise of a set of principles, i.e., PbD Principles and a process, i.e., the process being a PIA. The 7 Foundational Principles developed by Ann Cavoukian are used as PbD principles to build a workable model to implement PbD process using PIAs.[2] The assessment of compliance with PbD principles is done by using the model developed by Privacy by Design Centre for Excellence under the guidance of Ann

[1] *Kroener – Wright 2014*
[2] *Cavoukian 2009*

Cavoukian.[3] A whitepaper developed by her is also used for this purpose.[4] The Risk assessment stage of the PIA is done by utilizing a risk matrix developed the Australian Government as its flexible nature enables use irrespective of the size of the system.[5] Further, the inspiration behind the structure of the PIA process and checkpoint creation is the New Zealand Privacy Toolkit.[6] This multidisciplinary model developed to conduct PbD process should help in understanding the privacy concerns present in the currently implemented design of the system and will then enable devising improvements and solutions to existing privacy issues and additionally will also serve as a guide for future developers to implement PbD in the lifecycle of their projects. Lastly, it will be shown how Privacy Preserving Measures (PrMs) can be used to show the presence of PbD Principles, thus proving compliance of the system to Privacy by Design. It is the goal of the thesis to start a much-needed discussion about the PbD process and show that this process can indeed be carried out though PIAs. A model to develop this process within the lifecycle of a system is also developed in this thesis using the specifications above.

To display the above-proposed model and the effectiveness of using Privacy Impact Assessments (PIAs) for PbD process, a demonstration is conducted within this thesis of an existing information system. This demonstration involves applying the proposed model to an existing system. The system that is chosen for the purpose of this demonstration will be based on it, having a good privacy track record. Using such a system will help demonstrate how Privacy Preserving Measures (PrMs), detected during this PIA, can be used to show compliance of PbD Principles. This PIA will be conducted to demonstrate the workability of the proposed model purely for academic purposes and is based on publically available relevant online documents of the organization. In a practical situation, the company will have more data at its disposal to conduct a PIA. The PIA in this thesis is just for the purpose of demonstrating the complementary nature of PbD and PIA, and thus, the data derived from the public online sources are sufficient to demonstrate this relationship.

The scope of this study is to address the aforementioned vacuum of standardization present in the operationalization of PbD as a process by formulating a model to do the same. The model will then be used to analyze a system and show that the two concepts do work together. The thesis proposes that PIAs can be an effective means of implementing PbD within the lifecycle of a project. Concerned stakeholders will be offered a copy of the study results if they so desire.

---

[3] *Ryerson University, Privacy by Design Centre for Excellence, Privacy by Design Certification. Online at: https://www.ryerson.ca/pbdce/certification/*
[4] *Cavoukian 2011.*
[5] *AUSTRAC 2014.*
[6] *Office of the Privacy Commissioner of New Zealand 2015*

The operationalizing element of Privacy Enhancing Technologies (PETs) are not within the scope of this thesis and require further work.

The objectives of the thesis are to be achieved by a review of the literature mentioned above to construct the PIA process and to operationalize PbD. Also, additional literature will be used to analyze the necessity, legal basis, and complementary nature of PIA and PbD. For the purpose of demonstrating the PbD process model, a PIA of the system Föli is conducted. For this PIA, Privacy Policy of the Application, along with other documents, is used. At multiple points within the thesis, illustrative figures have been shown to explain the concepts, and a flowchart will be used to demonstrate the final developed lifecycle model.

The introductory chapter of this thesis will explain the various concepts related to privacy. It will show how privacy has evolved from physical privacy to virtual privacy. It will also briefly introduce the legislation and literature regarding privacy and privacy by design, specifically the General Data Protection Regulation as it is the bastion leading in Privacy legislation around the world. Then the thesis will connect privacy to its design aspect and will show the theoretical basis of PbD by using Lessig's Theory of Regulation. Then the thesis will try to address the gap in the operationalization of PbD process and will propose using PIAs to fill the gap created by lack of regulation. For this purpose, the common aspects of both concepts will be analyzed. After presenting the Assessment Framework to check compliance of PbD Principles within the PIA, a working PIA model will be constructed. The model will then be demonstrated using the Föli system. The thesis will conclude by showing that the compliance to PbD principles can be effectively demonstrated by detecting Privacy Preserving Measures (PrMs). Along with this, a model to implement this developed PIA throughout the lifecycle of a system will be presented.

1.1 The journey from physical privacy to virtual privacy

The notion of the right to privacy concerning protecting a person and property is as old as the common law itself.[7] It is also inherent to every democratic society.[8] From time to time as technology advances laws have to update to keep up with it and the law of privacy has gone through this process of playing catch-up for over a decade as we have transitioned into the information and technological revolution.[9] These transitions often result in the emergence of new rights depending on the political, social, and economic factors to meet the demands of society.[10] As a result, multiple legal fields about privacy have emerged, namely, the common

[7] *Brandeis – Warren 2018, pp. 2-3*
[8] *Grodzinsky - Tavani 2004, p. 50*
[9] *Brandeis – Warren 2018, pp. 2-3*
[10] *Brandeis – Warren 2018, pp. 2-3*

law torts, criminal law, constitutional law, national laws, and supranational laws.[11] It is possible to link the emergence of information privacy to new technological developments happening around the world that have poised limitations to the ability of people to protect their personal information.[12] The creation of demand for new laws to address changes in technology that increase collection, dissemination, and use of personal information.[13] The Internet is now an integral part of the social and economic aspects of society, and hence, there was a societal necessity to interpret and evolve privacy in the context of the internet.[14] Because of the number of people accessing the internet reaching four billion in 2018, it is evident that surfing the Web has now become a daily activity. [15] Information now pervades everything, from buying a movie ticket to ordering food. It is not just the amount of people using the internet, but also people on average spend 6 hours each day using internet-powered devices and services, which is one-third of their waking lives.[16] People now socialize online and store a lot of their personal life online. The interactions that people have online have increased, and so has the activity of recording and processing them, for example, liking or disliking something on social media.[17] The adverse effects of breach of privacy were first illustrated by George Orwell in 1949.[18] In his book, the country of Great Britain *("Airstrip One")* has become a province of a super-state called Oceania. Oceania is presided over by the *"Party,"* who recruits the *"Thought Police"* to persecute individualism and independent thinking.[19] Thus, he describes the creation of a totalitarian society due to the government abusing the right to privacy. All this without the existence of the internet. The problem has only intensified since the advent of the information age.[20] Personal communication and access to services, everything can be done on this information superhighway. Internet penetration in Northern Europe is the highest in the world.[21] There are regions in the EU with 95% of the population using the internet.[22]

Although there is a considerable digital divide regarding internet penetration in comparison with some of the underdeveloped nations, the pace at which this divide is reducing is unprecedented.[23] Online services involve the collection, storage, analysis and sharing of the

[11] *Solove, Daniel J. 2006, pp 1-3*
[12] *Tamara, Dinev – Hart, Paul 2006, p. 61*
[13] *Solove, Daniel J. 2006, pp 1-3*
[14] *Antón, Annie I. – Earp, Julia B. – Young, Jessica D. 2010, p. 22*
[15] *Digital 2019: Global Digital Overview 2019, online report, "The number of internet users in 2018 is 4.021 billion, up 7 percent year-on-year, social media users are 3.196 billion and mobile phone users are 5.135 billion"*
[16] *Mander 2015, website*
[17] *Antón – Earp – Young 2010, pp. 21-22*
[18] *Orwell 1990*
[19] *Chernow - Vallasi 1993, p. 2030*
[20] *Mason 1986, p. 5*
[21] *Eurostat 2018, website*
[22] *Eurostat 2018, website*
[23] *Digital 2019: Global Digital Overview 2019, online report*

personal information for either delivery of the service or just for profit.[24] The services involve both public and private sectors some of which are e-commerce, social networks, government services, and surveillance.[25] The amount of data transferred through online services has increased exponentially over time due to technological innovations like biometrics, smart devices, or the Internet of Things.[26] Most services on the internet involve the use of personal information. It is this personal information that is subject to protection on the internet.

Over the years, Privacy-Intrusive Technologies have appeared over the horizon and have motivated the evolution of law to safeguard user's personal information on the internet.[27] For this purpose, PETs or Privacy-Enhancing Technologies have been developed, which through implementing an array of principles like a limitation on collection of data, giving notice to users or specifying which data is collected attempt to enhance user privacy.[28]

Thus, the evolution of privacy to the virtual domain was imminent, and now legislation around the world are contemplating different ways to approach the concept. This thesis is about one such way to achieve virtual privacy which is Privacy by Design (PbD). This paper will initially introduce the concept of PbD and talk about the recognition it has received from prominent legislations around the world. It will then proceed to address the issue of implementing this process through an organizational measure called Privacy Impact assessment. The paper will then develop a model where PbD and PIA work together to develop a privacy-centric ecosystem throughout the lifecycle of a project. Application of PIA based PbD model to an existing system will act as a proof of their complementary nature. The primary aim of the thesis is to show that PIA is an effective way to begin PbD and to conduct the PbD process throughout the lifecycle of a project.

1.2 Recent recognition was given by Legislation

Enforced on 25 May 2018, the EU's General Data Protection Regulation (GDPR) harmonizes the handling of personal information of EU residents. GDPR is a result of the rising global concerns towards the safety of an individual's personal information on the internet.[29] It also showcases the growing global recognition given to the value of an individual's personal information. Aside from the fact that the internet has been around for a while now[30], the concern

[24] *Lambrecht - Goldfarb - Bonatti - Ghose - Goldstein - Lewis - Yao 2014, p. 332*
[25] *Dinev 2014, p. 97*
[26] *Phan – DeRitis - Shiroff 2018, website*
[27] *Aquilina 2010, p. 142*
[28] *Aquilina 2010, pp. 135-136*
[29] *Tesfay - Hofmann - Nakamura - Kiyomoto - & Serna 2018, pp. 15-16*
[30] *It was on 6 August 1991 that the World Wide Web went live for the first time.*

and value for personal information have only recently increased.[31] A pocket-sized computer capable of high processing power has made it possible for every individual to have access to all services through the same device from anywhere at high speed.[32] Often these services are accessed using an individual's personal information. Technology has enabled the traditional acts of theft to transcend into the digital realm and thus resulting in *'cyber theft'* of personal information. The result is criminals adapting to the new technological frontier and has resulted in the creation of an array of *'cyber-crimes.'*

The term cybercrime has evolved experientially and is thus hard to define as they occur within many different facets and in a wide variety of scenarios and environments.[33] The meaning is also subjective, i.e. it depends on the perception of both observer/protector and victim and is partly a function of computer-related crimes geographic evolution.[34] The Council of Europe's Cybercrime Treaty uses the term *"Cybercrime"* in a much broader sense to include offenses ranging from criminal activity against data to content and copyright infringement.[35] However, some suggest that the definition is even more extensive and includes credit card fraud, software piracy, unauthorized access, child pornography, and cyberstalking.[36] It is accepted that cybercrime is a broad term and has evolved recently; it is a severe threat to personal information.

New technologies like Bigdata analysis allows organizations to track and predict individual behavior and also use invasive privacy techniques like automated decision-making. These problems, combined with advanced technology and issues about the infringement of personal data by public and private bodies, has resulted in the EU passing new laws to clarify the data rights and to ensure an appropriate level of EU-wide protection for personal data.[37]

Twenty years before GDPR, the DPD (Data Protection Directive) had implanted standards for EU data protection. Within the EU, the states are free to legislate their laws as long as they do not interfere with the common EU standards. The result has been EU states making their laws to protect the personal information that exceeded the standards of DPD. Hence, there has been the creation of a lot of complex webs of laws for each state. It made the understanding of the rights increasingly tricky for EU citizens. The EU Commission decided to unify the law which would be an effective way of achieving firstly, protection of the rights, privacy, and freedoms

[31] *Byer 2018, website*
[32] *Walters 2012, p.1*
[33] *Gordon - Ford 2006, p. 1*
[34] *Gordon - Ford 2006, p. 2*
[35] *Gordon - Ford 2006, p. 2*
[36] *Zeviar-Geese 1997, p. 1*
[37] *Team, ITGP Privacy 2017, pp. 1-2*

of natural persons in the EU and secondly, decrease the barriers to free business by facilitating the free and easy movement of data throughout the EU.[38]

GDPR requires all data controllers and processors that handle the personal information of EU residents to "implement appropriate technical and organizational measures […] to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" or face fines of up to €20 million or 4% of annual global turnover – whichever is the greatest.[39]

In the context of this thesis, GDPR plays an influential role as it is the leader in privacy legislation around the world. It is also one of the first to give recognition to PbD and some of its principles. Thus, GDPR has been one of the main motivations of this study.

2. Connecting privacy to design

Most of the consumers in 2019 access services provided on the internet through their mobile devices.[40] It has become customary for an online service provider to have an application for mobile devices, at least for the two most popular platforms, namely, Android and Apple.[41] As a service jumps from one platform to the other, accessibility or user-friendly access becomes essential. The nature of services now being multiplatform is pertinent as most online services are personalized towards the users. Also, an essential factor is that mobile devices are entirely different from standard desktop devices not just regarding their size but also the various features and sensors. Mobile devices have additional sensors like proximity sensor, Bluetooth, GPS and motion sensors which forms a part of the Application layer.[42] They can collect even more user data than a conventional desktop device, and they personalize the services, even more, depending on the context of usage.[43] Due to more data existing online, easier deidentification, higher rewards for exploitation and more information being available publicly, there more are the avenues for exploitation.[44] Thus, this makes the design focus of the application critical from the perspective of safeguarding the privacy of the user. The past has shown with Facebook and Cambridge Analytica that bad design concerning privacy settings leads to privacy issues.[45]

[38] *Team, ITGP Privacy 2017, pp. 1-2*
[39] *Team, ITGP Privacy 2017, pp. 80-81*
[40] *Digital 2019: Global Digital Overview 2019, online report, "There are 5.11 billion unique mobile users in the world today. 3.26 billion people use social media on mobile devices in January 2019."*
[41] *Net Market share 2019, website*
[42] *van Sinderen - Aart Tijmen van Halteren - Meeuwissen - Eertink 2006, pp. 96-97*
[43] *van Sinderen - Aart Tijmen van Halteren - Meeuwissen - Eertink 2006, p. 97*
[44] *Romanosky – Acquisti – Hong - Cranor - Friedman 2006, p.1*
[45] *Ibrahim - Blandford - Bianchi-Berthouze 2012, p. 427*

Thus, an application made with good privacy design and with the consideration of safeguarding data will better guard the data of the user and deliver services without any threat to user privacy.

The users of these devices, be it mobile or desktop, interact with the user interface of the online service. This interface is the design that the user interacts with which enables him to receive the services. Thus, it is vital that the design is centered around the requirements and privacy of the user and this is the thought behind the concept of UCD (or User-Centered Design).

Norman in his book states *that 'user-centered design emphasizes that the purpose of the system is to serve the user, not to use a specific technology, not to be an elegant piece of programming. The needs of the users should dominate the design of the interface, and the needs of the interface should dominate the design of the rest of the system.'*[46]

Thus, at the heart of a UCD should the user and his/her best interests. PbD places privacy, which is a user-centric requirement, at the heart of the design of a system. Principles of UCD are elucidated well by Gulliksen, J., Göransson, B., Boivie, I., Blomkvist, S., Persson, J., & Cajander in their work.[47] These UCD principles serve as a useful guide when organizations want to implement privacy principles into the design of their systems. The principles talk about how the design should be evolutionary, simple representation, prototyped, explicit and conscious, professional and multidisciplinary, usability champion, holistic, process customized and should imbibe a user-centric attitude. The main takeaway from all these principles in the context of Privacy by Design is that the user and the design of the service are inherently related. It also shows that it is possible to have a design that can imbibe certain principles to deliver a specific user-centric approach. Hence, the whole ideology of protecting the privacy of a user online can achieve by modifying the design of a system to make it more centered around the privacy of the individual. The idea of a user-centric approach to privacy design is what was precisely envisioned by Ann Cavoukian, former privacy commissioner of Ontario when she came up with the principles of privacy by design.[48] Making the design privacy-proof and resistant to infringements is the primary motivation of the concept of Privacy by Design.

In order to understand how the law of privacy and the architectural design of systems can be used to produce good Privacy by Design, it is necessary to put PbD under the theoretical magnifying glass developed by Lawrence Lessig called the Theory of Regulation.[49]

---

[46] *Norman, Donald A. 1986, p. 67*
[47] *Gulliksen - Göransson - Boivie - Blomkvist - Persson - Cajander 2003, pp. 401 - 403*
[48] *Ibid Cavoukian 2011*
[49] *Lessig 2009*

2.1 Controlling the design of cyberspace through the law

With time technology evolves and with it so do our concerns regarding its impact on various social aspects of life. During the times, when cyberspace was not a part of daily life, privacy was limited to social and physical notions. Now, with technology evolving and becoming an integral part of daily life it is only natural that our desires to uphold the fundamental right of privacy evolve alongside it. The struggle of law trying to grapple around the ever-evolving cyberspace is not new, and the emergence of Privacy by Design (PbD) is the result of this struggle. In order to understand how the law of privacy and the architectural design of systems can be used to produce good Privacy by Design, it is firstly needed to understand the workings of Lessig's theory of regulation, code as law, and secondly, the concept of PbD. After that this section will then proceed to explain how PbD has a strong and evident theoretical base through Lessig's theory of regulation and can indeed possible to regulate the design of cyberspace through law.

2.1.1 Lessig's Theory of Regulation

Lawrence Lessig is the pioneer behind developing the complex academic theories on regulation and then applying the same to the regulation of cyberspace.[50] His approach to regulation has been 'general in nature,'[51] which means that in order to control the new regulator of the 21st century, i.e. *'code,'*[52] Lessig's approach is to look at regulation from a broader and simpler perspective: the four constraining forces[53]. His Pathetic Dot model attempts to implement this general outlook on the concept of regulation for a better understanding of how to regulate the internet. Introduced by Lessig in the *'New Chicago School'*[54] and made famous in his subsequent book, *Code Version 2.0, Code and Other Laws of Cyberspace,* the Pathetic Dot Model is a well-accepted theory of regulation.[55]

According to this model, Lessig identifies four prominent forces that play an active part in constraining the actions of the 'dot.'[56] The dot, in this case, is the individual, whom Lessig says can be *"a creature (you or me)"* i.e., any layperson.[57] In his theory of regulation, Lessig uses

---

[50] *Lessig 2009, p. 124*
[51] *Lessig 2009, p. 121*
[52] *Lessig 2009, p. 121. According to Lessig "Threats to liberty change". Over time threats to liberty tend to change and the same is true for threats on cyberspace in the 21st century. He calls the new regulator of cyberspace as 'code' i.e. "the instructions embedded in the software or hardware that makes cyber space what it is." The code is used to build the social environment of the internet, hence also known as the 'architecture'.*
[53] *Lessig 2009, p. 123. According to Lessig the 4 constraints of regulation are: the law, social norms, the market, and architecture. The regulation of a person (the dot) is the sum of these four constraints. More about these forces is explained subsequently in the answer.*
[54] *Lessig 1998*
[55] *Lessig 2009*
[56] *Lessig 2009, p. 123*
[57] *Lessig 2009, p. 122*

this dot to show how regulation as a concept works from the perspective of an individual who is regulated. Through well-demonstrated examples in his literature,[58] Lessig shows how the four forces - the law, social norms, the market, and architecture – are used to regulate the behavior of individuals in different aspects of society. The interplay between the forces is collective, and changes in one affect the regulation of the whole. Each constraint is called a regulator.

The four forces applying regulatory constraints on an individual's behavior is called the 'Old Chicago School.' Under the New Chicago School model, each alternative constraint is seen as subject to the law.[59] Thus, the law is seen as a constraint that can affect other alternatives.[60] The ability of the law to affect other alternatives introduces a new dimension to regulate individual behavior indirectly by law affecting other constraints. Thus, the regulation under the New Chicago school has two aspects, namely, direct and indirect.

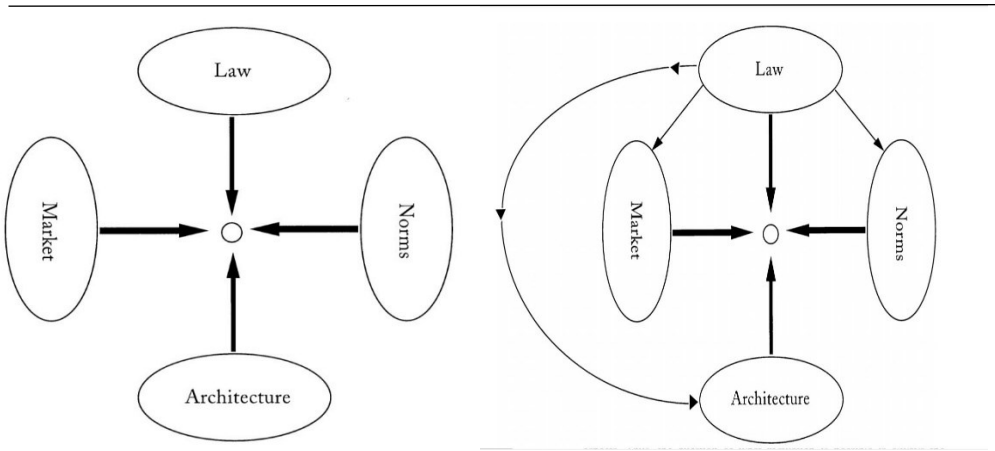


Figure 1 Old and new Chicago School

Source: Lessig 1998, p. 667

[58] *Lessig 1998 pp. 667-672, well elucidated examples on regulation using the Pathetic Dot Model of smoking, seat belts, discrimination against the disabled, drugs and abortion can be found. In each of these examples Lessig analyses the 4 forces of constraint and presents how law regulates the dot directly and indirectly.*

[59] *Lessig 1998, p. 666*

[60] *Lessig 1998, p. 666, "Norms might constrain, but law can affect norms (think of advertising campaigns); architecture might constrain, but law can alter architecture (think of building codes); and the market might constrain, but law constitutes and can modify the market (taxes, subsidy)."*

2.1.2 Applying the Theory of Regulation to PbD

The establishing of these constraints makes it is possible to apply them to PbD. Let us begin by understanding PbD. The White Paper for Regulators, Decision-makers, and Policy-makers by Ontario's Privacy Commissioner states the following:

"The aim of Privacy by Design (PbD) – the philosophy and methodology of embedding privacy into the design specifications of information technologies, business practices, and networked infrastructures as core functionality. Privacy by Design means building in privacy right up front, directly into the design specifications and architecture of new systems and processes."[61]

Developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, the concept of PbD is now a well-known function of Privacy law[62]. It was developed in the 1900s as a response to the growing threats to online privacy.[63]

While applying the theory of regulation to cyberspace, the code embedded in the software and hardware constitutes the architecture of cyberspace. PbD creates a model to influence, shape, and regulate this architecture to achieve multiple functions, including upholding privacy.[64] In the context of privacy, all the four constraints of Lessig's model are valid. Privacy in cyberspace is all about protecting personal data. Let us take the example of EU legislation. In this case, the law to protect privacy passed by the government, GDPR, penalizes the misuse of personal information. This law attempts to regulate the behavior it wants to change directly, i.e., stop people from infringing individual privacy. PbD in this context falls under the indirect attempt of law to regulate the architecture of cyberspace.

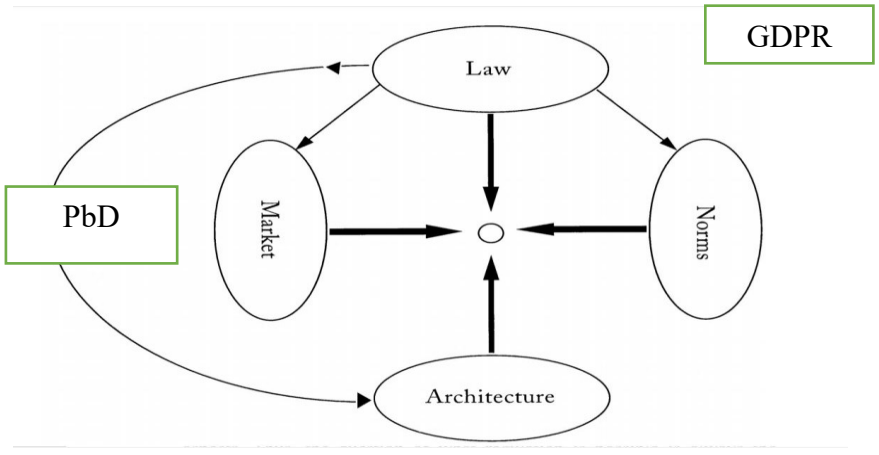


Figure 2 Pathetic Dot applied to PbD (EU example)

[61] *Cavoukian 2011, p.10.*
[62] *Article 25, Regulation (EU) 2016/679 GDPR*
[63] *Cavoukian 2011, p. 3*
[64] *Cavoukian 2011, p.13*

The table below shows how in the context of privacy, all the four constraints of Lessig's model are valid and PbD is the indirect legal constraint on the architecture of cyberspace.

New Chicago School: Regulating behavior in cyberspace directly and indirectly through law

Smoking	Privacy Infringement
Objective = Reduce Cigarette consumption Product = Cigarettes Market = Cigarette market supply chain Norm = Public perception of smoking Realm = Real World	Objective = Reduce personal data infringements Product = Individual's personal information Market = Information on cyberspace Norm = Public perception of privacy Realm = Cyberspace
• Direct legal regulation: Ban Cigarette consumption.	• Direct legal regulation: Ban misuse of personal information.
• Indirect legal regulation: Architecture Regulate nicotine in cigarettes, requiring manufacturers to reduce or eliminate nicotine.	• **Indirect legal regulation: Architecture** **Regulate the code to mandate PbD principles into the very design of information technologies, network infrastructure, and processes.**
• Indirect legal regulation: Market Tax cigarettes to reduce supply and accessibility.	• Indirect legal regulation: Market Supply and demand dynamics of information are changed as companies cannot use personal information of people without explicit consent. Consent requirement to collect and process personal information changes its accessibility in the cybermarket.
• Indirect legal regulation: norms Introduce law to fund a public ad campaign against smoking.	• Indirect legal regulation: norms Introduce law to fund a public awareness campaign to show the effects of misuse of personal data. Law to educate children from an early age about privacy. Educate senior

	adults suffering from digital – divide about online privacy.

2.1.3 Code as Law

The Cyberpaternalist School has always advocated design based regulation through code (architecture) of cyberspace.[65] This school of thought was formed in the late 90s after a series of papers by Jack Goldsmith's *'Against cyberanarchy,'* Joel Reidenberg's *'Lex Informatica'*[66] and Lawrence Lessig's *'The law of the horse: what cyberlaw might teach.'* Reidenberg believed that regulation through technical protocols and design of cyberspace is as effective or even more effective than traditional state laws.[67] Reidenberg advocated that network designers regulated by traditional lawmakers should control changes to cyberspace. He stated six ways for traditional lawmakers to facilitate the regulatory development of cyberspace: "(1) the bully pulpit[68], (2) participation, (3) funding, (4) procurement, (5) regulated behavior and (6) regulated standards." Later Reidenberg's approach was adopted by Lawrence Lessig to develop the book: *Code and Other Laws of Cyberspace*. Thus, the four constraining forces, the modalities were formulated.

The four modalities (constraints) of regulation regularly interact with each other. One modality may enable the other, or it might undermine the other.[69] Adopting Reidenberg's Lex Informatica theory, Lessig suggests that Cyberspace is different from real physical space in a regulatory sense. In real space, architectural controls are constrained by fundamental physical laws of nature. It is either possible to regulate by designing a change in the environment, or we can leave the universal laws in place.[70] Murray and Andrew say that,

"In Cyberspace when one escapes the basic carrier level of cables, servers, and routers, there is no predesigned environment. We design that environment to achieve whichever ends we want, and we do so by designing the software which manages the environment. We can design software that allows for privacy or which removes it; we can design software which will filter content, or which will not; we can design software which allows files to be shared across peers or which does not."

[65] *Levi-Faur 2011, p. 271*
[66] *Reidenberg 1997*
[67] *Levi-Faur 2011, p. 272*
[68] *Reidenberg 1997, p. 588. According to Reidenberg, "Government can use the bully pulpit approach to threaten and cajole industry to develop technical rules. For example, in the context of children's programming, the Senate sought to encourage video games producers to restrain the dissemination of violent programming to children."*
[69] *Lessig 2000, p. 4*
[70] *Levi-Faur 2011, p. 274*

Thus, cyberspace architecture is made by us, and hence the Cyberpaternalist School sees the code as a potentially perfect, covert regulator.[71] The nature of regulation is *ex-ante*[72] , and hence there is not much the user can do but comply. This type of regulation also has the threatening possibility of the internet completely losing its autonomy and personalization.[73] Hence, here Reidenberg and Lessig's combined model of online and offline regulation works best.[74] Then, there are also arguments and critiques by Cyberlibertarians like David Post[75], who says that internet regulation should not be directed paternalistically. Post belongs to the Cyberlibertarian school of thought and does not believe that if left unregulated commerce will dictate the future terms of internet regulation. He believes in self-regulation.[76]

Finally, while applying the theory of regulation to code, it is essential to understand the architecture constraint has a more *"virulent interaction"* in cyberspace.[77] This interaction is because it is a platform that is designed entirely by humans with code, unlike the architecture of the real world which is based on laws of physics and biology. A lot depends on the design of the architecture of cyberspace; for example, the design might either enable the effect of social norms or based on the design it might disable that capability. The same is true for the market function as it can either enable it or make it too costly. The code decides what is enabled and disabled and how the nature of life on cyberspace. Thus, the code can be a perfect tool for regulation of cyberspace indirectly through the law (code as law).

2.1.4 PbD has a robust theoretical basis under the Theory of Regulation

The pathetic dot theory or the New Chicago School theory is the theory of regulation. It identifies forces that constrain individual behavior and narrow them down to four: the law, social norms, the market, and architecture.

PbD has a robust theoretical basis within Lessig's theory of regulation as it aims to harness the power of architecture of the internet to regulate and enforce the principles of privacy and data protection within the fabric of cyberspace. The strong theoretical basis is because the design-based regulation through architecture is arguably (according to Reidenberg and Lessig) able to regulate cyberspace as effectively as, or even more effective than, traditional state-based laws.[78] The architecture of cyberspace is inherently different from real-world architecture as humans

[71] *Levi-Faur 2011, p. 274*
[72] *In this case this means the regulation is implemented within the network in the background of cyberspace.*
[73] *Levi-Faur 2011, p. 273*
[74] *In this context online and offline regulation refers to network designers being regulated by traditional lawmakers.*
[75] *Post 2000.*
[76] *Levi-Faur 2011, p. 275*
[77] *Lessig 2000, p. 4*
[78] *Levi-Faur 2011, p. 272*

can directly and easily manipulate it. PbD's nature to alter the architecture of cyberspace to protect privacy perfectly fits within Lessig's indirect regulation through law aimed at changing individual behavior by regulating the very architecture (code) of cyberspace.

3. Privacy by Design

3.1 Protection of Data through Design

Lawrence Lessig in his Pathetic Dot Theory argues that multiple constraints affect the behavior of an individual.[79] Lessig and Reidenberg, who belong to the Cyberpaternalist school of thought, believe that the most effective way to regulate cyberspace is by regulating behavior indirectly through the architecture of cyberspace, i.e., the code.[80] They suggest a blend of traditional lawmaking (offline regulation) to regulate network architects (online regulation). This blend they say will also preserve the autonomy and personalization aspects of the internet. PbD is a process that does precisely this; it indirectly regulates behavior on cyberspace through its architecture.[81] The ability of law to control architecture of the internet has not gone unnoticed and finds its way in many of the world's IT legislation, including GDPR.[82] "The aim of Privacy by Design (PbD) is embedding privacy into the design specifications of information technologies, business practices, and networked infrastructures as core functionality. Privacy by Design means building in privacy right up front, directly into the design specifications and architecture of new systems and processes."[83] This definition is similar to how Ann Cavoukian defined PbD in her famous whitepaper.[84] PbD intends to incorporate its privacy principles into the very fabric of the development process of IT systems and aims to secure them against privacy breaches from the get-go. With the increasing awareness of privacy and now with prominent legislation, the 7 Foundational Principles of PbD are garnering the attention of policymakers and industry stakeholders alike. This attention has played an important part in opening a dialogue about the range of instruments can complement the process of PbD, how and at what stage PbD may be incorporated, in ways that preserve its characteristics.[85]

Instructions embedded into software and hardware make cyberspace what it is – they are its architecture. PbD offers a framework for influencing, shaping and regulating this architecture in ways that recognize multiple legitimate functionalities, including privacy.

---

[79] *Lessig 2009, p. 122*
[80] *Levi-Faur 2011, p. 271*
[81] *An apt example is Article 25 of GDPR*
[82] *Article 25, Regulation (EU) 2016/679 GDPR*
[83] *Cavoukian 2011, p.10*
[84] *Cavoukian 2011, p. 1-2*
[85] *Cavoukian 2011, p. 10*

3.2 Privacy Impact Assessments (PIAs)

3.2.1 What is a PIA or DPIA?

A DPIA is a process that helps organizations identify and minimize privacy risks, and is usually conducted ahead of implementing new processes, projects or policies. DPIAs aim to seek out potential problems so that they can be mitigated ahead of time, thereby reducing the likelihood of occurrence and the associated costs. The working party defines it is *"A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data."*[86] Further, DPIAs benefit the organization by improving policies, processes and systems, and securing relationships with customers and stakeholders.

The UK's ICO code of practice for PIAs is quite comprehensive.[87] The code states specific steps which an organization should carry out during the assessment process.[88] The formulation of this code was before the time of GDPR but still serves as a good guidebook as to how to conduct PIAs. The ICO has subsequently put up a GDPR based guide on its website which also provides an excellent checklist which the ICO recommends is an excellent way to conduct a DPIA.[89]

For this paper, Privacy Impact Assessment Toolkit developed by the Privacy Commissioner of New Zealand will be used[90]. This choice is because this model has been prepared with consideration to new mobile technologies and is easily adaptable to changing systems. It also aims to introduce PIAs within the lifecycle of projects by introducing checkpoints, which is also the aim of this study.

According to this Toolkit, the main goal of a PIA is to identify privacy risks and work to mitigate them. Along the way, it is also possible to identify opportunities that proper privacy management will create. Documenting this process for future use though PIA reporting is advocated.[91] Real action based on the reporting is vital for this process to work and to adapt the PIA as the project develops is essential.[92] Additional steps like approaching shareholders for consultation is needed if the project is complicated and extensive.[93]

---

[86] *Article 29 17/EN WP 248 rev.01 of Directive 95/46/EC pp. 1-2*
[87] *ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.*
[88] *Act, Data Protection, ICO, 2014, p. 3*
[89] *Act, Data Protection, ICO, 2014, p. 4*
[90] *Office of the Privacy Commissioner of New Zealand 2015 part 1.*
[91] *Office of the Privacy Commissioner of New Zealand 2015, part 1, p. 3*
[92] *Office of the Privacy Commissioner of New Zealand 2015, part 1, p. 3*
[93] *Office of the Privacy Commissioner of New Zealand 2015, part 1, p. 3*

This toolkit describes PIA as a *'practical analytical tool'* that is useful to understand if the project might affect the privacy of individuals.[94] The effect could be positive or negative. This effect means that a PIA is used to find privacy gaps but is also used to demonstrate positive steps taken by the project to protect privacy already. Identification of legal and organizational compliance and adjusting a project to get the best out it is also crucial for a PIA.[95] The most important of this toolkit is the checkpoints it envisions to create so that the information can be used again in a future PIA.[96]

A Privacy Impact Assessment is for all shapes and sizes of projects, the essential ingredient of which is personal information, i.e., information about identifiable individuals.[97]

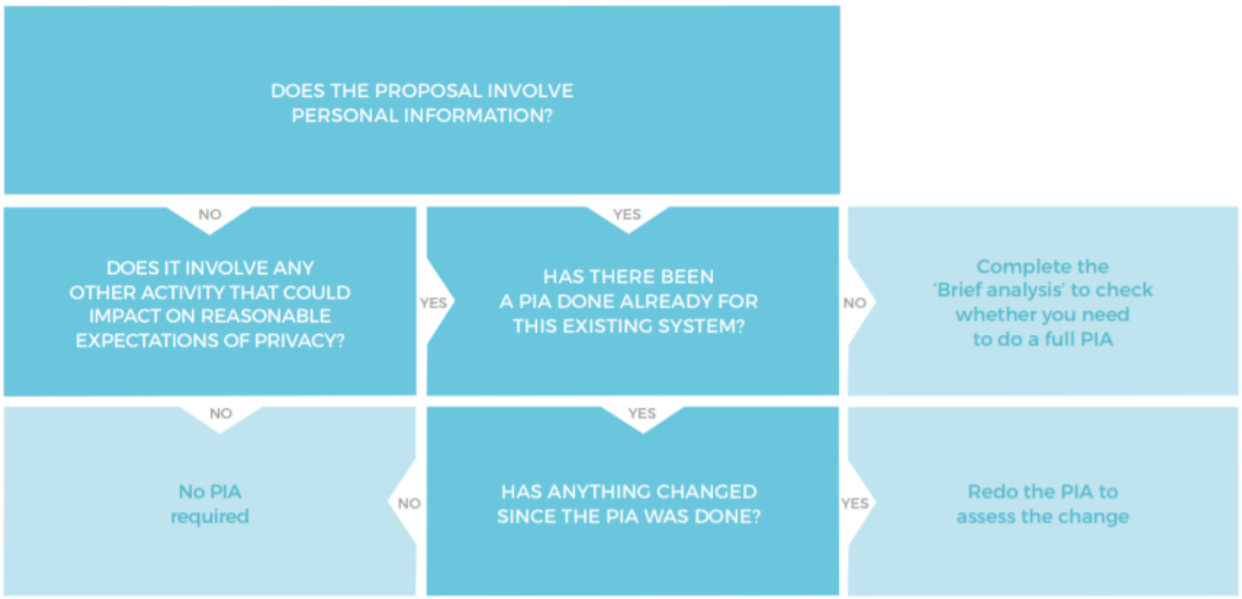


Figure 3 Flowchart to figure out if a PIA is beneficial for a project or not.

Source: *Office of the Privacy Commissioner of New Zealand 2015, part 1, p.* 11

[94] *Office of the Privacy Commissioner of New Zealand 2015, part 1, p. 9*
[95] *Office of the Privacy Commissioner of New Zealand 2015, part 1, p. 9*
[96] *Office of the Privacy Commissioner of New Zealand 2015, part 1, p. 9*
[97] *Office of the Privacy Commissioner of New Zealand 2015, part 1, p. 10*

A checklist is an excellent way to figure out if a PIA is needed or not for a project.

PROJECT FEATURES THAT MAY INVOLVE PRIVACY RISKS	YES / NO
Information management generally	
A substantial change to an existing policy, process or system that involves personal information	
Collection	
A new collection of personal information (for example, information about location)	
A new way of collecting personal information (for example, collecting it online)	
Storage, security and retention	
A change in the way personal information is stored or secured	
A change to how sensitive information is managed	
Transferring personal information offshore or using a third-party contractor	
A decision to keep personal information for longer than you have previously	
Use or disclosure	
A new use or disclosure of personal information that you already hold	
Sharing or matching personal information held by different organisations or currently held in different datasets (for example, combining information with information held on public registers; or sharing information to enable organisations to provide services jointly)	

Figure 4 checklist to use to ascertain if a PIA is needed

Source: *Office of the Privacy Commissioner of New Zealand 2015, part 1, p.* 9

3.2.2 The Regulation describes the purpose of DPIAs:

Since GDPR has been passed, we have a legislative reference of PIAs. Recital 83 of GDPR states that *'In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. […] In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may lead to physical, material or non-material damage.'*[98]

The GDPR prescribes a minimum for DPIAs, as mentioned by the working party paper, which is a description of the processing and purposes. *'It also includes description of valid interests*

[98] *Recital 83, Regulation (EU) 2016/679 GDPR.*

pursued by the data controller and an compliance assessment of the necessity and proportionality of the processing, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, all safeguards and security measures to demonstrate compliance, an indication of timeframes if processing relates to erasure, an indication of any data protection by design and default measures, a list of recipients of personal data, confirmation of compliance with approved codes of conduct, details of whether data subjects have been consulted."[99]

In the past, even before the times of GDPR, privacy impact assessments (PIAs) were widely considered best practice by regulators and industry alike.[100] Given the societal acceptance of PIAs, both as driven by norms and market, the PIA model can serve as a good base for DPIAs. From a practical perspective, PIAs and DPIAs serve the same purpose.

3.3 Vacuum in implementation of PbD process

Irrespective of the new EU regulation and the global efforts to streamline the PbD process, there is uncertainty about the meaning of "Privacy by Design" and how to implement it within the lifecycle of a project.[101] The legislation does mention some Privacy Principles in recital 78 as a part of the technical and organizational measures to be implemented and documented by an organization, but the aspect of how to do it is left entirely up to the organization. This lack of further guidance leads to another problem: other than some privacy measures like anonymization and data minimization mentioned in the text; there is hardly any clear privacy measures to implement. It is left up to the organizations to figure out the privacy measures that will achieve the said privacy principles. This dichotomy is observable not just in GDPR but is common also across other jurisdictions. Cavoukian herself says that there is much work to be done to bring clarity to this and there are similar thoughts expressed by other academics who have worked on operationalizing PbD like Kroener and Wright. They say that operationalizing the PbD process will involve a multifaced approach involving PbD principles, a PIA process, and several PETs.[102]

[99] *Article 29 17/EN WP 248 rev.01 of Directive 95/46/EC, p. 7. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.*
[100] *Schwerin 2018, p. 62*
[101] *Privacy by Design: issues and information, gdpr-info.eu, 2018, website*
[102] *Kroener – Wright 2014, p. 362*

The endgame here is that we have the Privacy Principles, Privacy Preserving measures but nothing to connect them. The first organizational measure suggested by Cavoukian is PIAs, and this has the potential to operationalize PbD process.[103]

3.5 Principles of PbD

Many times, when privacy is implemented into systems at the end of their development cycle, there is usually a tradeoff between adding some functionality of the system and adding some privacy feature. PbD seeks to eliminate tradeoffs yielding a win-win situation. This concept of functionality is one of the seven foundational principles of PbD created by Ann Cavoukian. These principles were only meant to serve as a reference framework, and they were not detailed enough to allow the direct application or engineering into systems. This nature of the principles meant there was still a long way to go in making these principles operational in the development lifecycles of systems and this is the aim of this thesis. The seven foundational principles are described by Ann Cavoukian as follows:

Cavoukian has also mapped each foundational principle to the related Fair Information Practices. (from now on FIPs)

1. Proactive, not Reactive; Preventative not Remedial: This approach is all about prevention and predicting privacy breaches before they happen. This principle advocates integrating privacy into the product in such a way that security is a top priority since the beginning and protects from potential privacy infringements.

2.Privacy as the Default: Something to have a default configuration implies that it must be designed that way.[104] Therefore, this Privacy principle also finds its way in the name of the GDPR legislation Article 25 titled Privacy by Design and by Default.[105] This is a 4-tier principle. Firstly, this principle is based on the FIP of Purpose Specification Principle[106] – 'the principle that establishes that a citizen needs to be informed why his/her personal data is being collected and the specific purposes for which it will be processed and kept.'[107] The purposes should be clear, limited and relevant to the circumstances. Secondly, this principle also includes the FIP of Collection Limitation, i.e., there are to be established limits to the collection of

[103] *Kroener – Wright 2014*
[104] *Kohei, Arai – Rahul, Bhatia – Supriya, Kapoor 2018, p. 135.*
[105] *Article 25, Regulation (EU) 2016/679 GDPR*
[106] *Article 5, Regulation (EU) 2016/679 GDPR. "Personal data shall be:*
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');"
[107] *Cannataci – Bonnici 2010, pp. 101*

information, with consent and knowledge of the data subject in a lawful and fair manner.[108] Thirdly, there is Data Minimization, which means that personal data is to be processed with due consideration to the adequacy, relevance and limited to what is necessary.[109] Lastly, there is the FIP of Use, Retention, and Disclosure Limitation, which states that personal information that is used, retained and disclosed is subject to the limitation of necessary purpose for which there has been given a concent by the user except for a few exceptions like archiving, scientific or legal purposes.[110]

3. Privacy Embedded into Design: This principle is the heart of the concept of Privacy by Design as it states that privacy should be at the forefront of the design of a system.[111] The objective of the thesis to develop a lifecycle model falls under this principle as a lifecycle model achieves embedding privacy into the design of the system. Privacy is not an extended feature of the design of a system, but it is to be at the core of its design. That is privacy embedded into the design and architecture of IT systems.[112]

4. Full Functionality – Positive-Sum, not Zero-Sum: *'Compromise'* is the term that is most often used when discussing the privacy features of a system.[113] Accommodating interests and the objectives of data subjects to generate a positive situation for all parties is the principle of Full Functionality. As long as there are no bad trades involved in accessing certain features of a system, this principle is said to have been satisfied. An ideal system should not have to compromise between access to features or between privacy and security.

5. End-to-End Security – Lifecycle Protection: Privacy considerations must be applied across the lifecycle of a system without any compromise on protection or accountability. The principle of security forms a big essence of this principle and envisions proportionate lifelong security measures for a system.

6. Visibility and Transparency: Visibility and transparency envision to make visible to the user the information transfer and status of personal information.[114] The core of this principle is the delivery of status of the user's personal information to the user in a transparent and easy to

---

[108] OECD, 1980.
[109] Article 5, Regulation (EU) 2016/679 GDPR. "1. Personal data shall be:
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"
[110] Article 5(1)(e), Regulation (EU) 2016/679 GDPR. The fifth principle is the principle of "storage limitation".
[111] Rubinstein 2011, p. 1410. See also Cavoukian 2009, p.3 'Build in privacy from the outset' has been Cavoukian's approach, to 'avoid making costly mistakes later'.
[112] Everson 2016, pp. 31-32
[113] Everson 2016, pp. 32
[114] Cavoukian 2010, p. 250

understand manner.[115] Further, FIPs of Accountability, Openness, and Compliance also fall under the domain of this principle. Proper documentation, audits, and evidence of compliance are important tools to ensure that users are kept in the loop of what is happening to their information.

7. Respect for User Privacy: The empowerment of the data subjects and placing their privacy at the top of the agenda should be the goal of architects and operators of systems. This agenda includes privacy defaults, appropriate notice, and empowering user-friendly options.[116] User-centricity is vital for this principle.

4. Operationalizing Privacy by Design

This chapter brings forward some relevant developments that have taken place to transform PbD from a regulatory standpoint to a more operational engineering (technical) framework. PbD principles are by nature vague and misconstrued in IT systems groups and hence necessitate this section. Privacy is a blurry concept by itself and often wrongly substituted with security.[117]

The importance of a PIA in the identification of privacy risks by locating areas where PbD principles can provide solutions has been advocated strongly by Kroener and Wright.[118] They also say that because of there is a lack of policy or guidelines with Ann Cavoukian's Privacy Principles to assess if a project does or does not possess these principles, and hence the concept of PbD continues to be abstract rather than enforceable.[119] They went on to state that operationalizing the PbD process will involve a multifaced approach involving PbD principles, a PIA process, and several PETs.[120]

Hoepman has advocated the importance of utilizing design patterns as a design methodology.[121] Difference between design strategies, design patterns and PETs is his forte and ascertainment.[122] Connecting privacy with the development process of a system, Hoepman suggests the following:

---

[115] *Cavoukian 2010, p. 250*
[116] *Cavoukian 2010, p. 250*
[117] *Kohei, Arai – Rahul, Bhatia – Supriya, Kapoor 2018, p. 135. "The already murky waters that contain PbD are made more difficult to navigate when we introduce complex abstractions like 'privacy' and 'security'. To unpack these quickly, privacy is not the same as security but in some circumstances, privacy may be delivered by security and vice versa."*
[118] *Kroener – Wright 2014, p. 360*
[119] *Kroener – Wright 2014, p. 362*
[120] *Kroener – Wright 2014, p. 362*
[121] *Hoepman 2014, p. 448*
[122] *Hoepman 2014, p. 448-449*

- application of privacy design strategies in concept development and analysis phases,
- design patterns applied in the design phase, and
- PETs during the implementation phase.

A good instance is NOKIA's efforts to implement PbD in engineering practices. It built and advocated the Privacy Engineering & Assurance Discipline.[123] Privacy activities were mapped onto production creation phases such as Education, Planning & Concepting, Design, Implementation, Testing, Release, and Operations.[124] The Privacy Engineering & Assurance Process consists of a Privacy Engineering component, which involves the following:

- threat identification[125]
- mitigation cycle[126], and
- the Privacy Assurance component[127].

There is also the EU backed Preparing Industry to Privacy-by-design by supporting its Application in Research (PRIPARE) program. They have developed a methodology for the application of PbD that can be easily combined and implemented within varying system development phases. This PbD process is divided into Analysis, Design, Implementation, Verification, Release, Maintenance, Decommission stages. Environment and Infrastructure is an additional stage which is essential to access the organizational structure. A PIA process is integrated into the lifecycle to run in parallel, beginning at the analysis phase. These efforts have been a positive move towards operationalizing PbD, but more work must be done to create standardized frameworks for implementing PbD in different kinds of technological systems. Thus, the importance of this thesis in contributing to the PbD process.

[123] *Nokia, 2014*
[124] *Nokia 2014, p. 8*
[125] *Nokia 2014, p. 6*
[126] *Nokia 2014, p. 6*
[127] *which involves verifying that privacy requirements have been properly implemented*

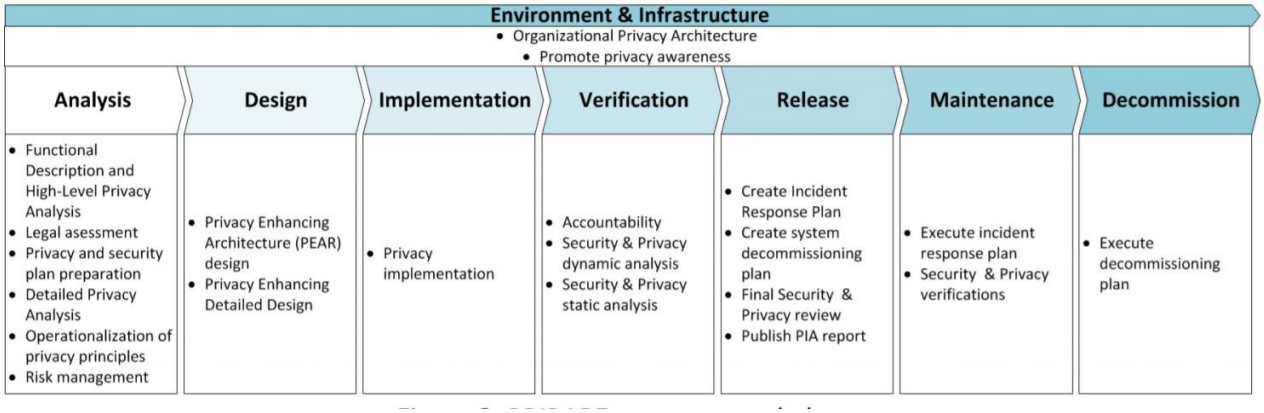


Figure 5 structure of (PRIPARE) program

4.1 Using PIA to begin PbD

Privacy Impact Assessment (PIA) is an effective method used in this thesis to display some results from data collection during this study and more importantly, to analyze them. It has also been used here to some extent, to demonstrate the use of this technique and its relevance to engineering PbD. A PIA is a process used to detect privacy risks, analyze those risks and recommend solutions in the form of privacy controls concerning a system or project. A PIA is made of different steps, and risk analysis is the critical step concerning PbD.

4.2 Privacy by Design

Instructions embedded into software and hardware make cyberspace what it is – they are its architecture. PbD offers a framework for influencing, shaping and regulating this architecture in ways that recognize multiple legitimate functionalities, including privacy among them.

4.3 Integrating PbD Into Practice

Implementing PbD is dependent on location and scope. Location in this context is the ascertaining the suitable position within the business/ service process. There are many options for integration. Some of which are: 1) sector-by-sector basis 2) broad basis 3) across the business-consumer information ecosystem 4) legislated requirement basis 5) a safe harbor-type basis or, 6) choice of an instrument for individual organizations.[128] If the law describes how to proceed with a PbD then the choice becomes quite clear, but in cases like the EU legislation, PbD finds mention in GDPR, but aside from some guidance, there is a lot about implementing PbD that is left to organizational discretion.[129] Article 25 of GDPR instructs to implement

[128] *Cavoukian 2011, p. 13*
[129] *For example, Article 25, Regulation (EU) 2016/679 GDPR deals with PbD.*

appropriate technical and organizational measures to ensure that by default only personal data which is required for a specific purpose is collected and processed. Aside from some guidance in the article and recitations[130] there is not much mentioned as to where and how the PbD process is to take place. This gap is where Privacy Impact Assessments (PIAs) come to assist PbD. A PIA is defined as a tool used to assist organizations in making sure that the choices made in the design and structure of a system or process meet the adequate privacy needs of that system. This is done usually through a directed set of questions, based on privacy requirements.

4.4 Commonality Between PbD and PIA

Ann Cavoukian describes various approaches to incorporate privacy by design into organizations. PIA, according to her, finds itself on the *'Organizational Approaches'* branch of tools available to compliment the PbD process (in the figure below[131]). The chart below summarizes the range of available instruments for encouraging the operationalization of the 7 Foundational Principles of Privacy by Design.

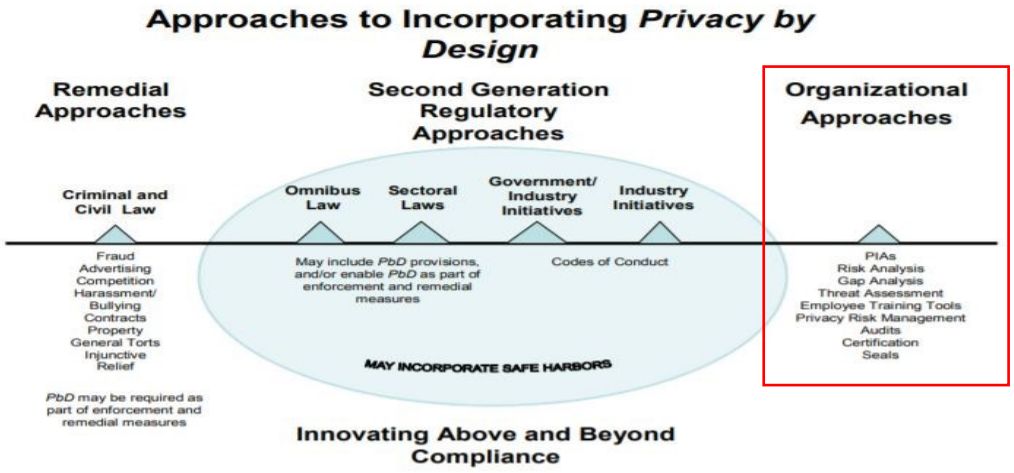


Figure 6 range of available instruments for encouraging the operationalization of the Seven Foundational Principles of Privacy by Design.

Source: Cavoukian 2011, p. 14

[130] *Recital 78, Regulation (EU) 2016/679 GDPR. The Article elaborates a bit more about the appropriate technical and organizational measures be taken to ensure that the requirements of this regulation are met. (Recital) "In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, … to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."*

[131] *Cavoukian 2011, p. 14*

The PbD process suffers from an organizational gap. It lacks a real starting point, and PIA can be the perfect tool to fill that gap. Adopting PbD for an organization is of advantage, and over time it can generate a lot of value and trust within the company. PIAs are traditionally used later to find privacy shortcomings in an already existing cyberspace activity.[132] This answer argues that the PIA process can also be relevant in the earlier development stages of cyberspace architecture. PIAs can be an internal evaluation tool and be a *'PbD tool'* for early evaluation to implement better and more informed PbD.[133]

4.5 Approaching PbD Through PIA – The Relevance Factor

Adoption of PbD by an individual organization is instrumental in building business and competitive advantages for that organization. Traditionally PIA is used at a later stage of the development process of cyberspace architectures. David Wright and Paul De Hert in their book say, *"PIA of individual projects is typically undertaken well after the main design parameters have been set, an organizational structure committed, and significant costs incurred."*[134] The traditional approach to PbD and PIA tends to look at both as fundamentally different, one aiming to implement privacy in the development stage and the other existing to find privacy flaws in already developed cyberspaces. However, this thesis argues that there is indeed a common ground between both the concepts, and they can work to enhance each other.

Concerning PbD, PIAs can find to be of relevance in the very first stage of implementation of PbD process. PIA can be the first point of ascertaining the nature and privacy considerations in the proposed design of a system. In this case, it will be the idea of a new system that will be put to the test of PIA. This will give a focused approach to begin implementing the PbD process, in a much more systematic and meaningful way as the risk areas have been identified. Moreover, the employees and network designers involved in the architecture building process of the project will be aware of the specific considerations to implement, and the stages in which they are to be implemented.

According to Ann Cavoukian, *"PIAs can be an excellent entry point for applying the principles of Privacy by Design."*[135] PIAs can play a pivotal role in ensuring the fact that choices made in the design of a system in consideration are based on concrete considerations to privacy principles. A PIA can be accompanied by a threat and risk assessment for more better results. A PIA has two prominent purposes concerning PbD: 1) assistance in privacy compliance 2)

[132] *Wright - De Hert 2011, p. 151*
[133] *Wright - De Hert 2011, p. 114*
[134] *Wright - De Hert 2011, p. 150*
[135] *Cavoukian 2011, p. 15*

build and communicate within the organization the information about governance and risk management process currently in practice, including the status of implementation of PbD principles.[136] This will better help the employees to understand how to incorporate PbD into the architecture and help them ascertain the relevance of their work. This will directly add value to the overall PbD process.

PIAs are not bound by the existing 7 PbD principles but can go over and beyond and also incorporate data protection principles.

Different authorities have given their preferences as to how a PIA is to be conducted[137] , but the nature of the process remains the same. It will always aim to document issues, ask questions and guide actions required to have healthy compliance to privacy.[138] Because of their nature of identifying privacy design issues they are relevant in the PbD process. Thus, a PIA is relevant both while starting a new project and for evaluating existing ones.

4.6 Assessment framework for checking PbD principles

Using PbD principles within a PIA will require some criteria on which to assess the compliance. Assessment Control Framework developed by Privacy by Design Centre for Excellence at Ryerson University does an excellent job at this has been developed under the watchful eye of Ann Cavoukian. She is currently working as an Expert-in-Residence at Privacy by Design Centre of Excellence at Ryerson University.

'Privacy by Design controls framework' developed as a part of *'Privacy by Design Certification Program: Assessment Control Framework'* correctly detects and presents a robust assessment criterion for abstract Privacy Principles.[139] These can be used as a part of the PIA process to ensure proper and detailed compliance assessment of PbD Principles takes place.

The following are the assessment criteria inspired by Privacy by Design Certification[140] and are developed for use within a PIA to assess PbD Principles:

[136] *Cavoukian 2011, p. 15*
[137] *Cavoukian 2005, pp. 1-3*
[138] *IBM has developed their own way: Privacy by Design: From Policy to Practice Information and Privacy Commissioner, Ontario. Available at: http://www.ontla.on.ca/library/repository/mon/25009/313067.pdf*
See also, Working Party 29 17/EN WP 248 rev.01
[139] *Ryerson University - Deloitte LLP, p. 2*
[140] *Ryerson University - Deloitte LLP, p. 2*

#	Assessment Criteria	Description
1. Principle 1 – Proactive, not reactive; preventative not remedial		
1.1	Privacy Governance assigned to a person	Contact Person is assigned For EU: Appoint Data Protection Officer[141]
1.2	Privacy Impact Assessments and Risk Analysis	Privacy Assessment Process is conducted and documented. Risk assessment, recommendations and actions map.
1.3	Privacy Infringement & Breach Management	A Breach Management Process/Program is developed which includes a notification policy to the users and post-breach evaluation. The post-breach evaluation includes an internal audit.
1.4	Compliance, Monitoring, and Enforcement	There is a mechanism to review Privacy Policies, track Privacy Risks and their compliance with the law
1.5	Privacy Training	A process for Training and communication of Privacy awareness for staff and relevant qualifications for staff that deals with Privacy Compliance.
1.6	Third Party Protection	There exist Third Party Agreements to monitor personal information to transfer obligations to Service Providers and for Cross-Border Data Transfers.
2. Principle 2 – Privacy as the default		
2.1	Privacy Settings by Default	Privacy User Settings are available for the user and defaulted to the Privacy Protected State
2.2	Data Minimization: Collection shall be Limited to Identified Purpose	Appropriate procedures to Limit Collection of information and conduct reviews to ensure Limited Collection. Explicit Consent to be taken for Sensitive PI Using Anonymization and De-Identification for PI.
2.3	Usage of Personal Information	Appropriate procedures to Limit Use. This use must be according to provisions of consent taken and according to Law. New consent to be taken for the new purpose of the use or new PI collected.

[141] *Article 37, Regulation (EU) 2016/679 GDPR*

3. Principle 3 – Privacy embedded into design		
3.1	Consideration of Privacy in Design Documentation, Operational Procedures and Processes, and Change management	Design documents should show that privacy was a requirement at the design stage itself. Privacy was considered throughout the lifecycle till now and will continue. Privacy considerations will be implemented considering the size of the project and the PI used. This documentation also mentions plans for continuity of Design Documentation and Recovery of said documentation in case of disaster. Design documents show that privacy was maintained in the final solution of the product. Privacy is considered when changes are planned within the project.
4. Principle 4 – Full functionality – positive-sum, not zero-sum		
4.1	Positive Sum	Limit Unnecessary Trade-Offs regarding the requirement of PI and the associated function of the application. The situation must be a win-win for both the user and the service provider and certainly not a disadvantage for the user.
1. Principle 5 – End-to-end security; full lifecycle protection		
5.1	Mention Security in Privacy Policies	Specific security measures taken by the organization must be mentioned in the Privacy Policies to topics like: Access and use of personal information, collection, and transmissions, assessments conducted for security, information transfers, network security, logging, data loss, and prevention. These measures must be documented not necessarily in the policy. The responsibilities of security must be acknowledged.
5.2	Safeguarding of Personal Information	There are specific people accountable to maintain security. There is Information Security Awareness and Training conducted for employees and developers. Company has the policy to classify collected Personal Information into specified groups. This protocol helps in giving access to only required information to involved parties. It also helps to achieve logical access.

5.3	Logical Access to Personal Information	Access must be based on "Need to Know." Proper User Authentication is a must to allow access to information for example via username and password, two-factor authentication or certificate. The examples are not exhaustive. Role-Based Access Control can be implemented to give access to only individual employees. Special security measures are in place for Remote Access to Personal Information. User Access to viewing, modification, deletion of records is possible, and logging of actions takes place.
5.4	Physical safety of information	The physical premises of the organization have proper security measures like locked doors, access verification, and logs of who walks in and out.
5.5	Transmitted Personal Information	Encryption of information transferred takes place in a well-documented process.
5.7	Retention and Storage of Personal Information	There is a process of Retention with its limitations and special mobile device safeguards for applications. The Encryption of stored information takes place.
5.8	Disposal or deletion of information	Destruction of information takes place according to retention time and according to a specified process which is documented.
2. Principle 6 – Visibility and transparency: keep it open		
6.1	Privacy Policies Contents and Transparency with mention of the contact person	Privacy Policy of the organization defines and documents its information handling practices concerning the following: Notice; Choice and consent; Collection; Use, retention, and disposal; Access; Disclosure to third parties; Security for privacy; Quality; and Monitoring and enforcement. Further, it is user-friendly, concise and easy to understand language; informs of automatic processing; informs of the foreign service provider. The policy must mention how the complaints are handled. The policy must be available easily in relevant languages, preferably all languages supported by the system.

3. Principle 7 – Respect for user privacy – keep it user-centric		
7.1	Purpose of Collection - Notice	A visible notice is presented when information is collected mentioning details of what is being collected and by whom. Also, the existence of automated decision-making and processing should be mentioned.
7.2	Consent and Notice	Clear and Concise Notice for Privacy Choices Available to User And a clear Notice of the Consequences for Failing to Provide certain Personal Information. There should be provision for withdrawing consent and Explicit Consent for Sensitive Information and Consent for New Purposes.
7.3	Access to and Correction by Individuals of their Personal Information	There should be a specific provision for this.
7.4	Right to deletion ("right to be forgotten") and right to object	There should be an explicit provision for this.
7.5	Accuracy	Review of information and provision for users to check the accuracy of the information and a way to change information if not accurate.

5. Developing a working model to operationalize PbD process

The thesis proposes a model to operationalize the process of implementing PbD in the developmental lifecycle of a project inspired by Ann Cavoukian, Kroner and Wright. The model is as follows:

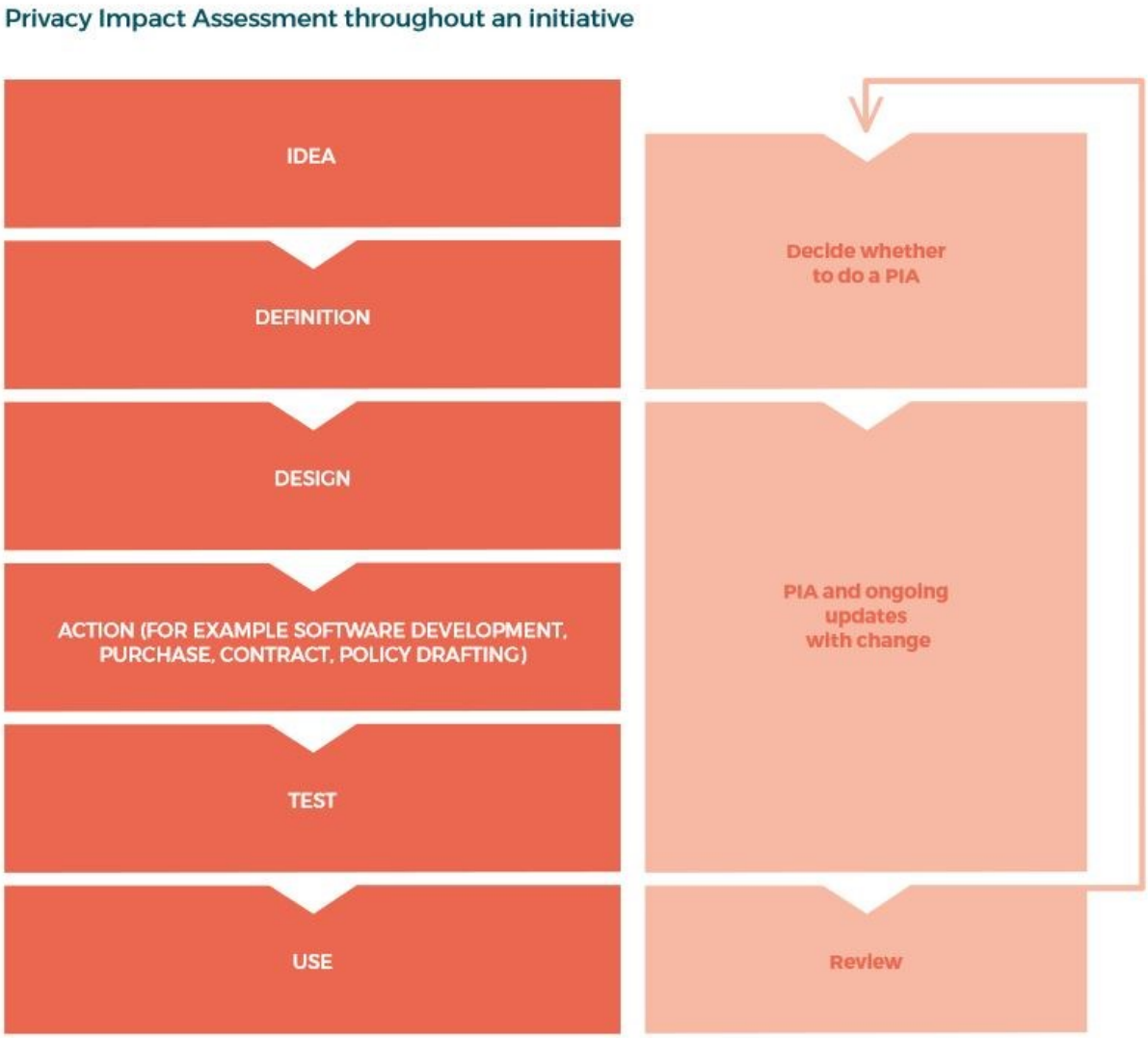
1. First, conduct a PIA using PbD Principles with risk assessment and Ryerson Framework
2. Use the data from PIA and risk assessments to identify technical privacy-protecting measures.
3. Use these privacy-protecting measures as checkpoints in the future developmental lifecycle.

Traditionally, PIAs are conducted for an already existing cyberspace activity. Therefore, they are also designed in such a way that they assess issues that would occur in already functional systems. The common aspect between a PIA and a PbD is that both involve scrutiny of the design of the system and then aim to improve the said design towards the protection of privacy. The PIA analyses the system and PbD advocates implementing privacy at the core of the said design. This common element makes both the processes complementary to each other; the PIA can ensure better strategic implementation of PbD. A PIA can be used at any stage of the project in order to introduce PbD into its design. A new project which is still just an idea is as good as a candidate as a project that has been running for a substantial amount of time. The goal is the introduce the Privacy Principles into the design of a project, and PIAs is the perfect tool to do it.

In order to understand this better and to develop a PIA for PbD, the framework of a PIA is crucial to be built. The PIA toolkit developed by the Privacy Commissioner of New Zealand gives a very in-depth well-illustrated view of the lifecycle of a PIA within a project:

Figure 7 PIA throughout an initiative

Source: *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 5*



It is important to note that the toolkit envisions a PIA being used at the early developmental stages of a project a.k.a. the 'idea' stage of an initiative in the figure above. Many advocates and manuals teaching the means of conducting a PIA suggest that the PIA process can only be conducted after the commencement of a project. The truth is that PIAs to be effective are a continually evolving process. No PIA is the same as the previous one and hence the issues discussed, and questions asked by one PIA will always be different from the other one. It is, therefore, necessary to develop different questions for an early developmental PIA.

The toolkit advises that *"A Privacy Impact Assessment is not a last-minute legal compliance checklist – rather it is an active tool to help inform the major decisions involved in planning*

and implementing your project."[142] What this advocates that a PIA is not an instrument that comes into the picture at the last stages of the development or lifecycle of the project, instead it is an *'active tool'* that is applied to analyze the project in perpetuity in order to gain insights to make better privacy decisions.

If conducted at early developmental stages of an initiative a PIA can help to better formulate the design of the initiative by making available data to make informed design decisions regarding the system and operations.[143] This way of implementation will save time and cost further into the development process and make it more privacy oriented.[144]

It is very typical for a project to change over time. For example, it is very reasonable for a mobile app to update and introduce a new feature. In order to facilitate a smooth transition during this update, it is necessary to introduce *'privacy checkpoints'* in the development process. Thus, there is use for a PIA at different stages of a project. An early PIA may not be able to answer every question and more information may come to light later or just that the project wants to introduce a new feature. To facilitate this one or more *'privacy checkpoints'* can be constructed into the project plan. The main question to ask here is: "Has anything significant changed since you did the early pre-development PIA?". If the answer to that is a yes, then a PIA can be initiated to check the existence of new privacy risks and how to manage them.[145]

5.1 Initializing a PIA process: PIA Ascertainment

The most basic and important question which will initiate any PIA process is to ascertain whether a PIA is necessary at the current stage of the project. These are also to be asked at *'starting privacy checkpoint'* if the project is still new and just an *'idea.'* The stage of ascertainment is suitable for both, an already existing project or a new project.

The following questions can be asked at a starting PIA and then also for determining *'privacy checkpoints'* at later stages of the project[146]:

[142] *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 1-3.*
[143] *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 4*
[144] *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 4*
[145] *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 4*
[146] *The questions have been developed by analyzing the recommendations by the following: NewZealand Commissioner toolkit, Ann Cavoukian's Privacy Toolkit, IBMs Self-Assessment Privacy Toolkit.*

Starting privacy checkpoint	Subsequent Privacy checkpoints
• Is the project going to involve the collection, storage or processing of personal information?[147] • At what point in the project will a PIA be most helpful?[148] • Who should do the PIA?[149] • How long will the PIA take, and how detailed should the PIA be?[150] • Whom to consult as part of the PIA?	• Has the project gone through a significant change? • Have the aspects of the collection, storage or processing of PI changed in any way? • Has the project changed since the last PIA?

5.2 Length of an early PIA

To understand this a *'starting privacy checkpoint'* can be conducted. This checkpoint will be conducted only once before the beginning of the project or while introducing the PbD model into an existing system for the first time. This will give an idea regarding the *'size and scope'* of the PIA.[151] At this point, the PIA process has already begun and determining the length is now a part of the process. The following set of questions are asked to determine this:

Questions to determine the length and scope of early PIA	Questions to determine the length and scope of later PIA
• What is the scope of the PIA? • Which areas are outside its scope?	• Are there significant changes since the last PIA? How significant? • What will the PIA cover and which areas will be outside its scope?

[147] *For example, if the PIA is part of the design of a new IT system and the project collects, stores or processes personal information. In this case, it will be very risky to not conduct a PIA and only do it at later stages of the project wherein the system has already been designed/ built. An early PIA will help better design the system and avoid potential future costs and save time in dealing with privacy related consequences.*
[148] *Preparing an early roadmap for the 'privacy checkpoints'*
[149] *Which person in the organization will manage and conduct the PIA process*
[150] *To get an idea of the scope.*
[151] *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 6*

• What is the scope of information gathering? What are the sources and their types? Is this an office or a field exercise?[152] • Who are the people involved and what is their availability? • Where does the PIA fit in the project plan and calendar? • Who are the decision makers for the PIA? What are the organizational processing times for these decisions? • Is the decisionmaking online or offline? • Is there a need for external consultation for this PIA? How are the said consultants determined? • Are there any third parties involved? How are the processing times with them? Do they need to be involved within the PIA?	• How much can data be imported from the last PIA? • What is the scope of information gathering? What are the sources and their types? Is this an office or a field exercise?[153] • Who are the people involved and what is their availability? • Where does the PIA fit in the project plan and calendar? • Who are the decision makers for the PIA? What are the organizational processing times for these decisions? • Is the decisionmaking online or offline? • Is there a need for external consultation for this PIA? How are the said consultants determined? • Are there any third parties involved? • How are the processing times with them? Do they need to be involved within the PIA?

The presence of an early PIA should also make the subsequent PIAs more focused and hence more concise: they will focus on the changes that have occurred in the project since the last PIA. Some questions regarding the gathering of information remain the same while determining the length of any PIA.

5.3 Who should conduct a PIA?

A person conducting a PIA need not be a privacy expert, an engineer or a lawyer.[154] As long as the team includes a person who is familiar with the privacy principles and can advise on the privacy impacts of the project, it is adequate for such a team to conduct a PIA. If the PIA is

[152] *Office of the Privacy Commissioner of New Zealand 2015, part 2*
[153] *Office of the Privacy Commissioner of New Zealand 2015, part 2*
[154] *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 6*

bound to involve complex issues which are at the core of the design of the project, then it is advisable to let an expert handle the PIA.[155] It is good always to involve internal staff in the PIA process even if an external expert is appointed at the reins of the PIA process. Involving the staff and particularly the designers of the project can be particularly of value as they will gain valuable insights of the privacy concerns and information of the organization, thus helping them better design the project at hand. It is vital that the people in charge gave access to the information and resources of the organization.

5.4 Determining people to be involved in the PIA process

Most of the people who need to be involved in the PIA are within the organization, although a complex PIA may also involve external stakeholders.[156] The first checkpoint and the length determination process should determine the people involved. A small organization means that there will be fewer people to talk to and hence a faster PIA process and the opposite is exact for larger organizations. The following is a list of people who need to be involved:

1. People familiar with the privacy ecosystem within the organization
   - the privacy officer is a must
   - other specialized privacy related staff is an asset if present
2. People familiar with security in the organization
3. Project staff and analysts: they understand the aim of PbD process for the project
4. Information technology related employees: they have technical system information and are aware of the information flows and storage.
5. Marketing employees: they know the stakeholders and can get in touch is information is required from stakeholders.
6. Risk assurance personnel: for risk assessment
7. Customer representatives: to contact customers if needed

5.5 Steps of the Privacy Impact Assessment

The content of each step of the PIA is more important than the order in which they are conducted.[157] While applying the privacy principles to an initiative, there might be realizations that there is more information required or the required action is not clear as the risks involved are uncertain. In this case, it is all right to deviate from the order of the steps and do them in a custom subjective fashion in order to solve the problem at hand. Every organization is different,

[155] *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 6*
[156] *External stakeholders could be business related colleagues, Local Chamber of commerce, local city government bodies, the privacy commissioner.*
[157] *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 8*

and every project is unique and might require the steps to be implemented in a different order. Hence, the order can be changed to suit the needs of the initiative, but the content needs to remain consistent. Be it a predevelopment PIA or a post-development PIA the fundamental nature of the process remains the same and hence so do the steps. Hence, it is possible to map the necessary steps involved in every PIA[158].

5.5.1 Step 1. Gather all the information needed

The essential task here is to describe:

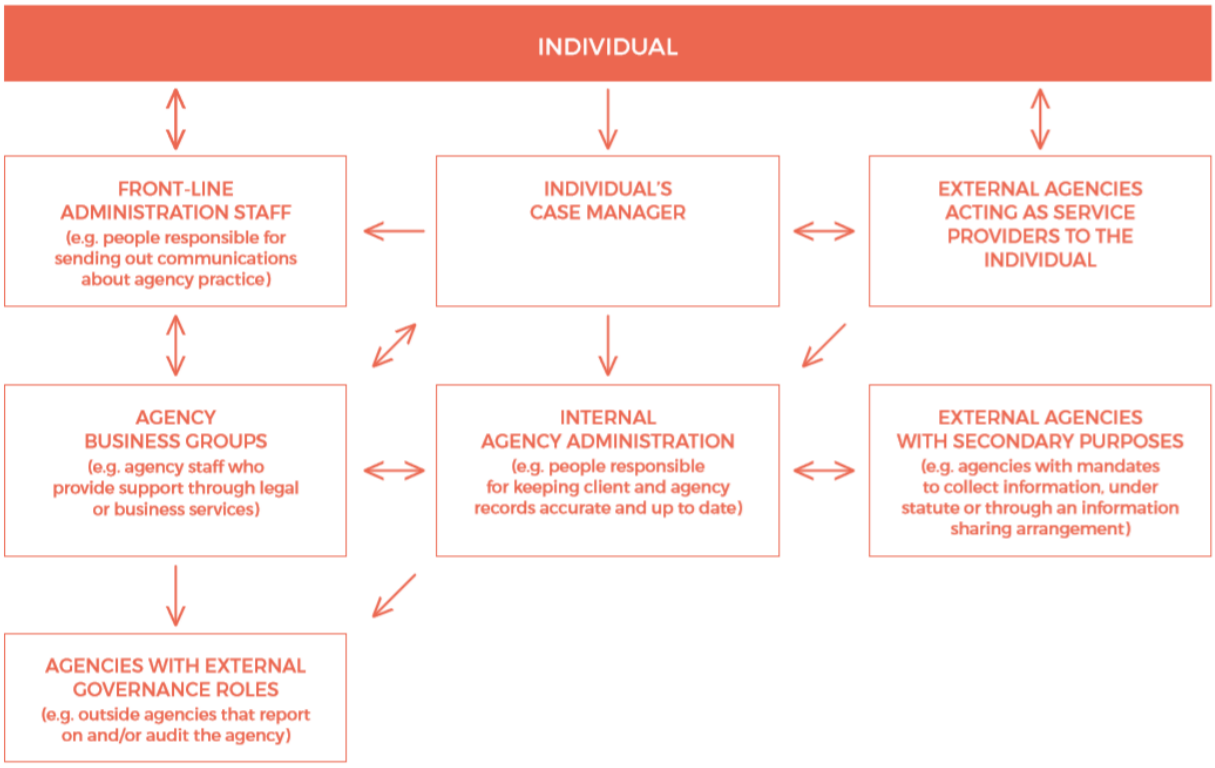
1. the nature of personal information collected
2. the organizational state of affairs
3. purpose (business of legal) of changes made to personal information
4. the project is standalone or is a modification of an existing one
5. the information flows within the system and its lifecycle
    - point of collection of information and its subsequent flow
    - effect of the project on the current flow if the project is already functional
6. the project including changes and use of personal information
    - the new personal information (previously not collected)
    - origin of new personal information
    - the kind and method of use of existing (already possessed) personal information
7. the measures to check the accuracy of personal information
8. the repurposing of information, if involved
9. the notification protocol of the organization
10. the access protocol of the organization
11. the retention protocol of the organization
12. the disposal protocol of the organization

Presenting the information lifecycle within the origination through information flow diagrams is an excellent way of facilitating visibility and transparency. Additionally, it is also useful for doing a PIA to understand the parties and factors (where, how and who) involved in the information transfers. The PIA toolkit shows an example of an information flow diagram.

[158] *Office of the Privacy Commissioner of New Zealand 2015, Part 1 and 2.*

Figure 8 Information Flow Diagram

Source: *Office of the Privacy Commissioner of New Zealand 2015, part 2, p. 10*



During the first step, it is also essential to include the organizational contextual information in the PIA process. This involves considering the implications of privacy concerns on the functioning of the organization.

The necessary background information organization includes details of:

1. the privacy responsibilities assigned, designations and human resource management
   - ideally done by Data Protection Officer or any privacy specialized officer
2. the organizational standards and policies concerning personal information
   - privacy and security policy
   - retention and disposal policy
   - breach and audit policy
   - change policy
3. the risk management standards within the organization
4. the accuracy protocols, security protocols, training protocols of the organization.

5.5.2 Step 2. Check against the PbD principles

This step deviates from the New Zealand Toolkit and proposes to use the PbD principles instead of general privacy principles. This is an essential step of a PIA wherein the principles are listed in the first column followed by the personal information. For the compliance Assessment, the assessment framework visualized in Chapter 4.6 is used.

The following format can be used to check against the PbD Principles:

#	Description of the PbD principle	Summary of personal information involved	Compliance Assessment	Risk Identification
1				

5.5.3 Step 3. Identify any real privacy risks and how to mitigate them

Pick up the data from the previous PIA and then use it to identify risks to Privacy and then analyze ways to protect and mitigate risks with available data and resources. Privacy risks can be defined as various concerns regarding the privacy of personal information of individuals that have the probability of a detrimental intrusion. International Organization for Standardization defines risk as “the combination of the probability of an event and its consequences.” The possibility of an event that has the potential to cause damage. Mitigation of this risk is also called as Risk Management. The process of recognizing and subsequently minimizing such a risk is called Risk Management. The following risk matrix can be used to ascertain risk with the goal of minimizing it:

Figure 9 Risk Matrix

Source: AUSTRAC: Australian Transaction Reports and Analysis Centre, Risk management - A tool for small-to-medium sized businesses, Australian Government, 2014.

Likelihood	Impact - how serious is the risk?		
Very likely	Acceptable Risk Medium 2	Unacceptable Risk High 3	Unacceptable Risk Extreme 4
Likely	Acceptable Risk Low 1	Acceptable Risk Medium 2	Unacceptable Risk High 3
Unlikely	Acceptable Risk Low 1	Acceptable Risk Low 1	Acceptable Risk Medium 2
What is the chance it will happen?	**Minor**	**Moderate**	**Major**

The above figure shows both impact and likelihood in order to ascertain a rank for the associated risk.

The following format has been developed to ascertain risks in this step:

Analysis of Risks

Privacy Requisites	Privacy issues	Likelihood	Impact	Risk Assessment	Comments

5.5.4 Step 4. Produce a PIA report

The PIA report is a significant reference point for employees and their organization. It should at least: • include all relevant information about the project and what it is intended to achieve • describe how information flows through the system • include analysis against the privacy principles and other relevant material to show what the privacy impacts are (both positive and negative) • identify critical risks and how to mitigate any adverse impacts • recommend any necessary changes • to identify whether the PIA should be reviewed during the project, and/or once the new system is operating

5.5.5 Step 5. Take action

After gathering all the information and analyzing it in the previous steps this step brings it all together in the form of action. An action list can be prepared for this purpose to track and manage the decisions taken as a result of the PIA.

The action list may contain items to be completed as part of the project itself, or it can be integrated into routine operations (such as maintaining a risk register, or as part of a security action plan). It is vital to make sure that the action list identifies who is responsible for doing what. Also, make sure that it notes any relevant timelines and contingencies.

The PIA may identify more extensive opportunities for action, so it is possible to make privacy-enhancing changes throughout the organization. For instance, it may show that there are other parts of the business where it might be possible also to achieve better security, better accuracy of the information, and more effective business processes for managing personal information.

The following action list is to be used to document the actions taken:

#	Actions approved	Responsible people	ETC
R/01			

5.5.6 Step 6. Review the PIA and use it as a checkpoint once things are in operation

If there have been changes that have an impact on privacy, do quick updates of the report and action plan that record: • what has changed • what the new impact is • how to address any new risk (or take advantage of any new opportunity). This will ensure the PIA continues to be used as a tool to check that the project does what it is meant to do. Once the changes are up and running, it is also worth using the PIA as a checkpoint for how the new process is operating. Is it working as anticipated, or are problems starting to emerge and further changes needed? Again, using the PIA as a reference point can save time and trouble.

5.6 Detecting Privacy Preserving Measures (PrM): a more technical approach

Privacy Principles by themselves sure are enough to conduct a PIA, as seen above, and then to implement PbD within a project. However, the fact also remains that they can sometimes also be very abstract and vague.[159] For example, Anonymization & Pseudonymization is mentioned in the GDPR as one of the Privacy Preserving measures that can be implemented as a part of PbD process. This can be effective to do away with the vagueness associated with the Principles. These measures are evident and emerge after doing a basic PIA only based on the

[159] *Kroner - Wright, p. 362*

Privacy Principles. Incorporating these new measures at a stage of the PIA can being more scientific certainty to the whole process of incorporating PbD in systems development through PIA. The mapping/detection of these measures is considered as an **Execution** Check**point** for this lifecycle model.

The process works as follows:

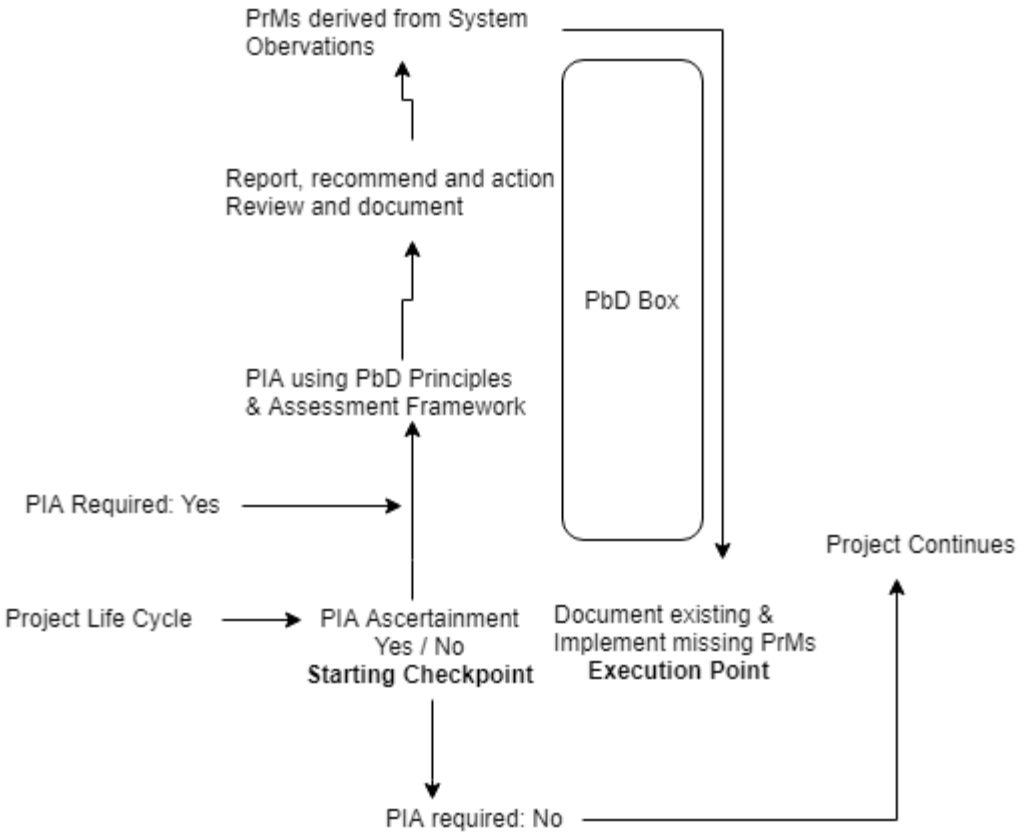


Figure 10 Process of proposed PbD box model; single iteration

A brief description of the proposed model is as follows:

1. The **Project Life Cycle** is its system development cycle. In order to introduce the PbD process a PIA is going to be used. So, the first step is to do a **PIA Ascertainment**. This ascertainment will help determine if a PIA is needed or not.
2. If the answer is **PIA required: No**, then it is not required, and the project can continue without one.
3. If **PIA Required: Yes**, then a **PIA using PbD Principles & Assessment Framework** is conducted on the Project. As a part of this PIA a report is created with recommendations, risks and actions. This is the step **Report, Recommend and Action**

Review and Document. Using the data from this step the last stage of the PIA will then **derive PrMs from PIA**.

4. As the last step, after the PIA, it is needed to **Document existing & implement the missing PrMs**. This concludes the process. It can be repeated again if new personal information is introduced or some other changes take place within the project.

The entire process can be summarized as a **PbD box**.

The observations then are to be linked to PrMs within the system under study and check if they possess the measures or not. This will show if the system contains PbD properties or it lacks them.

This can be done using the following format:

1. Format to link observations:

#	Observation within the System studied	Privacy-Preserving Measure	Compliance of System Yes/No
1			

6. Demonstration of using a PIA to implement PbD

Privacy Impact Assessment (PIA) is an effective method used in this thesis to display some results from data collection during this study and more importantly, to analyze them. It has also been used to demonstrate the use of this technique and its relevance operationalizing the PbD process. A PIA is a process used to detect privacy risks, analyze those risks and recommend solutions in the form of privacy controls concerning a system or project. A PIA is made of different steps, and risk analysis is the critical step concerning PbD. As the purpose of this section of the thesis is to show the complementary nature of PIA to the PbD process an application with a good track record of privacy has been chosen. The name of the application (app) is Föli, and it uses the platform developed by PayIQ to sell public transportation tickets, mainly for buses in the city of Turku. The application is critically acclaimed and has won an award for its functionality.[160]

[160] *The app was nationally awarded as the Best Mobile Solution in Finland 2016.*

6.1 Chosen field of the App: Transport Systems

Over the past decade, the transport sector has massively benefited from technological developments and digitization. In Finland, the Föli buses are fully electric and have a digitized ticketing system. For this purpose, the transport companies use their websites and apps as points of buying tickets and making payments for the same. These apps also are the collection points for customer's personal data.

6.2 Privacy in Transport Systems

Privacy is vital in the Transport Systems as most require customers to give their personal information in order to issue a travel ticket. These systems make use of wireless and mobile technologies, allowing for the possibility of unauthorized access to personal information. Patients need to have control over who collects, uses, stores and discloses their personal information. Therefore, privacy needs to be integrated into the system at the design stage as imposing privacy restrictions on an already developed system has the potential to reduce the functionality or restrict the purpose of the system. There should not have to be a choice between an added system functionality and a privacy feature. This significant problem of a trade-off between some critical system functionality and extra security or privacy features should be solved by implementing Privacy by Design principles in the development of systems.

Systems are generally at risk of privacy-invasive activities from employees of the controller, parallel organizations, third parties, and other unrelated entities or individuals. Avancha et al. categorized privacy threats in mobile health systems into three groups, Identity threats, Access threat, and Disclosure threats. They also discussed the importance of privacy-preserving mechanisms such as Authentication, Anonymity and Location Privacy are essential in mobile systems. It is necessary to authenticate not only the patient but also the service provider and the devices. Authentication is mostly done using a username and password, which may be viable to successful attacks if not implemented with strict policies. Two-factor authentication mechanisms are also growing in prominence. However, if such personal information is to be shared with third parties for academic, commercial, or other reasons, it is compulsory for this information to be de-identified before sharing. The subjects also must have been informed about this and its purpose, with their consent being gotten.

In order to understand the benefits of a PIA in implementing PbD, it will be of importance to conduct a PIA of a project. This PIA will be on an already existing project, but the information gained will also be useful in developing a PbD process for both an early or a PIA for an existing project. A PIA is conducted for this purpose in this chapter, and one general privacy assessment

of an organization's development activities as a part of the PIA process. The PIA is hence done based on the online documentation available of the company, namely, the Privacy Policy of the application (available only on the website)[161], the code of conduct of the company (only on website)[162] and the terms of the application (only on the application). In a practical situation the company will have more data at its disposal to conduct a PIA.

6.3 Privacy Impact Assessment of the Föli Application

Below the PIA created for the Föli project is displayed. Questions from the initial assessment of the project that have a 'yes' answer are stated below. These questions led to the conclusion of the need for a PIA to be executed. Does the project involve:

– The collection, storage, and processing of personal information? Yes.

– Sharing of personal information within or between organizations? Yes.

– The creation of a new, or the adoption of an existing identifier for service users; for example, using a number or biometric? Yes.

Other initial questions like the following need do not have a clear answer at the beginning as they are depending on the size and type of company running the project: •At what point in my project will a PIA be most helpful? •Who should do the PIA? •How long do I need, and how detailed should the PIA be? •Do I need to involve the Privacy Commissioner? Moreover, if so: – At what stage? – What can they do to help? •Whom do I need to talk to as part of the PIA?

6.4 Föli Privacy Management

There is a data protection policy for the Föli's operations in general. The policy is the code of privacy, which is in line with the national and EU personal data regulations. PayiQ, which is the organization in charge of setting up the remote interface between the app on the user's smartphone and the Föli's electronic system or journal, is well versed in security, and therefore it is assumed that it will utilize a privacy policy. Hence, in the context of the app in question, PayiQ is the service provider. The functionality of the app involves three parties, as per the privacy policy:

- the owner and service provider of the app: PayiQ
- the producer of the service purchased: Foli
- the user of the app: customer

[161] *Available at: https://payiq.net/tietosuojakaytanto/ Accessed on: 12th May 2019*
[162] *Available at: https://payiq.net/code-of-conduct-and-policies/ Accessed on: 12th May 2019*

6.5 Description of the System

The project is a mobile ticket booking application that aids travelers to book tickets and recharge bus cards on the go. The application has been developed and currently functions as a standalone app. A new feature which allows data to be transferred from the phone to the Föli's records allows users to log in to book tickets and recharge cards. This feature will be optional for an end-user as they can also choose to log in as a guest and then get a ticket anonymously.

The service provider or/ and data controller is a PayiQ. There is no secondary service provider. External software developers developed the application. Föli also performs quality assurance for the project. Föli seeks to use this app to make it easier for its customer to keep track of their tickets and record occurrences using smartphones which are always with them, rather than recording them on paper. It is a standalone app, with all data stored on the subject's smartphone and some information collected, stored and processed by the company for various purposes. The subject can take the phone to the bus to display and scan the ticket or just search for the most efficient route.

6.6 Project Scope

6.6.1 What information is to be collected?

The Information collected in this mobile application is personal information containing the email address and phone number. The current state of the application explicitly only asks consent to use the user's location to provide location services.

6.6.2 Purposes of collecting Personal information:

PayiQ collects and processes personal information for various purposes, such as:

- to provide services, including technical solutions and applications
- to answer inquiries
- up to date services, product development
- to allow to register for specific areas on the website
- to ensure identity though app authorization
- to ask for feedback, if contacted through the website.
- To monitor the functionality, usability, and security of the application
- to comply with any law or authority obligations imposed
- for internal statistical purposes regarding databases
- to target marketing communications based on the use of the website if contacted the company through the website.

- for other business-related purposes

The source for this information is the privacy policy of the app. There is no code of conduct for the app particularly so the code of conduct for the website is also referenced.

6.7 Information Flows

This section describes the flow of information in Föli system, making it possible to notice where privacy issues may arise. The information flow the diagram and table can show how PI is collected, used stored, secured, disclosed and disposed of. The word ‘secured’ as it is used here, refers to every mechanism used to protect the information and maintain privacy.

The figure shows Information flow table for Föli System. The PI in the system is the login details. The privacy-preserving mechanisms employed are stated in the column SECURED. This information is inferred from the privacy policies on the website and the phone pertaining to the application.

PI	Collected	Used	Retained	Secured	Disclosed	Disposed
Email address	By: PayIQ through application How: to register and log in to the app the email address is required. Also, if not registered it is required to send receipts of purchases.	By: PayIQ Uses: to register, login and receive receipts Where: Application	By: User and PayIQ Where: Phone and PayiQ servers How long: Reasonable period which is necessary to meet statutory obligations and to inform.	By: PayIQ Where: Phone and servers How: the phone with a PIN or user authentication by login or fingerprint. Method: Appropriate technical and organizational	Not disclosed to any third parties except if required for banking or online payment	By: PayIQ after user deletes account or after reasonable retention necessities are exhausted.

	From: user's phone			measures. Not specified.		
phone number	By: PayIQ through application How: While signing up it is required to verify the user and the phone From: User's phone	Uses: to verify the user Where: the application				
information about the device: device model, operating system, operator, IP address, and	By: PayiQ Application How: Background collection to check the version of OS and app version.	Uses: provide, maintain, protect, develop and improve service Where: at the PayiQ offices to improve service and provide				

application version	From: User's phone	customer services when contacted.				
records of purchases	By: PayIQ	Uses: to provide record keeping to Föli and for legal purposes Where: within the app and by email and provide customer services when contacted.				
location information	By: Application	Uses: to provide location services Where: within the app				

6.8 PIA of the System

6.8.1 Step 1: Gathering information

• Description of the project

Turku is a smart city in Southwestern Finland. The city began its cooperation with PayiQ when there was a substantial demand for a mobile platform for public transport tickets, particularly Foli buses. Competitive tendering was used to select a partner to develop this platform. The tender was won by PayiQ, a private IT company headquartered in Turku.[163]

The Turku Region has been the first significant clientele to use the platform by PayiQ. The name of the raw platform is PayiQ White Label, and the city decided to customize the application can use the brand name Föli. The app started with only basic features of location services and has gradually expanded to have mobile tickets and top up of travel cards. It is the first in the world to offer the top up of travel cards. There are also single tickets available that can be scanned in real time at the bus. There are ticket readers installed at the entrance of every bus.

Since Finland is one of the most advanced countries with respect to internet penetration and use of technology in the public sector, this application is the perfect choice for this study to check if the PbD process and PIA can work together in harmony. It will also bring out the Privacy preserving measures used in the app, which then can be used to develop a checklist for other less privacy-conscious regions around the world. The Foli app was also awarded Best Mobile Solution in Finland 2016 and also an award for best mobile payment application at the Slush event in autumn 2015.[164] The application is developed by iQ Payments Oy.

• Description of the personal information involved and what will happen with it

The app collects the following personal information:

1) Information Provided by User

The application can be used in different ways and, depending on usage, it collects different information. By registering with the application, it is possible to get access to all of its features, such as different payment methods. Signing up for an application requires consent to provide the following information: phone number and email address. The privacy policy states that this

[163] *Turku Region Public Transport System – Payiq, website*
[164] *Turku Region Public Transport System – Payiq, website*

information is asked so that the app can identify the user with potential issues and communicate with him/her.

Depending on the form of payment chosen by the user, the app may then also request other information that is required for that payment method to work. This information is required to process the payment correctly. The app uses third parties who may request additional payment information to process the payment. This information is processed only by a third party and the app then does not store this information.

There is also an option to use the application without registration, in which case there is no requirement to provide any information. However, if the app is used without registration, not all the app's features are enabled.

2) Data Collected by Application Usage

The following information about the device being used is collected and user actions in the application. More details are:

Device information such as device model, operating system, operator, IP address, and application version. This information is collected to improve service, improve service security, identify potential failures, and fulfill our obligation to keep records of purchases made within the period specified by law.

Event information is collected such as login and purchase for the application. This information is collected to provide service and to fulfill obligations of keeping records of purchases made for a period specified by law.

Location information is collected to improve service safety and provide location-based services such as route guides. Location blocking does not prevent the application from being used, but location-based services do not work without location support.

• Description of the organizational context

The organization has a unique privacy policy dedicated to the app. This is besides the privacy policy of PayIQ as an organization and its code of conduct. The data protection policy on the website speaks about how the company internally deals with information. The website is managed by IQ payment solutions.

The collected information about the use of the app helps the organization to provide, maintain, protect, develop and improve our service. Using this information, it is then possible to inform the user about the app’s services and about any problems that may present with app services. If

the user contacts the organization through Feedback Channels, the organization will keep in touch to resolve any issues customers may encounter.

In the application settings, all the information given by the user can be monitored. On the Products tab of the app, the user can see the last 30 purchases. The user has the right to review all his/her personal information and transfer it to another company if he/she so wishes.

The user can change the information provided in the application settings. It is also possible to add and remove payment methods. As an exception to the information, it is not possible to change the phone number and the email address. To change this information, the only way is to contact customer service: support@payiq.net.

According to the law, information on purchases must be kept for a specified period. User account will not be deleted without requesting deletion.

If the user would like to stop using the app, it is needed to contact customer service: support@payiq.net. User account and the information provided will be deleted subsequently. However, information about purchase transactions will not be deleted because the organization is obliged to keep them for a period specified by law.

• How will this project change the information flow?

This project will now allow users to buy tickets and Föli products through the app instead of the website or the office. The main change of information is through the transition of personal information through a mobile handheld device. The app data is now not only in the hands of Föli but also in the hands of the app creation and management company PayIQ.

6.8.2 Step 2: Checking PbD Principles

#	Description of the PbD principle	Summary of personal information involved	Compliance	Assessment of Privacy Gaps and comments
1	Principle 1 - Privacy as the Default – Collection, Purpose Specification and Data Minimization	1. *Email address* 2. *Phone number* 3. *Specifications of the device* 4. *Records of purchases* 5. *Location data*	*<u>Collection:</u> There must be a correlation between the collection of information and the purpose of the said collection. In this context (1 and 2) are collected for user identification, (6) is collected to provide specific location services, (5) is to comply with the law and all of the information is also for the general purpose maintain and develop services.* *<u>Purposes:</u> provide, 1. maintain, protect, develop and improve service. 2. inform the user about the services and contact about any problems we may have with our services.3. Information requires for third-party payment services.* *All three purposes mentioned in Privacy Policy on PAYIQ website.* *<u>Data Minimization</u>: identifiability: the user has the option to use the app without logging in, thus not giving any personal information, observability: the information collected is strictly only accessed by authorized company personnel, and linkability: it is possible to transfer personal information to another company if requested by the user.*	*The purpose of some collection is not made clear as it can be. For example, the app says that location data is required for security reasons whereas it is apparent that it is required to access location-based route services. The app does an excellent job of mapping collection to its purpose aside from a small issue; it is an excellent example of how Collection and Purpose limitations are utilized. The same can be said about data minimization as the data is collected only as much and processed only when required.*

#	Description of the PbD principle	Summary of personal information involved	Compliance	Assessment of Privacy Gaps and comments
2	Principle 2 – Visibility and Transparency - Source of personal information and Collection of information from subject Accountability Openness and Compliance	*How and from whom is the information collected: Information given by the user through the app is the only source of information.* *Any other sources of information: None*	*The Privacy Policy and data policy mentions that the information that is collected is only from the users during the use of the application.* *<u>Accountability:</u> Responsibility of communicating all privacy-related policies and procedures is done through dedicated privacy policies for the app on the PAYIQ website. There is also a policy accessible through the link in the app. The policy makes it clear that no personal information is transferred to third parties.* *<u>Openness:</u> The information of the privacy policies and related documents are available through the app and website of both PAYIQ and Foli.*	*Openness: The link to the app-specific privacy policy is only easily found through the Foli website. The said policy is only available in Finnish which may hinder ease of user-friendliness. The link to the same policy is not available on the app, but instead, it Provides a link to 'Terms of use.' This includes a clause 'Personal data and protection' which is only a summary of the earlier Privacy Policy. Special permissions like access to the camera are not explained in the policies.*

3	Principle 3 – Respect for User Privacy Consent, Accuracy, Access, and Compliance.	Information is collected considering the interests and needs of users.	*<u>Consent:</u> The app begins with a welcome screen and asks for permission to use user location to improve the 'security' of the app. The information for other permissions granted is not explicitly asked. The app then proceeds to display the 'Terms of Service' which from the look of it has only one clause dedicated to Privacy and does not mention all the information from the Privacy Policy found of the website. There is an acute lack of specific consent for the collection, use or disclosure of personal information.* *<u>Access:</u> The and updating of the information finds mention on the terms of use, and the user is advised to inform the organization if there are any changes to relevant personal information like the email address or phone number. Regarding the accuracy and completeness of the information is not directly mentioned but can be seen indirectly through the user information available to view and then the user can inform if changes are to be made.* *<u>Compliance:</u> Various redressal mechanisms are provided in terms of use of the application like reclamations related to tickets and jurisdiction of law applicable and where to lodge a claim.*	*The security aspect of location data is not explained by the app adequately. The assertion is vague. The other permissions granted to the app like usage of camera, network data, and device specifications are not asked explicitly nor is it mentioned in the following Terms of Use. Higher the sensitivity more the quality of the consent should be, and this is lacking.* *<u>Accuracy:</u> Measures taken to maintain accuracy and completes of information should be explicitly mentioned.*
4	Principle 4 – End-to-End Security –	*All relevant personal information collected.*	*<u>Security:</u> The privacy policy states that PAYIQ strives to protect best*	*<u>Applied security:</u> Technical and administrative*

#	Description of the PbD principle	Summary of personal information involved	Compliance	Assessment of Privacy Gaps and comments
	Lifecycle Protection Continuous security		*the data it collects and states the proper methods it uses to do so.* *Applied security: The Policy states that data is "protected against unauthorized access and unlawful or accidental data processing by appropriate technical and administrative measures." Processing of personal information is limited to only when in need of customer service, application development, and troubleshooting. Processing of data requires personal verification through the login of company employees. Any personal breach is reported within 72 hours through email.*	*measures are not mentioned in detail.*
5	Principle 5 – Full Functionality – Positive-Sum, not Zero-Sum satisfying all legitimate objectives – not only the privacy goals	*Legitimate objectives: Users to have access to services provided by Foli and Protect user data* *Privacy Goals:* *All data protection Principles*	*Functionality: Most functionalities of the app are available to both users who choose to give personal information to log in and those that choose to access the app without logging in. Logging in is required for instance to view purchases history.*	*The app does an excellent job of satisfying its objectives while upholding privacy. It is possible to avail all legal services without giving any personal information.*

#	Description of the PbD principle	Summary of personal information involved	Compliance	Assessment of Privacy Gaps and comments
6	Principle 6 – Privacy Embedded into Design Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrative and creative way.	*All personal information*	*Systematic and principles approach to Privacy within the organization and development of the app.* *When possible detailed privacy impact assessments to be carried out: This is not mentioned in any of the online documentation.* *Privacy impacts of technology: Processing of information is restricted to only minimal services and no information is transferred to third parties for marketing or other multifarious purposes.*	

#	Description of the PbD principle	Summary of personal information involved	Compliance	Assessment of Privacy Gaps and comments
7	Principle 7 – Proactive not Reactive; Preventative not Remedial Proactive Privacy Protection design approach which is preventative	*All Personal information collected*	*Commitment to laws: The commitment of PAYIQ to protect information is incumbent in its policies and design of the app which allows use without divulging personal information and follows GDPR, which is the applicable law. They also have an assigned privacy officer.* *Culture of continuous improvement: This does find mention in the policy where new additions are promised to be informed to users and their consent secured.* Established methods to anticipate and prevent threats: Current methods that the company employs are not mentioned in any of the online documentation. The login methods by PIN and fingerprint are some login security features but do not constitute tactics to anticipate and prevent threats.	*More information about the culture of improvement could be mentioned in terms of use.* *Laws: The details of the Contact person for matters related to the processing of personal data should be provided in terms of Use of the app and not only on the Code of Conduct of the Company.*

6.8.3 Step 3: Analysis of Risks

Privacy Requisites	Privacy issues	Likelihood	Impact	Risk Assessment	Comments
Privacy as the Default	Collection, purpose specification and Data	Unlikely	Moderate	Low	Personal user data is accessed only in the event of customers service

	minimization: Location data that is collected for 'security' is accessed by PAYIQ employees				or troubleshooting, and that reduces employees being able to access data without detection.
Use, Retention, and Disclosure Limitation	Email Data retained by PAYIQ is used for company marketing	Unlikely	Moderate	Low	There are different data policies for the data collected by PAYIQ on its website and for the Foli app. The apps data policy mentions that data is deleted on user request and also after the closing of the account. None of this data in its life cycle is used for marketing or any other third-party purposes.
Visibility Openness	The user wants to read the privacy implications of the application	Likely	Moderate	Low	The app does display the terms of use with a section dedicated to data privacy but is not the actual privacy policy, which is only available in Finnish.

Respect for User Privacy Consent, Accuracy, Access, and Compliance.	1. The user gets confused with permission for location data is asked for security reasons. 2.User confusion due to lack of Access of relevant privacy policies and other information	Likely	Low	Low	Location data is required by the app for stated security reasons. The reason is to access location-based route services but is not correctly mentioned. 2. The privacy policy is not available to view through the app. There is only a summary clause in the terms of the app.
End-to-End Security – Lifecycle Protection	1. An attacker may access traffic between the app and Foli servers	Likely	Moderate	Medium	Technical and admin procedures taken to secure data are not mentioned in the documentation. For example, data encryption used for traffic of data between Foli and PAYIQ.
Full Functionality – Positive-Sum, not Zero-Sum	None	None	None	None	None

Privacy Embedded into Design	Loss of Phone may lead to a privacy breach	Likely	Major	High	If the customer has logged in, then the personal information may be lost, but if not logged in, then no information is lost. The app allows to use it without logging in.
Preventive and Proactive policies	None	None	None	None	None

6.8.4 Step 4: PIA Report and Recommended Actions

A PIA report is nothing but a compilation of the previous three steps conducted within the PIA. The objective is to put all information together in one document so that the next steps of taking action and reviewing the PIA for formulating potential checkpoints can be done effectively. Since we already have the previous steps together in one place; this step is already accomplished. As an attachment, a proforma of a PIA report is attached for use. The only part of a PIA report that is left out is formulating recommendations which are done as follows:

#	Recommendation	Yes/No
R/01	Make available the entire Privacy Policy through the application in relevant languages supported by the application, i.e., Finnish, Swedish, English, and Russian	
R/02	Specify in the Privacy Policy more details about which technical and administrative procedures are used by PAYIQ to protect personal information.	
R/03	Specify the correct purpose for usage of personal location information from ‘security’ to ‘access location-based route services’.	
R/04	Ask specific user consent to use device information, email address and phone number for processing.	

R/05	Good privacy practices are always appreciated. Inform the user exactly which functions are accessible when logged in and when accessing the app without logging in.	
R/06	Mention information about the Data Protection Officer in the Privacy Policy, which is accessible from the Application.	
R/07	Inform users to keep phone password protected in the event of loss	

6.8.5 Step 5: Action list[165]

#	Actions approved	Responsible people	ETC
R/01	Create a button to access Privacy Policy within the Application. Translate it into relevant languages.	The application Design team in consultation with Data Protection officer.	
R/02	Specify in the Privacy Policy more details about which technical and administrative procedures are conducted	Network Management in consultation with Data Protection officer.	
R/03	Specify the correct purpose for usage of personal location information from 'security' to 'access location-based route services'.	Application Design team	
R/05	Inform the user exactly which functions are accessible when logged in and when accessing the app without logging in.	Application Design team	
R/06	Mention information about the Data Protection Officer within the app.	Application Design team	
R/07	Inform users to keep phone password protected in the event of loss	Application Design team	

6.8.6 Step 6: Review and use as a Checkpoint

Considering the growth plans of the application to include services and expand it is advised that the PIA checkpoint to implement PbD Principles be created in the event of the approval of such an upgrade to the application. The PIA process can be initiated as soon as the upgrade is approved so that the design stage of the app can benefit from the data derived from the PIA.

[165] *As this is a PIA conducted for purely academic purposes the information for responsible person is filled out only for understanding purposes and is not true.*

After the checkpoints are created, the same are to be informed across the organization, and a person is to be designed to oversee the PIA process.[166]

6.9 From abstract principles to robust technical measurements

Let us have a look at the various measures and design patterns that emerge out of this project:

#	Privacy Pattern or Privacy Preserving Measure	Observation in System
1.	Authentication	Username and password login or PIN-based login with fingerprint capability
2.	Privacy Policy	The application has a privacy policy and terms of use along with the company's code of conduct
3.	Encryption	Appropriate technical measures are mentioned to be used to protect data, but the method is not mentioned
4.	Anonymization & Pseudonymization	Using codes as identifiers Moreover, logging in without signing up
5.	Access control	Private information accessed only in specific scenarios and only by certain authorized personnel
6.	Notification & Awareness - Breach Management Process and notification	Planned notification and awareness when updating and introducing new collection or use of personal information. There is also an awareness plan in the event of a breach of personal data.
7.	Minimization of data	Concrete plans of what is collected as per requirements and processed
8.	Logs	Purchases and transaction logs of users are maintained
9.	Post incident Evaluation: Audit	No post-incident evaluation mechanism mentioned in Privacy Policy or code of conduct.
10.	Privacy User settings and defaulted to most secure	The app does not have a dedicated section for controlling privacy setting where users can control their privacy information
11.	Dedicated information security policy	Lack of information as to how all the information is secured
12.	Acknowledgment of security responsibility	Responsibility for reporting a breach is acknowledged and also of protecting the information

[166] *Preferably the DPO as he/she is well versed with privacy concerns.*

13.	Documented Privacy Assessments	Lack of documented privacy assessments

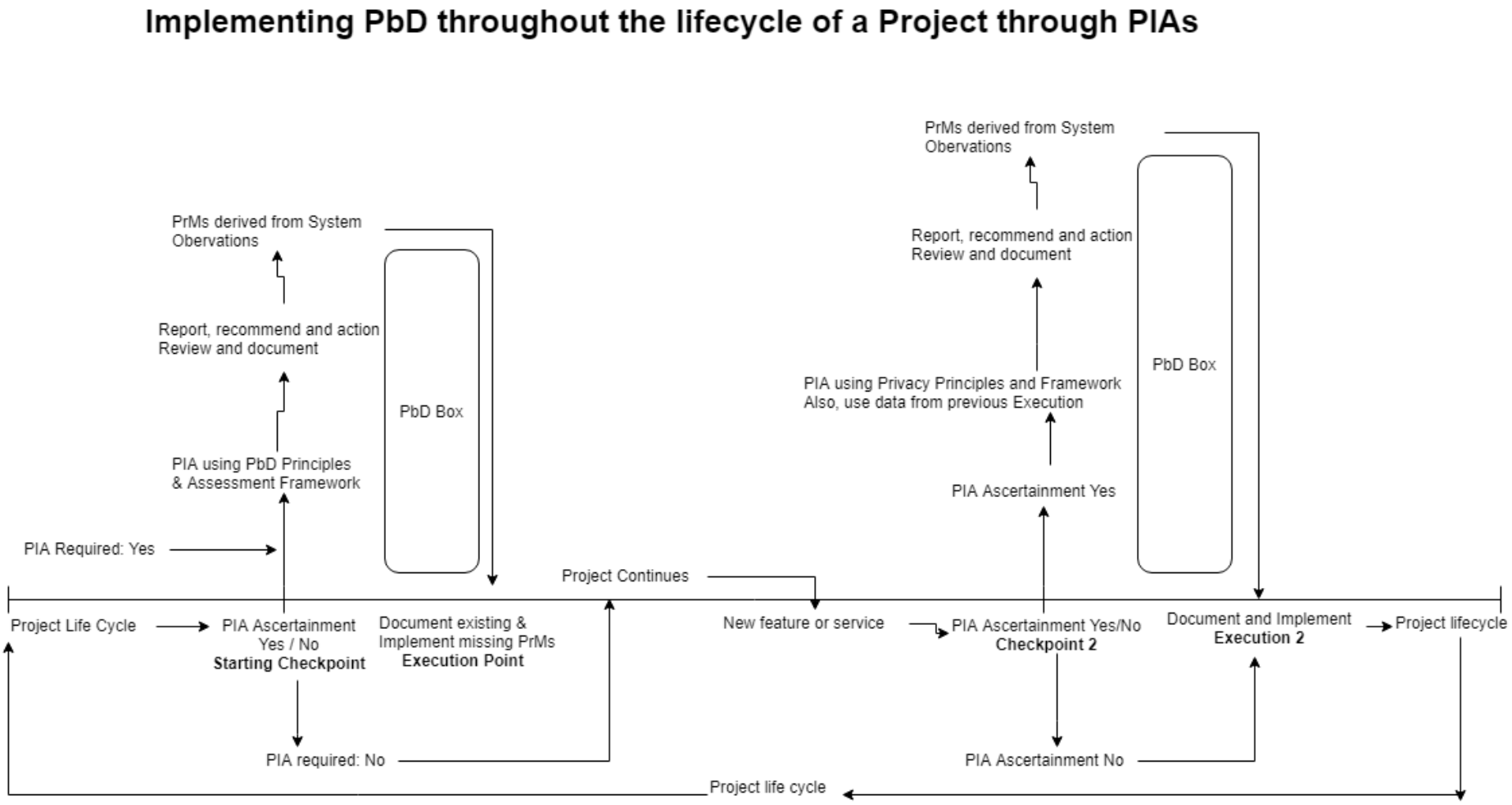
These Privacy Preserving Measures (PrMs) can now be connected to the Privacy Principles to demonstrate compliance with the PbD process:

	Authentication	Privacy Policy	Anonymization	Access control	Notification & Awareness	Minimization of data	Logs	Encryption	PIA and Risk Assessment	Audit	Dedicated Privacy Settings	Dedicated Security Policy	Acknowledgment of security responsibility
Privacy by Default			✓	✓		✓					✓		
Privacy Embedded into Design		✓							✓				
Full Functionality													
Lifecycle Protection	✓		✓					✓				✓	✓
Visibility and Transparency		✓					✓						
Proactive, not Reactive										✓			
Respect for User Privacy		✓		✓	✓								

Figure 11 Connecting PrMs to demonstrate compliance to PbD Principles

Mapping of these privacy measures will allow using them to be used throughout the development process of projects. These measures can then be used throughout the lifecycle of the project instead of the principles that were used during the PI

Figure 12 The lifecycle model for PbD process



7. Conclusion

The thesis has aimed to operationalize PbD by using a PIA process and deriving certain privacy preserving measures (PrMs) in systems under constant development, which is a characteristic of modern systems. For example, mobile applications are updated to include new features multiple times in their lifecycle. The thesis has performed a privacy analysis using PIA on one such mobile application system and subsequently also analyzed Privacy Preserving Measures incumbent in PbD Principles. A unique framework has been developed to implement the PbD process. This has been done to show the effectiveness of PbD process if conducted via PIAs and then to develop a model for lifecycle implementation. For the model to conduct PbD process, the following sources are used for the construction of this model: Ann Cavoukian's PbD Principles, Kroener and Wright's Operationalization suggestions, New Zealand PIA Toolkit, Australian Risk Assessment Model and lastly the Assessment Control Framework developed by Privacy by Design Centre for Excellence at Ryerson University.

Some privacy risks were identified through the PIA conducted concerning the Föli system. Several recommendations were made, and actions suggested as a part of the PbD process. Further to demonstrate its workability, the PrMs were derived from the Föli system as a part of the PIA process to show compliant and non-compliant elements. With this, the primary **Starting Checkpoint** and **Execution Checkpoint** were successfully created and, if chosen, this process can be continued throughout the life of this system, as shown in figure 12. The Föli app was developed in Turku, Finland, and awarded the best app in 2016. Hence, it comes as no surprise that it already has a lot of positive privacy considerations within its design, including most of the PbD Principles. This demonstration has successfully shown that the PbD process can indeed be effectively carried out through PIAs. Further, it has also been shown that to make the PIA process more technically robust, as the last step, PrMs are derived from the observations for future documentation and implementation.

The gap between the regulation of PbD and its operationalization has been due for a long time.[167] This thesis has attempted to address that gap by firstly instigating a discussion on the often-misconstrued topics of Privacy and then its subset, PbD. The process of PbD and its effectiveness through a PIA has been demonstrated through an experimental PIA conducted on an existing system.

[167] *Kroener – Wright 2014, p. 362*

All this cherry-picking of frameworks have contributed to building a model that can be used to assess the risks and gaps incumbent within a system has about the personal information.

Most importantly, this model has shown that PbD process can indeed be effectively conducted by using PIAs during the lifecycle of a system. The importance of PbD principles has been shown by incorporating them within the heart of the PIA process and identify gaps within the system. As suggested by Cavoukian, all the principles have been included in the PIA, and none have been left out. In order to address the vagueness of the principles, the Assessment Control Framework developed by Privacy by Design Centre for Excellence at Ryerson University has been used to bring some scientific certainty to the entire PbD Process. This facilitates both functional and new projects to have a quick checklist of technical measures which can be detected, thus ensuring the presence of PbD principles. This has enabled in creating a working lifecycle model which can be used throughout the lifecycle of a project. More work needs to be done to develop this model further and involve PETs within the process, as suggested by Kroener. Furthermore, work is needed in incorporating PETs into the operation framework of PbD and addressing concerns regarding the use of biometric data.

Although the mention of PbD within GDPR has meant substantial progress within the field, it is still clear that a lot of work is still needed to operationalize PbD. The ISO is developing its guidelines for a PIA process, and there is an expectation that it will also envision the use of PIA for PbD processes. Only mentioning PbD principles through the law is not enough, especially for information systems that are always subject to change and update. A more dynamic process is needed, and the currently developed model is one step in that direction. The PbD process also needs a certification mechanism which systems can use after they have completed the PbD process to show compliance. GDPR does envision such a mechanism in its Article 42, but still, further development is needed in this certification program.