

Privacy by Design  
Principles as a Foundation to a More Secure Internet of Things

by

Mohamad Oubai Rejleh

B. Comm, Ryerson University, 2008

A Major Research Paper

presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Master of Digital Media

In the Program of Digital Media

Toronto, Ontario, Canada, 2016

© Mohamad Oubai Al Rejleh, 2016

## **Author's Declaration**

I hereby declare that I am the sole author of this Major Research Paper (MRP). This is a true copy of my MRP, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this MRP to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this MRP by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my MRP may be made electronically available to the public.

Mohamad Oubai Al Rejleh

## **Abstract**

The Internet of Things (IoT) is a revolutionary concept that emerged in the late 21<sup>st</sup> century, whereby everyday objects such as household items, cars, and wearables, equipped with sensors and (Radio Frequency Identification) RFID chips, can communicate with the internet and to their physical surroundings. These chips allow the connected items to share information, and allow the user to collect information about his/her “quantified self”, measuring personal data such as habits of usage, lifestyle, and location through internet networks. IoT enabled devices are designed to collect, store, share, and analyze of highly personal data ubiquitously and in real time. However, with this new affordance of connectivity, comes a potential loss of privacy for users, as ever increasing sets of personal data are collected and tracked. As such, there is a pressing need for privacy considerations to be embedded within the early stages of design of connected devices and networks.

## **Acknowledgments**

I am grateful to the Creator, the most gracious and merciful, for allowing me to complete this research paper.

I first would like to express my gratitude to my supervisor, Ramona Pringle, who has guided me and believed in me throughout my time at Ryerson University. Her relentless encouragement and valuable input were key factors in the completion of this graduate research paper. It has been a great privilege to have worked with an inspiring and accomplished professor such as Ramona.

I would like to extend my gratitude to Dr. Ann Cavoukian, who has been a great source of inspiration in this research. I also would like to thank Mr. Michael Carter for the valuable support he has provided me with through my journey at MDM. I would like to extend my appreciation to my friends and colleagues in the MDM 2015/2016 Cohort for their constant support throughout my time at Ryerson University.

Finally, no words are enough to thank my parents Mouna and Ahmad, my siblings Dana, Kinan, Rasha, and Banan, and my loving and caring wife Rawa for their endless support, inspiration, and unconditional love. I am very blessed to have you in my life.

# TABLE OF CONTENTS

<b>Author's Declaration .....</b>	<b>ii</b>
<b>Abstract.....</b>	<b>iii</b>
<b>Acknowledgments .....</b>	<b>iv</b>
<b>List of Tables .....</b>	<b>vii</b>
<b>List of Figures.....</b>	<b>viii</b>
<b>Introduction.....</b>	<b>1</b>
<b>Chapter One – Evolution of Internet of Things .....</b>	<b>2</b>
1.0 What is The Internet of Things (IoT)? .....	2
1.2 The 3 Cs of the Internet of Things .....	6
1.3 The Evolution of the Internet of Things .....	8
1.4 IoT Applications .....	11
1.5 The Future of IoT.....	12
1.6 Securing the Internet of Things.....	15
<b>Chapter Two – Ethical and Privacy Concerns with IoT Applications .....</b>	<b>22</b>
2.0 What is Privacy? .....	22
2.1The Importance of Privacy in the Digital Age.....	25
2.2 Privacy v. Security .....	27
2.3 Privacy is Beyond Secrecy.....	28
2.4 Privacy in IoT .....	29
2.5 IoT Privacy and Security Risk Assessment .....	31
2.6 Should Consumers Be Worried For Their Privacy in the IoT Era? .....	33
2.7 Examples of Privacy Legislations in the Digital Era .....	35
2.8 Privacy by Design Is an IoT Must .....	36
<b>Chapter Three – Privacy by Design .....</b>	<b>38</b>
3.0 What is Privacy by Design? .....	38
3.1 Privacy by Design 7 Founding Principles.....	39
3.2 Benefits of PbD.....	41
3.3 Extending PbD Founding Principles.....	42
3.4 IoT Security Design Challenges .....	45
3.5 Why is PbD Important for the Future of IoT? .....	48
<b>Chapter Four – The Future of embedding Privacy by Design in IoT Applications .....</b>	<b>51</b>
4.0 How will IoT Change the Future of Cybersecurity .....	51
4.1 The Future of IoT Depends on Implementing Proper Security Measures .....	54

4.2 Why PbD is Essential to the Users of IoT .....	56
4.3 Challenges of Implementing Privacy and Security in IoT .....	62
4.4 Road Map to Overcoming the Challenges of Implementing PbD in IoT .....	68
Conclusion .....	75
<b>References</b> .....	76

## List of Tables

Table 1 - IoT Application Categories .....	11
Table 2 - Future Trends of IoT .....	13
Table 3 - Future Trends of IoT .....	14
Table 4 - Summary of OECD's basic privacy principles .....	36
Table 5- Extending PbD 7 Founding Principles for the IoT era .....	45
Table 6 - Top 10 Security Threats in IoT today.....	53
Table 7 - Summary of the seven categories of privacy threats and their potential impact .....	64

## List of Figures

Figure 1 - Components of an IoT System of Device .....	4
Figure 2 - The Evolution of the Internet of Things.....	5
Figure 3 - From WWW to the IoT; Next Steps in internet evolution .....	10
Figure 4 - The Internet of Things Opportunity and Applications .....	12
Figure 5 - Secure IoT Framework.....	16
Figure 6 - PTC Seven Steps to Minimize IoT Risks.....	20
Figure 7 - A diagram to help define privacy.....	24
Figure 8 - Privacy v. Security v. Anonymity .....	27
Figure 9 - Security Risks and Challenges for IoT Devices.....	32
Figure 10 - Privacy by Design 7 Founding Principles, overview .....	40
Figure 11- An illustration to demonstrate the top 10 challenges of securing IoT communications .....	48
Figure 12 - Understand your role in the digital security universe .....	52
Figure 13 - % of business executive respondents who rate IoT products in their industry high on resilience to cyber-attacks.....	57
Figure 14 - The Expanded Attack Surface of an IoT System .....	58
Figure 15 - A Framework for People-Centric Security as proposed by Tim Scholtz from Gartner73	
Figure 16 - The Three Stages of Cybersecurity Maturity Responses — Activate, Adapt and Anticipate (the three As).....	74



## **Introduction**

A smart coffee machine that is capable of re-ordering coffee beans automatically, autonomously, and without the need for human intervention is capable as well of brewing the perfect cup of coffee daily right when the homeowner walks up to start his day. A thermostat is smart enough to learn the temperature preferences and daily routines of its homeowners and it is capable of adjusting the temperature of a home to the homeowners comforts zone. These smart, internet-connected, and autonomous devices are part of a growing industry known as the Internet of Things (IoT). Citizens of today's digital world are progressively becoming heavy dependent on smart, interconnected, and autonomous applications in many phases of their daily lives. In December 2013, Gartner predicted 26 billion IoTs to be deployed globally by the year 2020 (Bradbury, 2015).

The Internet of Things (IoT) is soon becoming a vital part of our daily lives, yet its security and privacy vulnerabilities are a source of major distress affecting its future success and prosperity. A key question remains unanswered, who is responsible for the privacy and security of the IoT? How can technology vendors assure the security and privacy of possibly billions of IoTs from invasions by hackers and unauthorized parties, who might try to gain access to highly private consumer data and could seriously compromise the personal privacy of millions of people and even threaten the safety and wellbeing of societies? To better answer these pressing privacy-related questions, IoT developers and vendors need to put privacy and security of end users as a top of mind concern while designing their smart inventions. They need to ensure their users' privacy throughout the IoT application lifecycle. Hence, end users would be confident that their participation in the IoT era carries the minimum amount of risk for their privacy and security.

## Chapter One – Evolution of Internet of Things

### 1.0 What is The Internet of Things (IoT)?

IoT refers to a rapidly growing network of connected devices and systems that are able to make sense of its presence as well as its physical location while communicating with other connected devices via the internet. Connected devices have unique digital representation while connected to the surrounding devices and communication networks. In 1999, Kevin Ashton, cofounder and executive director of Auto-ID center, gave a presentation at Proctor & Gamble (P&G) about the importance of connecting Radio Frequency Identification (RFID) devices, a hot topic back then, to P&G supply chain (Techopedia, 2015). Kevin's thoughtful words could be best described today as the vision of IoT, *"If we had computers that knew everything there was to know about things - using data they gathered without any help from us - we would be able to track and count everything, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best"* (Kevin Ashton, 2009).

The simplest and most concise definition of IoT is adopted from Gartner's information glossary definition; IoT is the network of physical devices with embedded technology which enables them to communicate, sense, and interact with their internal states and with their external environment ("Gartner Information Technology Glossary," 2016).

According to a recent report on the Internet of Things by the office of the privacy commissioner of Ontario, most IoT definitions would include some or all of the following eight elements (Dennedy, Fox, & Finneran, 2014):

1. IoT devices are economic, widely used (ubiquitous) and are equipped with sensors to collect and transmit data.

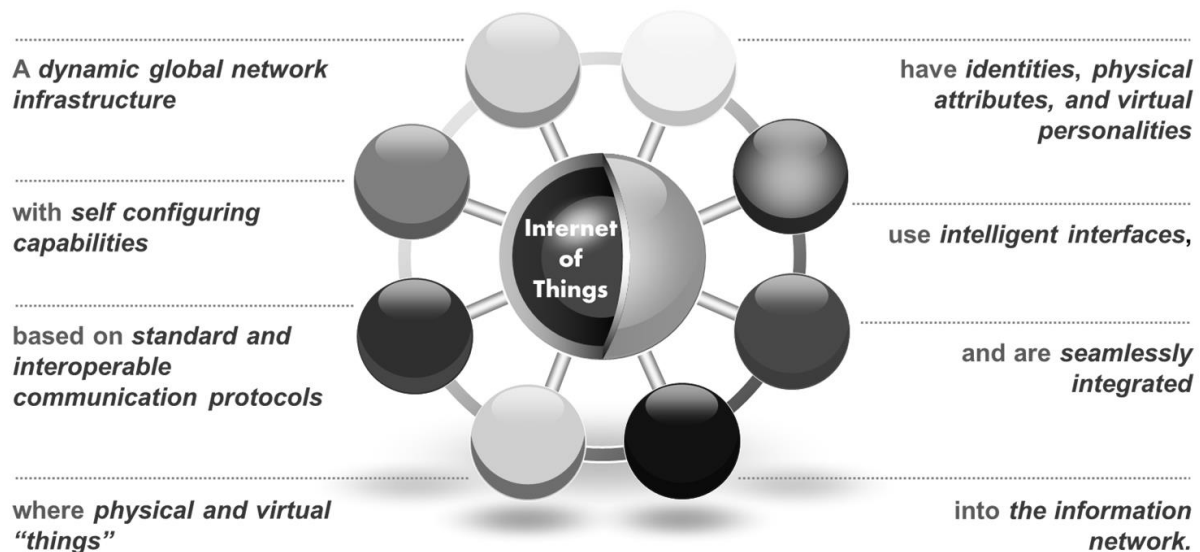
2. IoT devices are designed to collect and transmit commands and data.
3. Connected devices are integrated and do communicate with a larger network via internet and telecommunications technologies.
4. Since IoT devices bear their value from their ability to connect with other devices and networks to share data, they are equipped with communication protocols and standards to allow them to intercommunicate and transmit data.
5. IoT devices act as a bridge which connects the internet world with our physical (tangible world).
6. IoT devices have identities, physical attributes, and virtual personalities. This is important since they play a key role in communicating a unique set of user behavioral and user-geospatial data. Such data become unique user identifiers and could be used by vendors to customize unique products and services for specific end-users.
7. IoT devices and applications intercommunicate among each other without any human intervention in a fully autonomous way.
8. The data communicated and originally gathered by IoT devices are stored in data centers and grouped later for further analysis and data mining.

It is important to keep in mind that both IoT security and privacy are not discussed as a centerpiece to the definition of an IoT device or system. It is the lack of prioritizing end-users' privacy and security as a top of mind issue while thinking of IoT applications or systems is what inspired the research of this academic paper. Security and privacy have always been an afterthought while designing applications for IoT realm.

Therefore, an IoT system would be composed of eight key components (PTC Cloud Services, 2015, p.3):

- |                                    |                                 |
|------------------------------------|---------------------------------|
| 1. Connected devices / products    | 2. Business systems             |
| 3. Cloud-based technology services | 4. Communication infrastructure |
| 5. Smart product application       | 6. Connectivity                 |
| 7. External source of data         | 8. Internet of Things Users     |

What is evident from this list is that there is no mention to a security or privacy component in most of today's IoT products and services. The figure below represents the European Research Cluster on the Internet of Things (IERC)



**Figure 1 - Components of an IoT System of Device**

(Guillemin et al., 2014)

## 1.1 Why is IoT Important?

IoT is important because it has the potential to impact every aspect of our lives and every object people interact within a given day. The importance of IoT comes from the variety of applications they touch and have become integrated with. For example, IoT applications range from smaller scale smart devices such as Fitbits to the large scale and more complex applications such as smart cars and smart grids (Brendan O'Brien, 2014). Below are three key applications that are developing on a global scale (Brendan O'Brien, 2014):

- *IoT Applications for a Smart Natural Disaster Management:*

Connected and smart devices, in this realm, aim to help to predict natural disasters while allowing people to respond quickly and appropriately during emergency times.

- *IoT Applications for a Smart Urban Management:*

A civilized society aims to improve the standard and quality of living for itself and its fellow citizens. IoT could automate a lot of daily routines in today's urban life, such as traffic controls, power grid, and gas emissions from our energy facilities and power plants.

- *IoT Applications for a Smart Healthcare Management:*

Wearable smart devices can detect patients' wellbeing and potential medical issues and allow for prompt medical response and accurate medical care. Such cutting edge technology can and will improve the healthcare service and industry.

While the IoT applications are countless, they all share a single key attribute; IoT devices collect data about their users and their usage patterns and allow for data mining (Emanuele Angelidis, 2015). Let us take a look at IoT applications in Healthcare. A hospital with several smart and connected devices would allow the hospital's staff and probably third party healthcare professionals to collect very sensitive and personal information on the health status of patients

including private personal patient details. While the collection of such data could be helpful for the health staff to optimize and personalize their services, it poses tremendous amount of privacy risks to the patients and their family and loved ones if such data falls into the hand of hackers or unauthorized parties such as potential employers or insurance providers (Council, Healey, Pollard, & Woods, 2015; Hannah Becker, 2013).

Potential risks to humans' privacy will be discussed in greater details in further chapters. However, the goal here is to give a glimpse of the risks such unprotected data could cause to end users.

The intention here is just to bring a balanced view of the importance of IoT while drawing the attention of the potential risks associated with such great technology. In my opinion, IoT's first and foremost importance comes from its ability to share and transmit all sorts of data about itself, users, environment, and even detailed behavioral information about how a particular device could be used in the future. Still, there is a need to keep user privacy and security to be a top of mind issue within IoTs developers and designers.

### *1.2 The 3 Cs of the Internet of Things*

The three key areas of how IoT could affect our communities, businesses, and environments are, communication, cost savings, and control (Lopez Research LLC, 2013).

*Communication:* The internet of things is able to transmit and share critical data about people, systems, environments, and event habits of their usage. The key in this process is automation. In the past, sharing such data needed elaborate preparation and efforts. Currently, such process is done autonomously and in real time (Lopez Research LLC, 2013).

Though, the risk that Lopez research did not address yet again is privacy. The risks associated with misuse of data automation and what would happen if such critical data falls into the wrong hands. While automation aims to improve data communication streams, little attention is given to data monitoring and data governance. The goal is to protect the freedom and privacy of the very same people IoT has been created to serve. Thus, privacy needs to be the top of mind when data communication and IoT are being discussed.

*Control and Automation:* This would be the second C in how IoT could alter the daily lives of millions of people around the globe. As mentioned before, IoT brought a tremendous amount of automation to data collection and insights. It brought as well the ability to remotely control the smart device using an elaborate network of sensors and actuators. For example, smart homeowners would be able to remotely turn on or shut down a specific piece appliance at their homes or even adjust the temperature in their living room before they arrive home from work (Lopez Research LLC, 2013). Lopez report did not discuss the potential risk associated with IoT Control and Automation. For example, a smart lock could be attacked by a hacker who can initiate an access denial attack where an attacker prevents the homeowner from entering his/her own house or even worst, allowing unauthorized personnel to enter the premises.

*Cost Savings:* There is now doubt of the economic value of adopting the IoT revolution. For example, IoT provides the industrial world with great means to measure actual service and product performance while allowing for real-time monitoring of equipment readiness. This will reduce production interruptions, speed up production, improve delivery times, and help contain costs associated with equipment maintenance (Lopez Research LLC, 2013). Again, the author did not discuss the risk associated with poor privacy and security measures in IoT within the industrial and domestic settings. Vulnerabilities with industrial IoT connected devices could

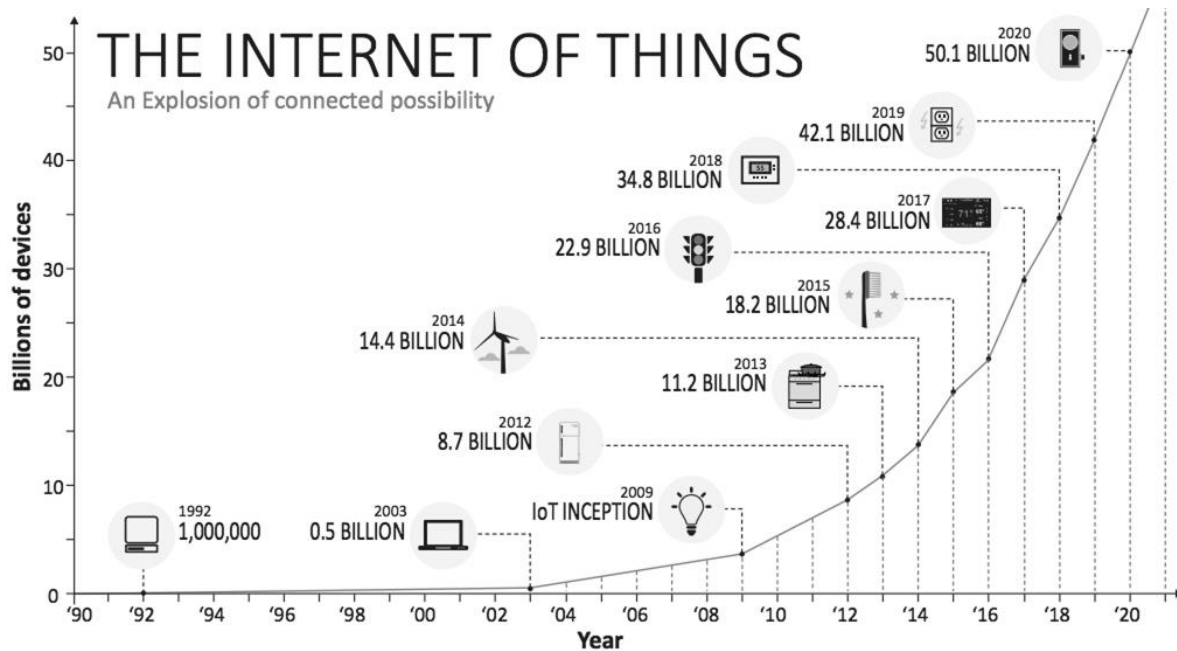
allow hackers to get access to private and proprietary sensitive information, thus resulting in industrial espionage (Bob Violino, 2013). As users expand their adoption of IoT, they need to pay close attention to risk issues which come with it. One must keep in mind that IoT, due to the current way it is designed, does have an elaborate network of infrastructure components, a lot of which are mission critical, and thus one would expect such system to be a primary target for hackers and industrial espionage (Bob Violino, 2013). In my opinion, while IoT comes with huge opportunities for cost savings and efficiencies, lack of proper security and privacy measures could cripple its potential and render an IoT investment null.

### *1.3 The Evolution of the Internet of Things*

In the early 1990s, Internet connectivity began to thrive within the enterprise markets and among a few high-tech enthusiasts. Nonetheless, it took the internet around 10 years before it gains momentum in the early 2000s. By early to mid-2000, getting access to the Internet became widely popular among enterprises, higher educational institutes, and governmental entities. In the early days of the internet, humans controlled the data collection and its transmission over the World Wide Web. One can say that automation and Artificial Intelligence signaled the starting era of the Internet of Things (IoT). In essence, IoT began when consumers started to witness some sort of autonomy and control from connected devices as to what Jim Chase from Texas Instrument said, *“When invisible technology operates behind the scenes dynamically responding to how we want “things” to act.”* (Chase, 2013, p.1)

It is expected that the number of connected devices will exceed 50 billion by 2020 (Chase, 2013).





**Figure 2 - The Evolution of the Internet of Things**

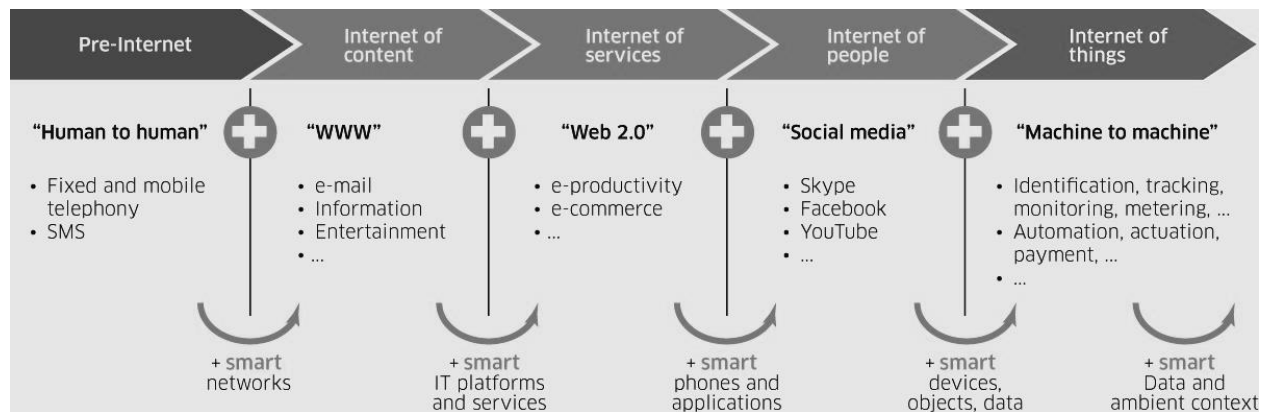
(Crews & Mangal, 2016, p.4)

Over the past 16 years, the internet has evolved from a network of computers and databases with static information into a dynamic and complex infrastructure of machines, smart devices, wearables, and applications (Jadoul, 2015).

There are five stages which led to the development of IoT:

1. Pre-internet (Human to Human Interaction): Physical Human direct interaction (Jadoul, 2015).
2. WWW (The Internet of Content): The internet as it is known as today, started in early 2000 with the creation of World Wide Web and HTTP (Jadoul, 2015).
3. Web2.0 (Internet as a Service): Started with the creation of e-commerce sites, and collaboration tools (Jadoul, 2015).

4. Social Media Networks (Internet of People): Late Steve Jobs and the legendary entrepreneur Marc Zuckerberg of Facebook are true fathers of the Internet of People revolution humans have seen since 2006/2007 (Jadoul, 2015).
5. Machine to Machine (Internet of Things): The future is now where everyday objects, such as wearables and smart machines (connected cars), are equipped with sensors, RFIDs, actuators, and internet connectivity. Such infrastructure enabled smart devices and systems to interact with each other creating a growing universe of connected devices (Jadoul, 2015).



**Figure 3 - From WWW to the IoT; Next Steps in internet evolution**

(Jadoul, 2015)

While the author discussed various ways to monetize the IoT through nurturing long tail industries and services, he failed to address privacy and security threats. In the IoT era, the “Things” are treated as autonomous fully-aware devices. Conversely connected “Things” are not capable of making a moral-guided decision when it comes to protecting end-users’ privacy and security. In efforts to bridge the security and privacy gap within IoT, leading IoT companies, such as Cisco and Intel, have become pioneers in creating services and products ecosystem to address the security threats of the new era. Such vendor-led efforts to protect IoTs were a reaction to enhance IoT adoption and to monetize and address threats of IoT to users’ privacy

and security (Tamarov, 2015). Such vendor-led efforts to protect the privacy and security of IoTs are great for the IoT space and for consumers' privacy.

#### *1.4 IoT Applications*

The IoT space has grown exponentially over the past 10 years, quickly becoming an integral part of the lives of many people around the world. In an effort to show the breadth of applications of IoT, as a means of explaining its rapid growth, this paper identifies thirteen key market application categories for IoT each with limitless possibility for great growth (Libelium, 2016; Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, & Hucheng Wang, 2014).

Top IoT Applications	Smart Cities and Buildings
	Smart Transportation
	Smart Environment
	Smart Water
	Smart Automotive
	Security and Emergencies
	Retail
	Logistics
	Industrial Control and Manufacturing
	Smart Agriculture
	Smart Animal Farming
	Smart Home Applications
	eHealth

**Table 1 - IoT Application Categories**

(Intel, 2016; Libelium, 2016; Shanzhi Chen et al., 2014)

While IoT applications are numerous, they all must have five key capabilities in order to be deemed effective and productive at delivering value to their end-users (Shanzhi Chen et al., 2014). These capabilities include Location Sensing and Sharing, Environmental Sensing, Ad Hoc Networking, and Secure Communications. Missing from this list of capabilities is a privacy protection framework. While IoT devices do have some level of basic security, privacy remains a key risk that the industry is yet to address. It is fundamental for us to distinguish privacy from

security. Without addressing privacy as an integral part of the IoT architecture and design, adoption of the smart things will halt and the cost to repair potential breaches of security and privacy will be irreparable.



**Figure 4 - The Internet of Things Opportunity and Applications**

(Jyoti Kundu, 2015)


As it applies to this context, security refers to the responsibility of the vendor to provide protection for all types of information in any form, so that the end-users' information's confidentiality, integrity, and accessibility are sustained at all times. Privacy, on the other hand, guarantees that end-users' personal information are gathered, handled, guarded and even if needed, destroyed in a legal and proper manner once requested by data owner (Siegel, 2016).

### *1.5 The Future of IoT*

The table below gives an overview of how IoT will be implemented on a global level over the next four years and beyond. The focus here is on building the proper infrastructure for full IoT applications utilization. There are lots of investments needed while building the right

technology, communication, and platforms to achieve ubiquitous IoT similar to that of the current global internet infrastructure. Despite the fact that the table below is dated back to 2008, the authors understood the necessity of addressing the importance of building proper security and privacy measures to support global scale adoption of IoT.

<b>Vision society</b>	<ul style="list-style-type: none"> <li>• Socially acceptable RFID</li> </ul>	<ul style="list-style-type: none"> <li>• Pervasive RFID</li> </ul>	<ul style="list-style-type: none"> <li>• Interacting Objects</li> </ul>	<ul style="list-style-type: none"> <li>• Personalized objects</li> </ul>
<b>People</b>	<ul style="list-style-type: none"> <li>• Realising benefits (food safety, anti-counterfeiting, health care)</li> <li>• Consumer concerns (privacy)</li> <li>• Changing ways to work</li> </ul>	<ul style="list-style-type: none"> <li>• Changing business (process, models, ways to work)</li> <li>• Smart appliances</li> <li>• Ubiquitous reader</li> <li>• Access rights</li> <li>• New retail and Logistics</li> </ul>	<ul style="list-style-type: none"> <li>• Integrated appliances</li> <li>• Smart transportation</li> <li>• Energy &amp; Resource conservation</li> </ul>	<ul style="list-style-type: none"> <li>• Mastered ambient intelligence</li> <li>• Interaction of physical and virtual worlds</li> <li>• Search the physical world (google of things)</li> <li>• Virtual Worlds</li> </ul>
<b>Politics &amp; Governance</b>	<ul style="list-style-type: none"> <li>• De-facto governance</li> <li>• Privacy legislation</li> <li>• Address cultural barriers</li> <li>• Future Internet governance</li> </ul>	<ul style="list-style-type: none"> <li>• EU governance</li> <li>• Frequency spectrum</li> <li>• Governance</li> <li>• Sustainable Energy</li> <li>• Consumption guidelines</li> </ul>	<ul style="list-style-type: none"> <li>• Authentication, trust and verification</li> <li>• Security, social well-being</li> </ul>	<ul style="list-style-type: none"> <li>• Authentication, trust and verification</li> <li>• Security, social well-being</li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>• RFID security and Privacy</li> <li>• Radio frequency use</li> </ul>	<ul style="list-style-type: none"> <li>• Sector specific standards</li> </ul>	<ul style="list-style-type: none"> <li>• Interaction Standards</li> </ul>	<ul style="list-style-type: none"> <li>• Behavioral Standards</li> </ul>
	<b>Before 2010</b>	<b>2010-2015</b>	<b>2015-2020</b>	<b>Beyond 2020</b>



	<b>Before 2010</b>	<b>2010-2015</b>	<b>2015-2020</b>	<b>Beyond 2020</b>
<b>Vision technology</b>	<ul style="list-style-type: none"> <li>• Connecting objects</li> </ul>	<ul style="list-style-type: none"> <li>• Networked objects</li> </ul>	<ul style="list-style-type: none"> <li>• Executable objects / semi-intelligent objects</li> </ul>	<ul style="list-style-type: none"> <li>• Intelligent objects</li> </ul>
<b>Use</b>	<ul style="list-style-type: none"> <li>• RFID adoption in logistics, retail and pharmaceuticals.</li> </ul>	<ul style="list-style-type: none"> <li>• Increased interoperability</li> </ul>	<ul style="list-style-type: none"> <li>• Decentralized code execution</li> <li>• Global applications</li> </ul>	<ul style="list-style-type: none"> <li>• Unified network that connects people, things and services</li> <li>• Interchanged industries</li> </ul>
<b>Devices</b>	<ul style="list-style-type: none"> <li>• Smaller and cheaper tags, sensors and active systems</li> </ul>	<ul style="list-style-type: none"> <li>• Increased memory and sensing capacities</li> </ul>	<ul style="list-style-type: none"> <li>• Ultra high speed</li> </ul>	<ul style="list-style-type: none"> <li>• Cheaper materials</li> <li>• New physical effects</li> </ul>
<b>Energy</b>	<ul style="list-style-type: none"> <li>• Low power chipsets</li> <li>• Reduced energy consumption</li> </ul>	<ul style="list-style-type: none"> <li>• Improved energy management</li> <li>• Better batteries</li> </ul>	<ul style="list-style-type: none"> <li>• Renewable energy</li> <li>• Multiple sources</li> </ul>	<ul style="list-style-type: none"> <li>• Elements of energy harvesting</li> </ul>


**Table 2 - Future Trends of IoT**

(Santucci & Lange, 2008, p.27)

It is estimated that by 2020 IoT will impact close to 6% of the world's global economy (BI, US Census Bureau, 2015). However, Asia, Africa, and Latin America will be leading the pack of global regions with IoT rate of adoption (PwC 6th Annual Digital IQ, 2014). The top three industries with the highest expected adoption of IoT are Energy & Mining, Power &

Utilities, and Automotive (PwC 6th Annual Digital IQ, 2014). Based on such huge potential and substantial growth, addressing IoT privacy and security is more important than ever.

<b>Vision society</b>		<ul style="list-style-type: none"> <li>Wide take up of RFID</li> </ul>	<ul style="list-style-type: none"> <li>Integration of objects</li> </ul>	<ul style="list-style-type: none"> <li>Interacting Things</li> </ul>	<ul style="list-style-type: none"> <li>Unlocked full potential of the Internet of Things</li> </ul>
	<b>People</b>	<ul style="list-style-type: none"> <li>Socially acceptable RFID</li> </ul>	<ul style="list-style-type: none"> <li>Ambient assisted living</li> <li>Biometric IDs</li> <li>Industrial ecosystems</li> </ul>	<ul style="list-style-type: none"> <li>Smart living</li> <li>In-vivo health g</li> <li>Security based living</li> </ul>	<ul style="list-style-type: none"> <li>Mastered continuum of people, computers and things</li> <li>Automated healthcare</li> </ul>
	<b>Politics &amp; Governance</b>	<ul style="list-style-type: none"> <li>First global guidance Standardisation</li> </ul>	<ul style="list-style-type: none"> <li>First global governance</li> <li>Unified open interoperability</li> </ul>	<ul style="list-style-type: none"> <li>Authentication, trust and verification</li> </ul>	<ul style="list-style-type: none"> <li>Inclusive Internet of Things</li> </ul>
	<b>Standards</b>	<ul style="list-style-type: none"> <li>Network security</li> <li>Ad-hoc sensor networks</li> <li>Protocols for distributed control and processing</li> </ul>	<ul style="list-style-type: none"> <li>Interoperability protocols and frequencies</li> <li>Power and fault resilient protocols</li> </ul>	<ul style="list-style-type: none"> <li>Intelligent devices cooperation</li> </ul>	<ul style="list-style-type: none"> <li>Health security</li> </ul>
		<b>Before 2010</b>	<b>2010-2015</b>	<b>2015-2020</b>	<b>Beyond 2020</b>



	<b>Before 2010</b>	<b>2010-2015</b>	<b>2015-2020</b>	<b>Beyond 2020</b>
<b>Vision technology</b>	<ul style="list-style-type: none"> <li>Low power and low cost</li> </ul>	<ul style="list-style-type: none"> <li>Ubiquitous integration of tags and sensor networks</li> </ul>	<ul style="list-style-type: none"> <li>Code in tags and objects</li> </ul>	<ul style="list-style-type: none"> <li>Smart objects everywhere</li> </ul>
<b>Use</b>	<ul style="list-style-type: none"> <li>Interoperability framework (protocols and frequencies)</li> </ul>	<ul style="list-style-type: none"> <li>Distributed control and database</li> <li>Ad-hoc hybrid networks</li> <li>Harsh environments</li> </ul>	<ul style="list-style-type: none"> <li>Global applications</li> <li>Self-adaptive systems</li> <li>Distributed memory and processing</li> </ul>	<ul style="list-style-type: none"> <li>Heterogeneous systems</li> </ul>
<b>Devices</b>	<ul style="list-style-type: none"> <li>Smart multi-band antennas</li> <li>Smaller and cheaper tags</li> <li>Higher frequency tags</li> <li>Miniaturised and embedded readers</li> </ul>	<ul style="list-style-type: none"> <li>Extended range of tags and readers and higher frequencies</li> <li>Transmission speed</li> <li>On-chip antennas</li> <li>Integration with other materials</li> </ul>	<ul style="list-style-type: none"> <li>Executable tags</li> <li>Intelligent tags</li> <li>Autonomous tags</li> <li>Collaborative tags</li> <li>New materials</li> </ul>	<ul style="list-style-type: none"> <li>Biodegradable devices</li> <li>Nano-power processing units</li> </ul>
<b>Energy</b>	<ul style="list-style-type: none"> <li>Low power chip sets</li> <li>Thin batteries</li> <li>Power optimised systems (energy management)</li> </ul>	<ul style="list-style-type: none"> <li>Energy harvesting (energy conversion, photovoltaic)</li> <li>Printed batteries</li> <li>Ultra low power chip sets</li> </ul>	<ul style="list-style-type: none"> <li>Energy harvesting (biology, chemistry, induction)</li> <li>Power generation in harsh environments</li> <li>Energy recycling</li> </ul>	<ul style="list-style-type: none"> <li>Biodegradable batteries</li> <li>Wireless power</li> </ul>

**Table 3 - Future Trends of IoT**

(Santucci & Lange, 2008, p.27)

## *1.6 Securing the Internet of Things*

Cisco has developed a technology-based framework to secure the IoT system. Cisco's vision is composed of four pillars (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016):

Authentication, Authorization, Network Enforced Policy, and Securing Analytics (Visibility & Control).

### *Authentication*

Authentication is the technical process by which the identity of an IoT device or system is verified. For example, when an IoT devices attempt to access the IoT network infrastructure, the permission is initiated based on verifying the identity of the smart device (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

### *Authorization*

Authorization is the second component of Cisco's security and privacy framework which allows an IoT to access the infrastructure network. Authentication and Authorization are the first two trust components that allow an IoT device to communicate and exchange data with other members of the IoT network infrastructure (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

### *Network Enforced Policy*

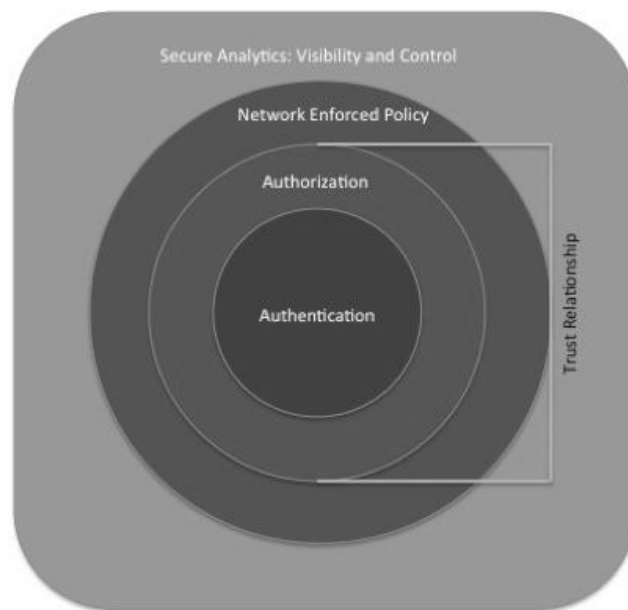
This pillar contains all technical features that transport and direct data traffic in a secure fashion over the various network infrastructure (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

### *Secure Analytics: Visibility and Control*

This pillar describes the services by which the various network infrastructure elements interact within the IoT ecosystem. It advocates the deployment of massive databases, combines business intelligence, and analytics capabilities to perform real-time data analysis to track any

suspicious data or information flow activities. It is important to gather data from multiple touch points to check for information integrity (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

What this framework is lacking is a privacy mechanism embedded throughout the lifecycle of the IoT device or system. Technology is not enough; in order to keep users and their data secure, companies need to change the way they think about privacy and security in first place.



**Figure 5 - Secure IoT Framework**

(Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016)

The proliferation of IoT applications requires thoughtful consideration to the potential security and privacy risks associated with a world filled with connected “Things”. Since the digital world meets the physical world in an IoT system, *“the threat moves from manipulating information to controlling actuation (in other words, moving from the digital to the physical world)”*.(Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016). Therefore, this increases the need to properly address the security concerns and propose a sustainable and viable security framework.



Adding to the urgency of addressing privacy concerns within IoT is the fact that connected devices gather and transmit lots of personal data such as users' name, address, habits, and geolocation, and other personal identifying data such as age, date of birth, and even credit card numbers in some instances (Caroleloomis & Hpecom, 2015). Anytime personal data is exchanged, stored, and sent unencrypted over the internet, a door is opened for hackers to attain and potentially misuse such sensitive information. There are several key data privacy and security issues IoT vendors need to address to ensure a secure connected world; Poor data authentication and authorization (Caroleloomis & Hpecom, 2015), Insecure and rather open web network( FTC Staff Report, 2015a), Insecure IoT middleware software (Caroleloomis & Hpecom, 2015; FTC Staff Report, 2015a), Lack or poor data encryption, Lack of transparency of data collection (Dennedy et al., 2014), and finally Heterogeneity and variety of IoT devices and platforms (Guillemin et al., 2014, p.90). For example, let us consider a Fitbit wristband which is a wearable accessory that gives its users feedback on their daily activities such as the number of calories they burned while commuting to work or while climbing the stairs daily. A Fitbit could authenticate the user as he or she access smart applications and devices. The issue is when the authentication process is poor or inadequate giving unauthorized third parties access to highly personal data about the user. On the other hand, lack or poor data encryption opens the door for hackers to exploit end-user's data and facilitate identity theft. Take an example of a user of a smartphone with poor data encryption. The poor encryption can open the door for criminals to decrypt the security on the phone and gain access to the end users' contacts and even banking details stored on the device.

*“By year-end 2017, more than 20% of enterprises will have digital security services devoted to protecting business initiatives using devices and services in the Internet of Things. It’s inescapable: The fundamental meaning of security is changing as things both inside your enterprise and those you create become connected to the Internet.”(Sondergaard, 2014)*

To address the previously mentioned privacy and security issues, a good practice is to start by:

- Building a task force of executive sponsors, security thought leaders, and privacy specialists who advocate for privacy-centric designs and business practices. Executive sponsors are needed to assure that initiatives get the utmost support from the highest level of the organization. Thought leaders and specialist are needed to design and propose effective privacy and security measures to make any IoT system more secure. The goal of creating such task force is to gain collaboration towards a more secure IoT systems (Turner, 2015).
- Embedding privacy and security measures and best practices in the early stages of any IoT product or system development will assure a sustainable solution to preserving end-users’ privacy and security. The best way to tackle privacy and security problems is to avoid them in the first place. This will be the most effective way to address such challenges (Turner, 2015).
- Clarifying and simplifying privacy and security basics and best practices among all beneficiaries of IoT systems, consumers, employees, and ecosystem partners. It is not enough for security and privacy task forces to be created or privacy to be embedded in the design of an IoT if the end users are oblivious of the basics to protecting themselves.

Consequently, the user-be-ware policy must be at the forefront before encouraging end users of an IoT (Turner, 2015).

- Simplifying and clarifying security and privacy policies in order to encourage users' adoption of IoT security and privacy best practices. Lack of training and education is as detrimental as poor security measures when it comes to addressing privacy and security concerns for IoT (Turner, 2015).

There will be always some level of risks no matter how carefully end-users approach the IoT space. However, IoT vendors and system designers can take a few steps to minimize inherited IoT risks during the early stages of planning the design of their services, connected devices, or even a group of connected smart objects. The goal is to lay the foundations for a comprehensive security and privacy plan for any IoT implementation.

First, IoT designers and vendors need to start securing the cloud infrastructure which supports IoT technologies. Securing an IoT infrastructure involves securing all communication channels between IoT endpoints, such as a smart meter and its IoT data hub, the place in the network where data is being processed and stored for further analysis and mining. Therefore, data servers must be encrypted so as the data which is transferred from the IoT endpoint to the data hub.

The second step to minimize privacy and security risks in IoT is to follow and apply industry-accepted privacy and security best practices such as the deployment of robust security controls to detect threats, protect end-user data, and provide continuous monitoring of the data flows in and from the IoT system.

A third step would be to design all IoT systems and components with keeping privacy and security in mind. Privacy and security by IoT design can eliminate early threats that could turn into big privacy disaster if left unchecked.

For a successful designing of an IoT device with privacy and security in mind, a forth good next step would be to secure the IoT device itself. Thus, the device needs to be physically secured from tampering and its internal codes and systems need to be well encrypted to prevent against hackers. For example, implementing a thorough authentication regiment is a key to assuring that an IoT device is securing all of the data it transmits. (PTC Cloud Services, 2015)

The fifth step in minimizing the privacy and security threats for IoTs is to secure the data connections between the IoT devices, IoT applications, and the IoT back-end network and computing services.

SEVEN STEPS TO MINIMIZE RISK
• Secure Cloud Infrastructure
• Leverage Standards-Based Best Practices
• Design for Security
• Secure IoT Devices
• Secure Device Connections
• Secure IoT Services and Apps
• Secure Users and Access

**Figure 6 - PTC Seven Steps to Minimize IoT Risks**

(PTC Cloud Services, 2015)

Since most data shared by IoT networks are stored in remote servers known as well as cloud servers, the sixth step would be to fundamentally secure the data centers which host the bulk of the end-users' data.

The last and seventh step in minimizing the security and privacy threats for an IoT system is to educate the end-users of the IoT system on security and privacy best practices and the safest way to handle and share their data(PTC Cloud Services, 2015).

Embedding privacy and hence security measures within the early stages of the IoT system design have to be the top of mind for IoT applications and systems to gain popularity and achieve their growth potential. What is privacy and why it is different than security? What are the risks that IoT users and vendors can face as a result of poor security measures with an IoT system or device? To answer those questions and others in better details, privacy and security professionals and advocates need to explore the various ethical and privacy concerns with IoT applications.

## **Chapter Two – Ethical and Privacy Concerns with IoT Applications**

### *2.0 What is Privacy?*

Privacy has many definitions and it varies from culture to culture. Yet, generally speaking, privacy is the right to have some personal time at a private place away from other people. Essentially, privacy is the right to be unaccompanied and away from distractions or interruptions (Iaap, 2016). An interesting phenomenon in the digital age is people's wide definition of privacy. For example, people's first reaction towards defining privacy normally shifts towards government surveillance and loss of privacy in today's connected world dominated by social networks such as LinkedIn, Facebook, and Twitter.

Edward Snowden, a former CIA contractor who fled the USA after leaking sensitive and scandalous information about deep and vast surveillance on a mass and global scale by various security agencies in the USA revelations in 2013, represented a huge wake up call for civil rights activists around the globe (BBC, 2014).

With that being said, privacy would be the right to be free from unwanted, unknown, hidden, or subtle surveillance, yet be able to make a decision as to if, when, how, why, and to whom one's personal details and information to be shared (businessdictionary.com, 2014; Doherty, 2016). Therefore, while discussing the topic of IoT privacy, designers and vendors need to take into account people's personal perspective and situation and reword the question and ask what privacy means to the individual (sourceLink, 2012).

The challenge in addressing privacy rights becomes even more complex given the proliferation of social networking and digital communication endpoints which challenge people's belief in privacy and freedom. Because of its widespread nature, it is beneficial to consider privacy through four different lenses; (1) privacy of the person, (2) privacy of personal behavior,

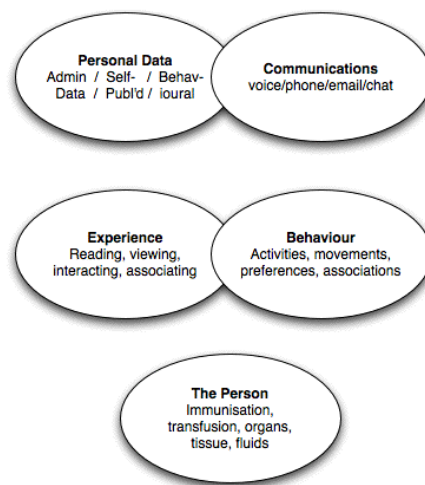
(3) privacy of the personal communication, (4) and finally privacy of personal information (Clarke, 2013).

In the past 30 years, computers and digital endpoints became an integral part of people's lives. Accordingly, information, communication, and privacy became inseparable elements especially as people exhibited a lot of personal behavior online such as shopping, internet browsing, social media communication, and another sort of digital behavior. This gave birth to the fifth lens of privacy – *personal experience privacy* (Clarke, 2013).

In the light of importance of privacy for a healthy society, below are key different dimensions of privacy (personal space which is sheltered from any interference by others):

- *Personal Privacy*: Personal privacy is the capability of a person or a group of people to segregate (remove) themselves, or hide personal facts about themselves, and hence express themselves selectively without fear of being judged or misunderstood.
- *Personal Behaviour Privacy*: This dimension of privacy is concerned with protecting individual's behaviours to sensitive matters such as personal habits, religious beliefs, sexual orientation, political affinities and views.
- *Personal Communication Privacy*: The right of individuals to interact with each other without fear of being monitored by others.
- *Personal Information Privacy*: This is the right of individuals to have a great degree of control over their own personal data such as the person or group who are allowed access to their data and how they use the data. This dimension is very important since IoTs gather and transmit personal data in real-time and then send and share such information over the internet.

- Personal Experience Privacy:** Personal experience is the act of reading a book or newspaper, browsing the web, watching a movie, making a phone call, taking pictures, visiting a place, walking the dog, and meeting friends and family. It is us being alive as humans. Before the inventions of smartphones, ubiquitous internet, and IoTs, all of these daily activities were temporary. None of them generated records that could haunt us back in the future to embarrass us. Take the example of those awkward high school graduation photos or wild drinking parties while on vacation. Each person's small-scale actions (experiences) and their combined extensive practices were hidden from others and from their out of context judgments. However, once peoples' experiences are uploaded on the World Wide Web, they become a record for someone to dig. As a matter of fact, most of peoples' daily activities and experiences now are monitored, stored, and recorded by corporations with data centers scattered around the globe. IoT end-users and customers have the right to live their daily lives and experiences without fear of someone judging them based on what they do and how they spend their personal time while browsing the net or living life.



**Figure 7 – A diagram to help define privacy**

(Clarke, 2013)



## *2.1 The Importance of Privacy in the Digital Age*

Digital privacy is a major concern for today's privacy-savvy consumers and digital-age-citizens especially after the 2013 revelation by Edward Snowden, as previously cited. Individuals have the right to control the data gathered about their digital behavior. As such, IoT designers and vendors need to differentiate between data and information when they speak of the digital age. Data refers to passive symbols, signs, and other general facts, figures, and numbers (Clarke, 2013). Such data would not lead necessarily to identifying a specific person; rather it would help build a general persona about people who share similar attributes. On the other hand, information refers to specific personally identifiable data about a specific individual, so allowing for personal identification and meaning extraction (Clarke, 2013).

The risks end-users of the digital economy face every time they browse the internet, engage in conversation on social media, or even shop online is to share a lot of highly personal and identifying information. As a result, citizens of the digital economy lose their privacy and put themselves at risk. This risk is aggravated in a case of a hacker gain access to end user's personal information and private data and use them for malicious purposes (Weitzner, 2007).

IoT can enhance various daily lives functions and dependability, such as cars, appliances, environments, business operations and processes, but what is the privacy and security price tag they potentially pay? Does this improved and convenient way of life have to come at the expense of people's right to lead a private personal life without the fear of being misjudged or monitored all the time? Every time customers use a smart device, an IoT, they face the risk of divulging their personal data to the third party who might abuse it or at least interpret it out of context in an undesirable manner.

Ignoring potential risks and turning a blind eye to them could be tempting (Cohn, 2015). So what if an intruder used a smart appliance to get access to private homes or even worst, control the cameras in our smart TVs or computers? How dangerous could that be? No one of us would want others to have access to their homes and record what happens in their living and bedrooms. Have end-users of IoT thought of what would happen to them if their insurance provider got access to their driving routes and habits? What if they decided to raise the premium or canceling their policy?

Our personal data can be misused if the vendor that collects our personal information and data opt to exploit the information or even worst, sell our personal data to the third party who has despicable intents and plans on using the data in a malicious way against us.

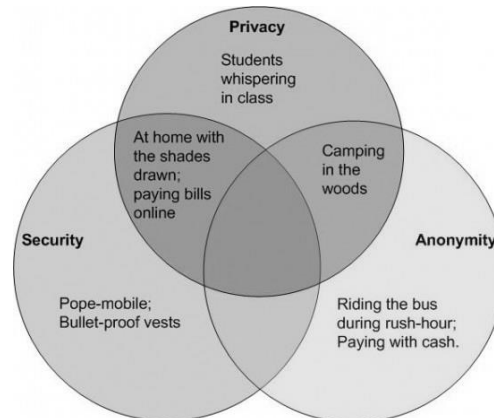
Take the example of a legitimate service provider that collects customers' data for valid reasons such as improving the customer experience or personalizing product or service offering. The company servers may get attacked, and the attacker illegitimately gets hold of consumers' private data. Sometimes, no attacker is involved. Take the example of a human error which results in private consumer data shared with other companies or entities without consumers' knowledge. Hence, exposing end-users' identity, shopping habits and preferences and much more.

This scenario in particular can subject companies collecting private consumer information to costly lawsuits and loss of consumer trust.

It is critical for all IoT designers and service providers to have effective frameworks and policies which govern how they use end user's data and how they can assure end-users' privacy. With that being said, the protection of end-users' data privacy begins at the source especially when data privacy has become a concern in today's digital economy (Iaap, 2016).

## 2.2 Privacy v. Security

The term privacy is often mistaken for security. Security refers to the protection of personal and important data against exploitation, unauthorized access, and modification by unauthorized personnel. On the other hand, privacy definition is much wider because it grants individuals the ability to control their own data and empowers them to have a say over who has access to their data and what kind of data is being gathered about them. Since security ensures the protection of data, it is probably not enough to address privacy concerns in the digital age without exploring a systematic way to address privacy. Sustainable privacy mindset requires the implantation of processes, laws, and policies that govern how personal data is collected, consumed, and shared about individuals (Thorne, 2015; Valerio, 2014; Zanolli, 2015; Iaap,2016).



**Figure 8 – Privacy v. Security v. Anonymity**

(ROMANOSKY, 2011)

*"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."*(Weitzner, 2007; Westin, 1967)

### 2.3 Privacy is Beyond Secrecy

There is a widely held misconception that if you have nothing to hide, you have nothing to fear (CLARK, 2016). In principle, privacy is a right granted to individuals which reinforces the freedoms of speech, expression, association, and assembly in a democratic society (Doherty, 2016). Confusing privacy, which is a basic human right, with the assumption that someone must be hiding something is a total misrepresentation of the truth; individuals have the right to have control over their personal data and privacy.

*“Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say.” –*

*Edward Snowden (Doherty, 2016)*

The idea that privacy is beyond secrecy was pioneered by Mr. Alan Westin in his book published in 1967, *Privacy and Freedom*. Westin feared that human dignity, rights, freedom of speech, and freedom of expressions would decay by governments’ misuse of their power over people’s private data (Weitzner, 2007). Citizens of today’s digital economy need a strong and comprehensive privacy laws that can protect individuals’ privacy in which organizations, government bodies, and individuals are all stakeholders in assuring proper privacy measures in place. Protecting individuals’ privacy is fundamental to prevent and protect against discrimination based on personal information even if such information is available publicly (Weitzner, 2007).

*“We have to engineer Policy Aware systems based on design principles suitably robust for Web-scale information environments. Here we can learn from the design principles that enabled the*

*Internet and the Web to function in a globally-coordinated fashion without having to rely on a single point of control” (Weitzner, 2007, p.2).*

With the proliferation of the internet, IoT, and digital endpoints, privacy and security experts can no longer consider privacy to be the right to hide information; rather it should be looked at as a way for governments to protect their citizens’ rights, dignities, and freedom. This can only be achieved if privacy is engineered through design thinking in all technology and application IoT customers use throughout their daily life (Weitzner, 2007).

#### *2.4 Privacy in IoT*

When speaking of privacy of the Internet of Things (IoT), there is an apparent and pressing need to first define four key terms; Data Control, Data Surveillance, Personal data surveillance, and Mass data surveillance.

- *Data Control (DC):* Automation in today’s digital world does create the risk of loss of control on personal data for IoT users. IoT are created to be autonomous and are able to conduct data collection and transmission operations in an automated fashion without user consent or even user awareness of the data communication flow (Cavoukian & Jonas, 2009).
- *Data surveillance (DS):* “DS is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons” (Clarke, 2013). The key point here is automation of monitoring, collecting, and analyzing of personal data. In today’s’ digital era, automation is done at scale and IoT is capable by

its inherited design of collecting, communicating, and analyzing the vast amount of personal data such as location, age, habits, preferences, and much more.

- *Personal data surveillance*: As the name implies “*is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of an identified person*” (Clarke, 2013). A Fitbit, sport smart wearable, records a lot of personal information about its users such as behaviors, activity habits, energy levels and much more. It is no wonder that such IoT wearable can pose a serious threat to users’ privacy especially in the case of someone stealing the recorded data (Maddox, 2016).
- *Mass data surveillance*: This is data surveillance automated through a system and at scale for a large group of people. For example, a smart energy meter for a condominium building would gather enough personal details about each household down to the level when they wake up, take a shower, and how often they use the washroom or whether they wake up to have a midnight snack or not (Clarke, 2013).

With the ability to collect, send, store, and transmit a tremendous amount of personal identification data known as personal identifiers, IoTs could pose a significant amount of risk to end-users if the data they collect falls into the hands of the wrong party. Machine learning, artificial intelligence and cloud computing technologies have made it possible for organizations to create associations and predictions about consumers’ buying habits, shopping behaviors, and much more. The ubiquity of the internet has allowed many companies to form a digital person based on one’s digital body language. A digital persona is a representation of a person’s personality based on collected data, historical habits, transactions, and actions which are then used as a tool to group individuals for a variety of commercial and non-commercial use (Clarke, 2013; Green, 2016).

There is no doubt about the limitless potential of IoT. Nevertheless, the IoT space and its current applications, spark a huge level of privacy concerns among both security activists and government officials. The European Union (EU) is far more advanced in proposing solutions and remedies for privacy concerns compared to the USA and Canada.

For example, EU recently funded Rules, Expectations, and Security through Privacy-Enhanced Convenient Technologies (RESPECT) project in which its main goal is to enable governments and technology organizations design, build, and deploy Privacy-Enhanced Technologies (PETs) to reduce the impact of ubiquitous surveillance and data collection on people's privacy (Diehn & Goebel, 2012).

## *2.5 IoT Privacy and Security Risk Assessment*

*“IoT technologies in general don't have good security. There are no legal frameworks that demand good security. We're racing ahead yet again without putting the security and privacy in.”*(Zanolli, 2015; Landau, 2015)

Given its current momentum and growth, the IoT space is set to contend with serious privacy and security issues. The lack of confidence in current security and privacy measures for IoT, such as smart wearables, is jeopardizing peoples' lives and even the future of the IoT space itself. Smart (connected) medical devices provide a timely and real example of the serious security and privacy risks associated with IoT items. A hacker could gain access to an insulin pump or even to a heart pacemaker using Bluetooth-enabled defibrillators and remotely alter and

manipulate controlled drug infusion drips causing the death or serious injury to the patient using such smart devices (Hernandez & Appleby, 2014; Zanolli, 2015).

One reason for privacy and security inherited risks for IoT applications is the gap between the speed at which companies build end to end privacy system for the connected devices and the speed at which companies innovate and build connected devices and IoT solutions.



**Figure 9 – Security Risks and Challenges for IoT Devices**

(Joshi, 2016)

Gartner, a renowned technology research firm, predicts that the IoT market will continue to grow to reach 25 billion, 50 billion for some other futurists, connected devices by 2020 (Zanolli, 2015). Therefore, the rush for inexpensive, fast, compact, and even miniature connected (things) leaves security as an afterthought for many IoT developers and startups (Zanolli, 2015).

*“The whole development cycle works against you from a privacy and security standpoint, especially if you are a start-up,”* – Lee Tien, Senior Staff Attorney at the Electronic Frontier

Foundation (eff.org)



Unless privacy and security are built as a foundational building block in the development of any connect device, system designers will be walking a slippery slope of exposing end users and organizations to massive risk threats.

Data Ownership is a murky area in the IoT space today. The challenge is to clearly define who owns the data and who has the right to alter, omit, or completely delete someone's data of the IoT server (Zanolli, 2015). The International Data Corporation, IDC, a global provider of market intelligence and advisory services, believes that IoT collected data will be stored in the cloud by 2020. Once in personal information on the cloud, it will become very hard if not impossible to control the data flow and even harder to protect or delete such data permanently (Maddox, 2016; Zanolli, 2015).

## *2.6 Should Consumers Be Worried For Their Privacy in the IoT Era?*

The IoT ecosystem is a relatively young space whereby most of its pioneering devices and platforms producers are early stage startups that have little or no profits. Therefore, it is understandable that they focus on innovating and selling connected things with little effort put into security foundations or measures (Britt, 2016).

*“84 percent of building automation systems such as elevators and Heating Ventilation Air-condition and Cooling (HVAC) were connected to the internet, with 35 percent of those bridged to the enterprise network. Thirty-one percent of respondents said a cyber security attack could cause significant harm. Yet less than half (41 percent) had established security countermeasures for Internet of Things systems.”* (Britt, 2016; Facilitiesnet.com, 2015)

Contemporary IoT products are made to be readily available for consumers but not well secured to protect the privacy and security of the end consumers. It is ironic that the same devices/ things created to make consumers' lives easy are the ones posing a significant level of risk to their privacy, security, and wellbeing (Britt, 2016). There are four classifications by which IoT violates consumers' privacy (Al-Shakhouri & Mahmood, 2009):

#### *Unauthorized Data Acquisition*

This classification includes unauthorized access to the connected device of consumers and leading to the collection of private data and monitoring of Internet activities without the knowledge of consumers (Al-Shakhouri & Mahmood, 2009). For example, an unauthorized third party could hack an IoT network and gain access to personal data such as personal habits and health conditions.

#### *Unauthorized Access*

Unauthorized access involves the transfer of personal data about consumers without their consent (Al-Shakhouri & Mahmood, 2009). Many mobile applications today share our personal data with third party companies without sharing with us who are those end-users of data.

#### *Invasion of Consumer Privacy*

Consumer private information is illegally transferred to an unauthorized second party without the consent of the individual consumer. For example, when a mobile application developer shares their client personal details with other parties without the end-users' knowledge or authorization.

#### *Unauthorized Data Storage*

As mentioned before, Gartner expects most, if not all, IoT consumer data to be stored in the cloud by 2020. This will lead to a significant risk to consumers if the data falls into the wrong

hands (Johnson, 2016). For example, poor security of remote data servers can put consumers' privacy at risk of being misused by hackers.

## *2.7 Examples of Privacy Legislations in the Digital Era*

The best way to ensure a privet-centric digital era is a close collaboration between public and privet groups to coordinated efforts and policy enforcements against illegal data access practices such as information fraud and network hacking (Al-Shakhouri & Mahmood, 2009).

Protection of customers' privacy can only be enforced via systematic regulatory approach. Technologies would help, but in order for companies to follow through and implement a privacy-enhancing tech solution or even framework, there has to be a binding policy in place to assure compliance by all IoT ecosystem partners and stakeholders.

Some examples of Governmental regulatory initiatives include:

- U.S Federal Trade Commission (FTC) plays a key role in encouraging digital players to adapt and implement acceptable privacy principles (Al-Shakhouri & Mahmood, 2009; FTC Staff Report, 2015a). For example, it promotes public and privet partnerships in privacy and security matters.
- The U.S. Department of Commerce (DOC) provides businesses with information, guidelines, and practices for effective implementation of privacy and security regulations.
- The Online Privacy Alliance (OPA) is a US group concerned with introducing and promoting practices which provide a trusted environment for the digital economy through the protection of personal privacy (Al-Shakhouri & Mahmood, 2009; Wang, *et al.*, 1998).

- In Canada, the Personal Information Protection and Electronic Document Act (PIPEDA) was implemented as of 2001. PIPEDA Act demands user consent in advance of the collection or disclosure of personal information (FTC Staff Report, 2015b).

From an international perspective, the Organisation for Economic Co-operation and Development (OECD) issued a basic privacy guideline on protecting personal data.

The basic principles within OECD are summarized in Table 4 (Office of the Privacy Commissioner of Canada, 2010; Al-Shakhouri & Mahmood, 2009):

Table 4: Summary of OECD's basic privacy principles(Al-Shakhouri & Mahmood, 2009).	
Principle	Description
Collection limitation	There should be a limit to the collection of personal data and any such data should be obtained by lawful and fair means.
Data quality	Collected personal data should be relevant, accurate and up-to-date.
Purpose specification	The purpose for which data is collected should be specified at the time of collection and serve an agreed-upon purpose.
Use limitation	Personal data should not be disclosed or used for other purposes.
Security safeguards	Personal data should be protected by reasonable security measures against risks.
Openness	There should be a general policy of openness about the development, practices, and policies concerning personal data.
Individual participation	Individuals have the right to access and control their information.
Accountability	Data collectors should be accountable for complying with principles measures.

**Table 4 – Summary of OECD's basic privacy principles**

(Al-Shakhouri & Mahmood, 2009)

## 2.8 Privacy by Design Is an IoT Must

The design, enforcement, and adoption of a sustainable privacy framework, also known as Privacy by Design (PbD), are widely considered to be a key remedy and a viable solution to

protect the privacy and security of IoT users, whether for an individual user or an organization with IoT deployments (Coraggio, 2015b).

The IoT applications and systems raise vital concerns and introduce various new challenges for the privacy and security of end-users, corporations, networks, and business applications. For example, some IoT applications are closely linked to sensitive civil infrastructures of strategic nature such as energy and water distribution.

There are as well various applications that deal with sensitive people information such as their social insurance numbers, geolocations, or even their historical purchases and shopping preferences. Trust in and adoption of the various IoT applications will rely heavily on the privacy and security it affords to end-users and the effectiveness of security levels it guarantees to the network infrastructure (Akyildiz, Challal, Natalizio, Sen, & Vegni, 2014).

## Chapter Three – Privacy by Design

### 3.0 What is Privacy by Design?

The term “privacy by design” (PbD) was created by Dr. Ann Cavoukian, three-term Privacy Commissioner of Ontario, as a group of seven building principles to assure privacy and data protection are embedded in the design of computer software and computer systems (Cavoukian, 2011b). PbD has been translated into 38 languages and thus granting it a global respect and presence (Cavoukian, 2011b). The goal of PbD is to encourage software designers and technology organizations to follow through and fulfill their obligations towards protecting the privacy and security of their customers from the early stages of design of any project and throughout the service and product lifecycle.

*“PbD is predicated on the idea that, at the outset, technology is inherently neutral. As much as it can be used to chip away at privacy, it can also be enlisted to protect privacy. The same is true of processes and physical infrastructure.”(Information and Privacy Commissioner of Ontario, 2016)*

PbD shifts organizations’ attention towards putting the privacy of users as the top of mind prior to releasing any product or solution in the marketplace. PbD is a progressive and comprehensive thinking about maintaining the privacy for the IoT world. PbD is very useful to sustain end-users’ privacy especially that many IoT products are designed and released quickly in the market even if they do not meet proper security measures.

The privacy by design thinking process was pioneered to ensure safe and private software and hardware technology applications. It was clear that ensuring the privacy of any technological

system has to encompass the IT systems, the business practices and processes, and the physical design and network infrastructure (Cavoukian, 2011b).

### *3.1 Privacy by Design 7 Founding Principles*

#### *Principle # 1: Proactive not Reactive; Preventive not Remedial*

Privacy by Design (PbD) methodology is meant to be proactive rather than reactive. Professionals who apply PbD anticipate privacy threats and make sure they do not happen. “*Privacy by Design comes before-the-fact, not after.*” (Cavoukian, 2011, p.6)

#### *Principle # 2: Privacy as the Default Setting*

Privacy should be the default to ensure the automatic full protection of personal data in any given IT system or business practice (Cavoukian, 2011, p.6). The idea is for organizations, business leaders, and service providers to assume full responsibility of protecting consumers’ privacy. Consumers are not supposed to worry about their privacy in a system that embeds privacy in the early stages of its design.

#### *Principle # 3: Privacy Embedded into Design*

PbD is expected to be embedded into the early stages of system design and architecture. “*Therefore, privacy becomes an essential component of the core functionality being delivered*” (Cavoukian, 2011, p.6).

#### *Principle # 4: Full Functionality – Positive-Sum, not Zero-Sum*

Protecting the privacy of users by system designers and architects is supposed to be a positive-sum “win-win” situation. In a positive-sum situation, both parties win and no trade-offs are made. “*Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.*” (Cavoukian, 2011, p.6)

### *Principle # 5: End-to-End Security – Full Lifecycle Protection*

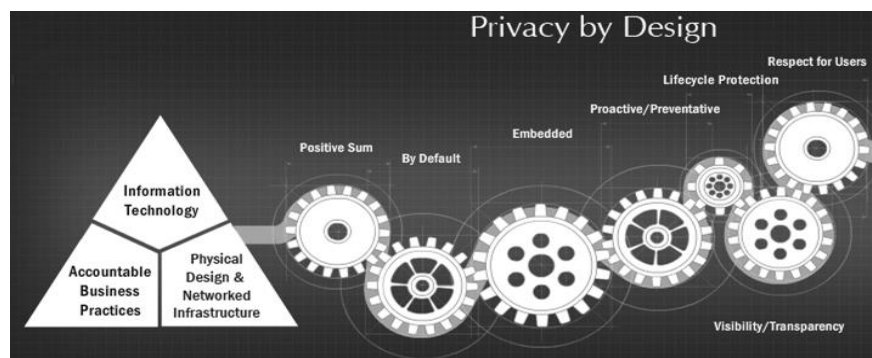
In an end-to-end full lifecycle PbD implementation, no information is being collected without ensuring top privacy and security measures from start to finish. The goal is for consumers' private data to be securely retained, and then securely destroyed at the end of the service, all in a timely manner (Cavoukian, 2011, p.6).

### *Principle # 6: Visibility and Transparency – Keep it Open*

PbD practices, promises, and measures are subject to independent verification to assure full compliance and delivery of security and privacy protection measures. It represents the well-known saying in negotiation, “*trust but verify*” (Cavoukian, 2011, p.6).

### *Principle # 7: Respect for User Privacy – Keep it User-Centric*

PbD is a user-centric methodology. Protecting the privacy of an individual proceeds protecting the privacy of a group (Cavoukian, 2011, p.6).



**Figure 10 – Privacy by Design 7 Founding Principles, overview**

(Cavoukian, 2011a)

With all being said, Privacy by design (PbD) is a systematic process concerned with protecting end users' privacy, security, and freedom of choice regarding when, how, and who has access to their personal information and data. To put it in a simple and easy to comprehend way, PbD means to incorporate comprehensive privacy into any object at the start of its design and production process. PbD advocates privacy assessment for new technology innovations and



services through the creation of internal systems to ensure that vendors and system designers put privacy as a top of mind concern all the time while thinking of new devices and services. System designers are encouraged to initiate privacy-protection mechanisms which are honed by employee and end-user privacy awareness training and best practices.

The first principle stresses the importance of preventing a breach of privacy accidents before they ever happen. The second principle accentuates the need for end users to be worry-free about their personal privacy in today's digital world. The third principle calls for implementing privacy into the early stages of any IT system or device process. The fourth principle expects privacy to improve an IT system design and functionality instead of weakening it. The fifth principle is highly important in today's shared economy since it emphasizes the protection of end-user data throughout the tool or system lifecycle, i.e. from collection to destruction. The six principle aims to empower end users with the power to command and control their personal data and information. Thus, in this principle end users have the right to know who has access to their data and how their data is being stored and used. The seventh and last principle calls for the respect of end user's privacy and keeping it user-centric. This means that privacy has to be top of mind for all stakeholders involved in an IT system design and production process every time and all the times (Kolkowska & Kristofferson, 2016).

### *3.2 Benefits of PbD*

There are four key benefits to embedding privacy in the early stages of designing IT system, solutions, and services:

- Privacy risks are easily identified at an early stage. Therefore, minimizing the cost of addressing them while eliminating or at least reducing the cost of privacy and security breach (ico.org.uk, 2016; Vael, 2015).
- Raising the awareness degree of privacy and information protection across all stakeholders (ico.org.uk, 2016; Vael, 2015).
- PbD ensures that system developers, designers, and architects follow through on their promises while assuming a full legal obligation towards protecting consumers' privacy (ico.org.uk, 2016; Vael, 2015). PbD aims to pre-emptively minimize the negative effects on individuals of any potential security and data breaches (ico.org.uk, 2016; Vael, 2015).

### *3.3 Extending PbD Founding Principles*

A key question to ask is whether PbD seven principles apply in the age of IoT or not? The answer to this question begins with knowing that PbD principles do in fact inspire IoT vendors and designers to assure that their IoT applications are safe, useful, transparent, and most importantly trustworthy in protecting end users' privacy (Cavoukian & Popa, 2016). An extension to the seven foundational principles of PbD was needed to assure privacy is integrated into a solid framework for IoTs.

IoT privacy first principle urges IoT designer and vendors to expect and work on eliminating any potential for privacy abuse. For example, the expected value of using an electric kettle or an oven with no intelligence or data collection and transmission capabilities, should always be weighed against future upgraded versions that offer the convenience of employing data collection and transmission capabilities with potential for such data to be misused if it is not securely protected by vendors. Consumers do not think about their privacy when they try to heat

a cup of water or prepare dinner. Though, future connected appliances can pose threats to users' privacy if the data it collects falls into the wrong hands (Cavoukian & Popa, 2016).

The second IoT privacy principle calls for vendors to deploy privacy configuration as the default for their devices and smart objects. Therefore, built-in strong privacy features are necessary to build good will needed for product adoption and safe of use. Customers will lean toward adopting and using IoTs that assures their privacy and protect their data (Cavoukian & Popa, 2016).

In the third IoT privacy principle, vendors and smart system designers need to build integrity into their design. Hence, privacy becomes a matter of moral principle rather than industry pressure or market demand. In an IoT proliferated world, customers will do business with companies whom they know have privacy as a key pillar in their mission statement and business philosophy (Cavoukian & Popa, 2016).

IoT privacy-inspired forth PbD concept calls for enhanced privacy experiences to include all smart devices to foster trust among IoTs stakeholders. Therefore, IoT users should not choose between their privacy or accept big brother monitoring and surveillance in exchange for security. This is definitely not positive sum equation. Hence, IoTs need to be safe and secure and enjoy a high level of rich functionality to improve user's experience while keeping the end-user and the community safe (Cavoukian & Popa, 2016).

The fifth IoT privacy-inspired PbD principle demands the designers and vendors of IoTs to clarify and simplify the smart devices' protection design. As a result, rigid implementation of end-to-end security measure, which guarantees end-user privacy and security throughout the IoT lifecycle, has to be easy to comprehend by end users. What is important to keep in mind is that

complexity in any design is an enemy to its usability. IoTs lead with a simple end-user benefit message which is clearly articulated by the designers and meant to be easily comprehended by end-users. Therefore, vendors need to deliver their privacy and security measures in IoTs in a simple and effective way to earn end-users trust (Cavoukian & Popa, 2016).

The sixth IoT privacy concept advocates for IoTs developers and designers to ensure privacy models which increase privacy awareness while encouraging responsible use of data by vendors to protect and strengthen the relationship between end-users and IoT vendors. Accordingly, this adjusted principle stresses the importance of differentiating between defensive monitoring of end-users and cunning and unneeded surveillance (Cavoukian & Popa, 2016).

The last and the seventh IoT PbD inspired concept calls for including end-users of IoTs as stakeholders rather than victims of IoT security breaches. Every user of an IoT system is a data-generating node, and respecting their privacy is critical for adoption and success of the entire IoT space and industry. As a result and in order to gain public trust as a measurable gain, it is crucial to consider users as key stakeholders, not as victims (Cavoukian & Popa, 2016).

Privacy by Design Foundational Principles	Extended PbD Principles for the IoT Era
1. Proactive not Reactive; Preventative not Remedial	Anticipate and Eliminate Opportunities for Abuse
2. Privacy as the Default Setting	Configure Privacy by Default
3. Privacy Embedded into Design	Embed Integrity into Design
4. Full Functionality – Positive-Sum, not Zero-Sum	Fuse Optimized Experiences to Full Functionality
5. End-to-End Security – Full Lifecycle Protection	Clarify & Simplify for Protective Design
6. Visibility and Transparency – Keep it Open	Control Monitoring and Awareness
7. Respect for User Privacy – Keep it User-Centric	Include Users as Stakeholders, not Victims

**Table 5- Extending PbD 7 Founding Principles for the IoT era**

(Cavoukian & Popa, 2016, p.6-9; Cavoukian, 2011, p.9)

### *3.4 IoT Security Design Challenges*

The internet of things faces some security design challenges that needed to be addressed to maximize its economic potential and value. Security issues began while designing and building IoT connected devices and systems (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016; Vael, 2015). For example, most connected devices are built by start-ups and early-stage ventures. Their main concern is getting their smart and connected products to the market as early as possible to generate sufficient revenue to fuel their growth. Therefore, most current IoTs lack proper security measures (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016). Another key design-related security and privacy issue with IoTs is the fact that complex, full-scale, and advanced security measures require strong computing capabilities which need sufficient computing memory. Yet, most current IoT devices and systems are unable to support complex and evolving security algorithms. With that being said, some of the key physical constraints with the compact design of current IoTs are:

- Inadequate built-in security measures
- Poor processing capabilities are unable to support complex security algorithms and encryptions
- *“Low CPU cycles vs. effective encryption”* (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016)

Another design-related privacy issue in current IoTs is that connected devices are designed to function autonomously in the field with no backup connectivity in case the primary

connection is lost. Consequently, hackers are able to attack such field-stationed IoTs and even take it out of service or use it as a bridge to attack the entire IoT network architecture (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016). The value of IoT comes from its ability to connect with other smart devices and data nodes to form the IoT network. This prolongs the onboarding process and allows hackers to attack IoT while the network is still not mature or well protected (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

Another design-inherited security and privacy issue with IoTs is that it requires ongoing security and remote management during and after onboarding. Unfortunately, this process is both costly and requires resources and commitment for the IoT system to scale its security parameters to accommodate the growth of the IoT network (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

Since IoT devices are expected to reach 50 billion by 2020, maintaining its security and privacy is both challenging and hard using conventional security measures that try to implement security and privacy as an afterthought process (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

Another challenge comes from the difficulty in properly defining and managing the various types of endpoints (Connected Things) in a scalable manner (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016). For example, in an IoT system, there are both individual endpoints such as a Nest (smart thermostat), and a group of endpoints which are connected together such as a group of smart light bulbs in a home or a factory. This represents a challenge in scaling security to be flexible enough to fit a limited number of IoTs and to be scalable to accommodate a growing group of connected things. Thus, some security experts recognize that the location of

the connected device is as important as the individual identifier (ID) in securing the network (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

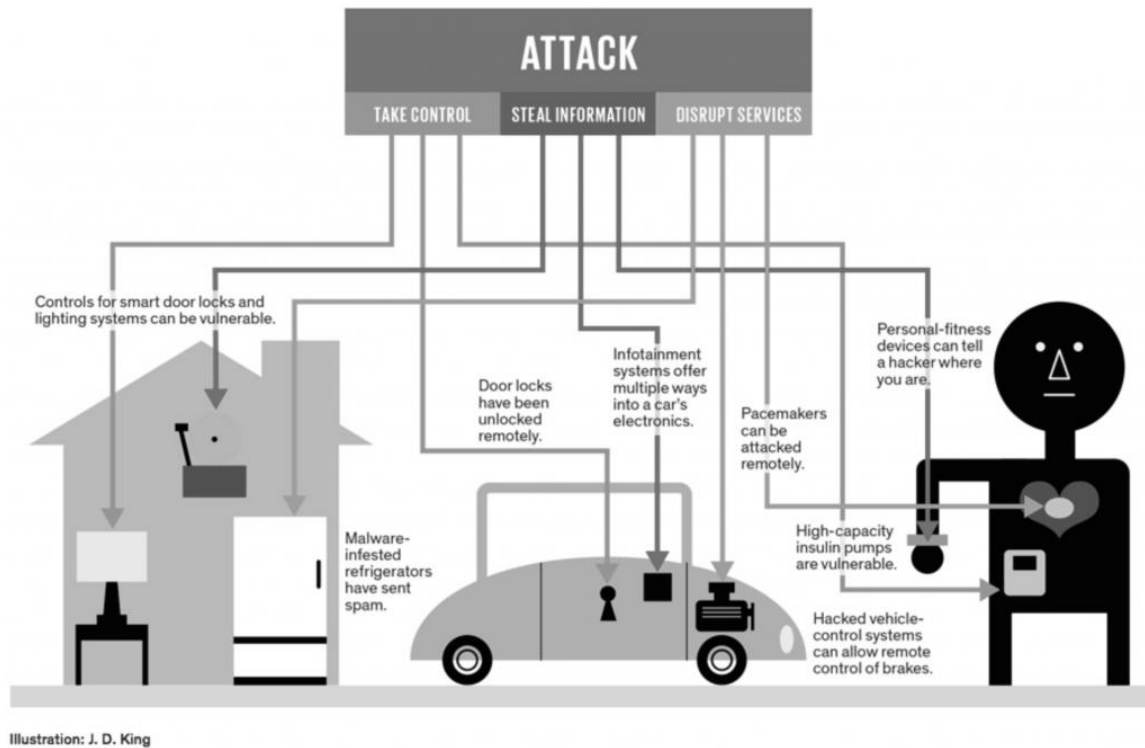
Another key challenge in securing IoTs is the management of multi-party networks where there are several stakeholders who share ownership of the network of connected things. Let us take the case of smart traffic lights (STL). STLs has several stakeholders such as emergency services as a key user, the local municipality as the primary owner, and the actual manufacturer which is the STL vendor (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016). The two questions that need to be addressed while securing STLs are (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016):

- “*Who has provisioning access?*”
- “*Who accepts Liability?*”

IoTs need to be easily encrypted throughout its lifetime. Another key challenge arises from the difference in the life of service expectancy between the connected device, which might remain in service for tens of years (smart meters are designed to serve for a period of 40 years), and the encryption algorithms, which could be cracked by a skilled hacker in a very short period of time. The result is a factual challenge that “*embedded devices may outlive algorithm lifetime.*” (Aurora, 2012; Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016)

Finally, IoTs require a digital protection against hackers and a physical protection against burglars, thieves, and intruders (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016). For example, connected devices could be stolen or simply taken off the network. Because of the nature of connected devices, being always on and always connected, they require constant protection against tampering (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

Hence, there is an urging need to properly secure IoTs based on a sustainable process which embeds privacy and security in the early design of the connected things and its system architecture.



**Figure 11- An illustration to demonstrate the top 10 challenges of securing IoT communications**

(Pandhi & Hanson, 2015)

### 3.5 Why is PbD Important for the Future of IoT?

*“Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of voice recognition.”*(Hern, 2015)

This warning by Samsung Electronics comes from the user agreement associated with its 2015 smart TV, capable of transmitting personal sensitive data about end-users to third party



companies. The data generated, collected and transmitted by the IoT could potentially pose many risks for the end users. For example, our homes which are filled with connected devices, such as smart meters, smart thermostats, smart TVs, and Tablets, could lose their appeal as private and personal sanctuaries and become besieged with smart devices which reveal our personal lives to the internet with unauthorized personnel or organizations. Clearly, there is a pressing need to propose a systematic framework to assure end-user data privacy. Such privacy-centric approach needs to involve all stakeholders involved in the development, manufacturing, implementing, and supporting of IoT applications, networks, and systems (Wessing, 2015). Humans are approaching an era where everything is connected; the personal data it collects is transmitted in real time and stored in the cloud on the third party servers. It would be very hard for all manufacturers around the globe to assure the privacy and security of its customers while adhering to the various privacy policies across multiple regions and jurisdictions (Valerio, 2014; Wessing, 2015; Zanolli, 2015). Thus, a systematic privacy-centric framework has to be embedded in the design and manufacturing thinking of all IoTs.

While the IoT applications and industry move from early stages to maturity, the IoT industry needs to implement a systematic and sustainable framework to assure proper protection, security, and privacy of its users and all stakeholders. The framework needs to be effective, simple and practical enough for all IoT stakeholders to adopt and invest in its longevity and success.

*“Now is the time to implement universally accepted guiding privacy principles that will effectively and elegantly spearhead consumer-centric design for the next few decades”.* Ann Cavoukian – three-term Privacy Commissioner of Ontario, (Cavoukian & Popa, 2016, p.9)

How can IoT developers and vendors assure a private and safe use of the various IoT applications? What would a privacy-centric design look like? How can they secure data privacy starting with the source? The future of IoT hinges on properly and effectively addressing the security challenges associated with collecting and transmitting of highly personal data.

## **Chapter Four – The Future of embedding Privacy by Design in IoT Applications**

### *4.0 How will IoT Change the Future of Cybersecurity*

*“We’re at an inflection point in technology history; the (IoT) now penetrates to the edge of the physical world and brings an important new physical element to security concerns. This is especially true as billions of things begin transporting data “somewhere.”* - Earl Perkins, research vice president at Gartner (Pemberton Levy, 2015)

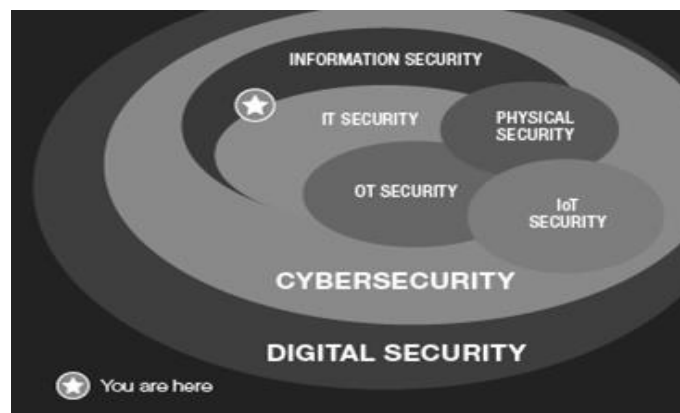
IoT applications will tremendously shape the future of our businesses, governments, and our personal lives. IoT is changing the way humans live, play, and even conduct businesses. Startups are adding new connected things (IoTs) on a daily basis so as the cyber threats of the new connected world.

The strengths and the potential threats of IoT reside in its ability to sense, transmit, analyze the vast amount of highly personal, community, and national level data that bridges both the physical and digital worlds. Thus, IoTs are able of providing the big data and insights field a whole new meaning with granular details about daily usage, habits, and patterns that can allow data scientists to model the data and predict future actions based on historical habits. The ease of data collection, transmission, and connection in the IoT era makes our society highly vulnerable to targeted and vicious cyber-attacks (Allan, 2015, p.13).

To understand the magnitude of IoT on the cyber security world, Gartner published a blog in 2015 to help security professionals visualize the relationship between the individual user of IoT and the entire security universe (Pemberton Levy, 2015).

As developers of the “Connected Things” create and assemble ever smaller connected applications, individual users of IoT assume a far greater important role in assuring that organizations maintain their security and protect their privacy in the new digital universe (Pemberton Levy, 2015).

The new world is an interconnected universe of IoTs which are able to identify themselves and connect to its surrounding “Smart Objects” while exchanging a real-time stream of insights. Citizens of the digital era are witnessing a world of ever-growing smart connected devices creating a gigantic information system universe. The scary part about this connected universe of IoT is that 70 percent of them contain serious inherited vulnerabilities as part of their built-in initial design (BARAJAS, 2014).



**Figure 12 - Understand your role in the digital security universe**

(Gartner.com/SmarterWithGartner; (Pemberton Levy, 2015)

*“There is undeniable evidence that our dependence on interconnected technology is defeating our ability to secure it.” (BARAJAS, 2014)*

According to The Open Web Application Security Project (OWASP), some of the more pressing security concerns with IoT today include Insecure web interface, lack of transport encryption, poor physical security, and insecure cloud interface to name a few.

The list below contains the top ten security problems associated with the IoT era.

<b>Top 10 security problems with IoT today</b>
1. Insecure Web interface
2. Insufficient authentication or authorization
3. Insecure network services
4. Lack of transport encryption
5. Privacy Concerns
6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configuration
9. Insecure software or firmware
10. Poor physical security

**Table 6 - Top 10 Security Threats in IoT today**

(BARAJAS, 2014)

As more of the objects consumers interact with on a daily basis become “smart”, it becomes necessary that security experts, privacy advocates, and legislators implement an effective and sustainable framework to assure built-in privacy and security in all IoT devices. This list was advocated by The Open Web Application Security Project (OWASP) to educate users on the key aspects of IoT security and encourage IoT developers and vendors to make their products more secure (BARAJAS, 2014; OWASP.org, 2016).

It is clear, from the list above, that IoT fueled the possibilities of cyber-attacks and therefore, it becomes important to implement a proactive rather than reactive defense mechanism that can be adopted as a guiding framework for IoT developers worldwide (West, 2015).

#### *4.1 The Future of IoT Depends on Implementing Proper Security Measures*

*“In a business of 263,000 million dollars in revenue and more than 25 billion devices connected by 2020, cybersecurity is a priority.”(Cía, 2015)*

There is a serious concern that IoT vendors will, and potentially already do, share the vast amount of highly personal data and consumer insights they gathered from smart wearables, mobile applications, and even social networks with third party companies in a big-data-black-market of consumer information (Cía, 2015). Even if IoT vendors are not selling or at least sharing consumers' data with third-party data vendors, online data available in the cloud can present a gold mine for hackers who are eager to exploit such sensitive data for their own personal benefit. These facts add extra pressure on IoT developers to invest in securing IoTs. In a recent Gartner report, IoT connected devices and service vendors will generate more than \$300 billion in incremental revenue, mostly in IoT-ecosystem services, by the year 2020 (Middleton, Kjeldsen, & Tully, 2013). Such growth potential should encourage vendors to invest in privacy.

The future is increasingly connected and the journey to the global mass proliferation of IoTs is accelerating the cyber-privacy and cyber security challenges globally. Therefore, poor privacy and security measures could significantly undermine the users' trust in all IoT-related products and services. Poor IoT security and privacy measures affect both users and organizations alike. In fact, the damage of a privacy and security breach could cost businesses significant financial and reputational losses and could be hard to rectify (HOWARTH, 2015).

Consider the example of the security breach of the famous US-retailer Target Corporation in 2013. The attack was considered to be one of the largest data security breaches in the US-retail history and resulted in the loss of over 40 million consumer credit card information.

*“What shocked security experts while investigating the attack is that the hackers gained access to Target’s information system infrastructure through Internet-enabled heating, ventilation and air-conditioning systems installed in its retail outlets”*

The future of IoT’s success and growth hinges on improving its security and privacy measures (Capgemini Consulting IoT Security Report, 2014). A recent Capgemini report concluded that 71% of the surveyed customers agreed that security and privacy concerns will influence their decision to purchase or use an IoT product or service (Capgemini Consulting IoT Security Report, 2014,p.4). Going back to the Target example, the retailer saw a 46% drop in its profitability as a direct result of the IoT security breach.

That was a devastating attack on Target Corp. and partially contributed to the US retailer leaving the Canadian market in 2015. Target issues did not stop here, the US retailer is facing a potential fine ranging from \$400 to over \$1 billion US dollars in case the government investigators concludes that Target did not take the necessary steps to embedding proper security and privacy measures to its IT and IoT infrastructure (Capgemini Consulting IoT Security Report, 2014,p.4).

It is clear that improving privacy and security measures within IoT systems and devices is no longer an option, it is the only way for the industry to succeed in earning end-users’ trust.

Privacy as a core pillar of the IoT design is an effective and practical way to mitigate security risks. Therefore, privacy and security need to be planned for and deployed throughout the totality of the service or product lifecycle (FTC Staff Report, 2015b; MCSWEENY, 2015)

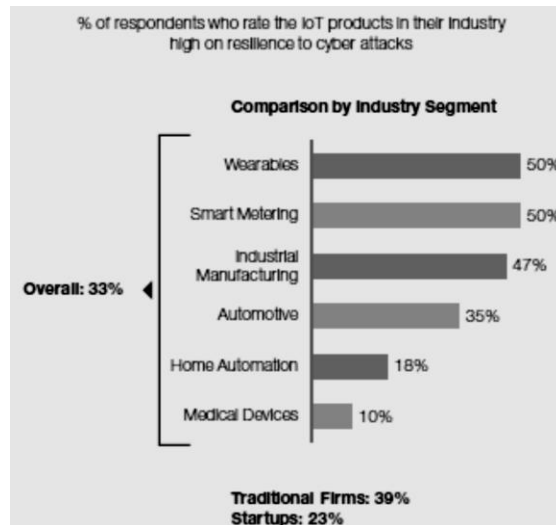
#### *4.2 Why PbD is Essential to the Users of IoT*

*“Even though we have seen a consistent rise in security and privacy threats, especially within IoT-enabled devices and systems, the majority of organizations are still lagging in taking the proper privacy and security measures to protect their Connected Things”* (Capgemini Consulting IoT Security Report, 2014, p.5).

In a recent 2014 Capgemini survey, only 33% of business executives believe that the IoT products in their industry are highly resilient to cyber security attacks (Capgemini Consulting IoT Security Report, 2014,p.5).

It is clear that current security and privacy measures within IoTs are not sufficient. 89% of consumers avoid conducting business with companies who fail to protect their privacy and security (Privacy Risk Summit Preview by Truste, 2016). IoTs of today lack proper encryption while communicating among themselves and with the servers they send users’ information and data to for further analysis (FTC Staff Report, 2015, p.10-13).





**Figure 13 - % of business executive respondents who rate IoT products in their industry high on resilience to cyber-attacks**

(Capgemini Consulting IoT Security Report, 2014, p.5)

*“An HP study revealed 250 vulnerabilities in ten commonly used IoT devices, including connected TVs, webcams, thermostats, door locks and home alarms. Most products supported very weak authentication features that directly exposed them to security risks. In fact, 8 out of 10 devices failed to require a password stronger than 1234.”*(Capgemini Consulting IoT Security

Report, 2014,p.5)

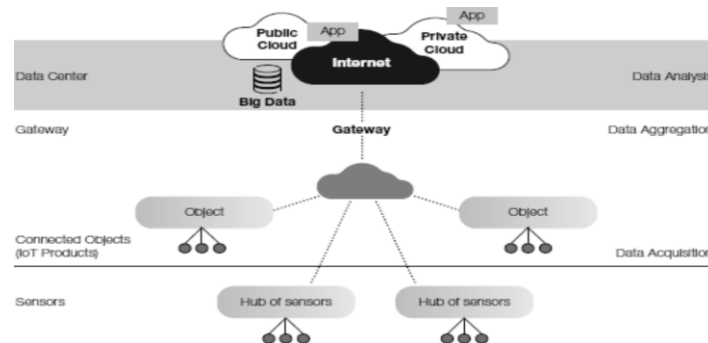
Target Corporation thought it was prepared to meet the security and privacy challenges of today’s connected world. Many companies such as Walmart, Neiman Marcus, and The Home

Depot thought, like Target, they are protected and well prepared for today’s privacy risks, but times proved them wrong (West, 2015; Snyder, 2014). Hence, the proactive defense is the answer and it requires a fundamental shift in privacy and security thinking; privacy needs to be embedded in the early design thinking and maintained throughout the product or service lifecycle. Privacy by Design (PbD) is undoubtedly a differentiating advantage for a modern

company who seeks to maintain a strong positioning in today's highly competitive market (West, 2015).

In an ever-growing universe of “Connected Devices”, maintaining a standardized level of security and privacy measures for all smart devices no matter where they are and who made them is a big challenge. Thus, a security breach in one single component of the IoT network could impact the security and privacy of the entire network. Therefore, it might be difficult to rely on the degree of integrity of every connected device globally. That said, the security of the whole system is potentially vulnerable due to the lack of proper privacy and security measures within any of its components or members (O'Connor, 2015).

In the figure below, it is evident how hard it is to maintain the security of IoT devices given the expanded attack surface of an IoT system (Capgemini Consulting IoT Security Report, 2014).



**Figure 14 - The Expanded Attack Surface of an IoT System**

(Capgemini Consulting IoT Security Report, 2014, p.7).

A big problem with today's privacy policies is that they lack the maturity to deal with our fast-paced digital economy and digital universe. IoT developers and vendors are accused of not taking enough steps to secure their IoT products and services. It is no wonder that many of those organizations are prone to hackers' attacks, poor IoT security development processes, and

reduced security measures starting at the architecture level of the IoT design (Capgemini Consulting IoT Security Report, 2014,p.7).

*“The focus on security can get lost if organizations rush to launch their IoT products, prioritizing speed-to-market over security.”*(Capgemini Consulting IoT Security Report, 2014)

Security, privacy advocates, as well as IoT end-users, need to make sure that privacy and security are the core focus of the IoT system development process for IoT to reach its full potential and global adoption. The importance of embedding PbD within IoT systems and products could be summarized in the following ten points (Solove, 2014):

*1. PbD limits the powers of unauthorized personal and organizations*

Information is power and the more someone knows about the end-users, the more power he/she has over them.

*2. PbD enables a culture of respecting the privacy of individuals*

People have the right to protect their privacy and they don't need to worry about it every time they use an IoT service or product. Their privacy needs to be top of mind for any IoT vendor or service provider.

*3. PbD empowers the preservation of someone's reputation in today's digital economy*

Humanity today lives in a connected world in which it does not have full control over its own digital reputation. Therefore, it is empirical for IoT vendors to take the proper measures to preserve someone's digital reputation upon using their connected products or services.

*4. PbD spreads a culture of trust in our modern democratic socio-political system*

Breaching confidentiality erodes trust within society. Therefore, healthy business and personal and professional relationships require privacy to maintain the trust bond as a key principle in our modern social contract.

5. *PbD is a great framework to uphold appropriate social boundaries among society members*

People have different levels of privacy depending on who they interact with. Thus, maintaining their privacy is a key to sustaining different social and professional boundaries.

6. *PbD assures the protection of individual's right to have full control over his/her life*

Our personal data has vast effects on our lives, starting with someone's ability to get a loan, to someone's professional reputation. Hence, PbD gives end users the power of knowledge of who has access to their data, what is the context, and how the data is being used.

7. *PbD is key for maintaining our right to freedom of speech*

An observant with eyes on everything that is being said, done, liked, explored, or even associated with, could deter the foundations of our society. Security should not contradict privacy and as late Benjamin Franklin said, "*Those who are willing to forfeit liberty for security will have neither.*"

8. *PbD is aligned with protecting our social and political freedom*

In our civil and democratic society, citizens have the right to associate with whoever they want both socially and politically. People should not worry about the privacy of their political choice on the election ballot especially while following their deep conscience.

*9. PbD can allow people the basic right to change and have a second chance*

Humans all make mistakes and they do learn from them and can change. The world is dynamic and there is nothing static in this life including peoples' actions, beliefs, and behaviors. PbD nurtures this fantastic opportunity in life to improve and be a better person than who they used to be yesterday.

*10. PbD allows the individual to act without having to explain or justify his or her actions to everyone who might question their action or behavior*

During daily routines, people do many activities, say things, listen to music, like stuff, follow trends, and so on. If judged from a distance by others observing them who lack the full picture, knowledge, and understanding of their particular situation, their actions and behaviors may seem peculiar or even embarrassing if not completely devastating. People have the right to protect their own personal life without worrying and fearing of a big brother watching over them all the time (Solove, 2014).

There are three key liabilities and risks that PbD can minimize in the IoT space:

- *PbD allows organizations to mitigate risks associated with global IoT applications and devices.* Not all IoTs are compliant with all global and regional privacy laws. Thus, PbD can help create a privacy culture and framework that can be adopted on a global level (Coraggio, 2015a). *“PbD methodology is now required by both US authorities and European data protection regulators as it emphasizes the need to adopt PbD framework while building or deploying any connected device or connected system”* (Coraggio, 2015b).
- *PbD can significantly minimize the damages caused by cyber crimes.* For example, in the case of a data breach, the IoT vendor or service provider is obliged to report the security incident to local privacy authorities and regulators if he or she proved incapable of

implementing adequate security measures to protect users' privacy and security (Coraggio, 2015a).

- *PbD encourages IoT vendors to utilize anonymization techniques to protect users' identity and privacy.* Hence, reducing vendors' liabilities and risks of violating end users' privacy (Coraggio, 2015a).

#### *4.3 Challenges of Implementing Privacy and Security in IoT*

Creating standards is a challenging task by itself since it requires several groups to come together and collaborate to agree on a set of rules and guidelines. The challenge with IoT is much harder. The reality is in IoT any set of security standards must address the challenge of scalability (Grau, 2016). For example, "Connected Devices" range in their physical design from tiny, cost sensitive "Connected Things" that use mesh networking technologies and require minimal computational power, to large smart "Connected Things" that require complex computational capabilities and memory capacity such as smart grids, smart cars, and even industrial automation controllers. Hence, the security requirements of each differ significantly among these smart connected "Things" (Grau, 2016).

With close to 50 billion IoTs entering our global economy by 2020, it is extremely important for IoT researchers, vendors, and policymakers to agree on privacy and security standards and guiding principles that can govern the IoT space. As mentioned before, privacy and security are two of the top areas of concerns for potential IoT customers. End-users need to have the full confidence that the smart devices they use will maintain their privacy and assure their security (Grau, 2016; West, 2015). Below are three key points to keep in mind when considering the topic of security and privacy issues in IoT (Samani, 2014):

- *IoTs has multi-billion points of vulnerability*

With an estimated number of 50 billion “Connected Device” within the IoT universe by 2020, each device represents a potential point of vulnerability that hackers could exploit. Vulnerability at one single connected device could jeopardize the entire privacy and security of the IoT network (Samani, 2014).

- *IoT systems and universe lack trust and face poor data integrity*

It is really hard for organizations and end users to trust data transmitted and produced by remotely connected devices especially if there is no mechanism to assure that the data has not tampered with in any shape, way, or form. For example, some smart energy meters could be hacked into or fail to alter usage levels (Samani, 2014; Ward, 2014).

- *IoT users have plenty concerns regarding data collection, information protection, and personal privacy*

Any data breach, privacy, or security threat could undermine consumers’ trust in IoT. Connected devices bridge that gap between the digital and the physical worlds and consumers are concerned that their personal data could be easily exploited by criminals (Samani, 2014).

There are seven key threats to privacy in IoT systems and products (Ziegeldorf, Morchon, & Wehrle, 2013):

1. Identification
2. Tracking
3. Profiling

4. Interaction & Presentation
5. Lifecycle transition
6. Inventory attacks
7. Linkage

Table 7 is a summary of a few selected features that can have the highest impact on a particular threat (Ziegeldorf et al., 2013).

	Technology	Size	Interconnection	Data Collection	Thing Interaction	System Interaction	Lifecycle	Vertical vs. Horizontal
1. Identification	Camera, face recognition		Fingerprinting			Speech, cloud interfaces		
2. Tracking & Localization	Indoor LBS			Decreasing awareness		Data trails		
3. Profiling		Explosion of data sources		Qualitatively new sets of data				
4. Interaction & Presentation					Presentation media	Pervasive interaction with users		
5. Lifecycle transition				Product history log			Exchangeability	Sensitive data on devices
6. Inventory attacks	Diversification		Wireless communication					
7. Linkage				Decreasing transparency				Drives Linkage Locally

**Table 7 - Summary of the seven categories of privacy threats and their potential impact**

(Ziegeldorf et al., 2013, p.8).

### *Identification*

Identification threat happens when an IoT system or connected device reveal identifying pieces of information, such as person's name, address, and / or an alias of any kind, with a specific unauthorized person or entity thus jeopardizing the end-users' privacy (Ziegeldorf et al., 2013).



Such identification is a serious privacy threat because it opens the door for correlating a specific identity to a potentially specific privacy violating context. Thus, allowing threatening actions such as profiling and tracking of individuals while combining multiple data sources (Ziegeldorf et al., 2013, p.7).

### *Tracking & Localization*

Recording an IoTs user's location through time and space represents a key threat to privacy. Today, our society is facing continuous tracking of individual users through a variety of technologies such as GPS and real-time traffic mobile applications which are similar to Waze, mobile triangulating localization and tracking application. IoT users feel threatened and watched by big brother who tracks every single move they make. While localization can come with lots of benefits, such as helping police track missing or stolen cars, IoT users need to feel empowered by having control over their data. IoT users need to be able to track their move and if they can stop others from tracking them. Like identification, IoT users are worried about their personal data being used in an inappropriate context (Ziegeldorf et al., 2013, p.7-8).

### *Profiling*

Profiling is the process by which an organization or person gathers personal information about a specific person or a group of people to gain an advantage over him, her, or them through the formulation of insights and assumption based on previous historical behaviors and predictive analysis (Ziegeldorf et al., 2013). A great example of profiling is when customers get their personal page customized by an e-commerce site such as Amazon. The e-commerce site tracks our digital behavior and historical data and recommends product offerings which the artificial intelligence smart system thinks will appeal to us the most.

An example where profiling leads to a violation of consumer privacy is price discrimination. In price discrimination, customers are presented with different prices while trying to buy a flight ticket or shop for some items online. One last example of dangerous profiling is the famous social engineering scandal that Facebook did to its site users a few year ago (Chou & Edge, 2012; Ozimek, 2013). Facebook started to display different content to different people to direct and alter their mood. As a result of the Facebook experiment, some people were presented with negative and emotional information and Facebook monitored how such data feed changed the subjects' mood and statuses on their wall.

#### *Interaction & Presentation*

This threat is powered and carried on by IoT applications used in public places such as smart retail venues. In privacy violating interactions, an IoT system or device transmits private information through an unprotected / unsecured public medium, could result in divulging of personal information to unauthorized parties and audience (Ziegeldorf et al., 2013).

#### *Lifecycle transition*

Humans live in a dynamic world where IoT devices such as smart wearables could be sold from one person to another while carrying with them tons of valuable personal data and historical behaviors of previous owners. Therefore, and in such a scenario, the threat comes from the possession and access of personal data during transmission ownership spheres during the IoT device lifecycle. People who buy or sell used phones faced a situation where private and highly personal photos and videos were found on used cell phones (Ziegeldorf et al., 2013).

#### *Inventory attacks*

Inventory attacks involve a process of collecting data about the existence and characteristics of a specific person or their personal situations, events, or even things. An

example would be data collected by smart TVs or smart appliances that can be communicated and queried over the worldwide web. The primary risk of Inventory Attacks comes from unauthorized groups or people querying and manipulating such data for illegitimate purposes.

Inventory attacks allow hackers to have access to an IoT connected device's digital fingerprint allowing the attacker spy on the victims' conversations within the privacy of their personal vicinity (Ziegeldorf et al., 2013).

### *Linkage*

IoT is a great manifestation of the reputation economy. In the reputation economy, the third party can collect information from separated data sources and combine data to reach new and revealing insights about prospective groups or individuals. Newly formed insights or conclusions could either be true or false, depending on its context and situation. The most important thing in Linkage is that the user did not give their permission to others to collect, analyze, and then reach insights or conclusions about who they are and what their actions or behaviors could mean. This represents a significant threat to personal privacy in the IoT era. Personally, I dread poor judgment about me by others due to loss of context when my personal information is gathered from different sources and analyzed by others who do not have enough information about me, my situation, history, and background (Ziegeldorf et al., 2013, p.10-11).

There is no doubt that the IoT era is here to stay and opens limitless opportunities for new industries and consumers. If there is one industry able to alter the relationship between machine and man, it will be The Internet of Things (IoT). However, the new era comes with vast security and privacy risks which need to be mitigated and addressed to allow IoT reach its full potential. Embedding privacy and security in the early stages of the conception of IoT devices and systems is definitely the right way to secure, not just the users of IoT, but also the future of the industry

itself (Wessing, 2015). Securing IoT would need the collaboration of policy makers, academics, privacy and security experts, technology vendors, privacy advocates, and pretty much all stakeholders within the IoT universe (FTC Staff Report, 2015b).

#### *4.4 Road Map to Overcoming the Challenges of Implementing PbD in IoT*

When IoT privacy experts speak of privacy by design (PbD), they advocate protecting end user's privacy from the get-go and throughout the IoT product or system lifecycle. There has been a serious consideration on an international level to develop an industry standard privacy framework which embeds end user's privacy as a building block in product design and development. It is important to mention that the vision of Privacy by Design (PbD) is the idea of Dr. Ann Cavoukian, three-term Privacy Commissioner of Ontario, for Information and Privacy who is now the executive director of Privacy and Bid Data Institute at Ryerson University (Kenyon, 2015). We will attempt to propose a practical framework to a more secure IoT via PbD. Historically speaking, regulatory compliance has proved to be unsustainable. Thus, in order to make the protection of consumers' data private, we must think of privacy as the default setting (Cavoukian & Popa, 2016; Kenyon, 2015).

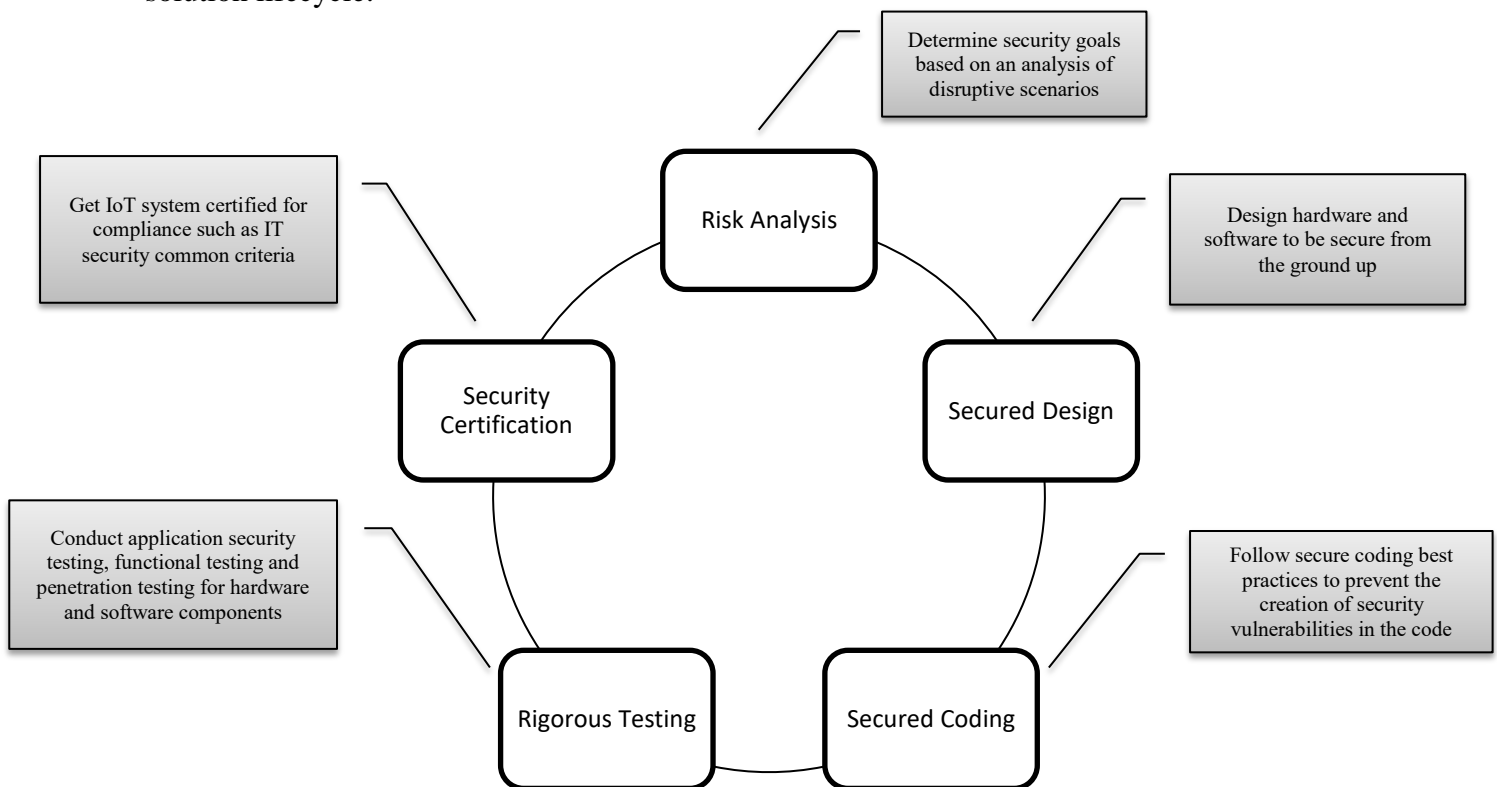
##### *Step One: Creation of Cross Functional Privacy & Security Task Force*

The first step in securing an IoT device or system is to consider its privacy and security as a core pillar of the value proposition it delivers to its end-users. This first step urges the different stakeholders, such as product development, security, marketing, PR, executive management, and engineering among others, to come together and collaborate to deliver a

roadmap with clearly defined next steps to embed security and privacy throughout the product or system lifecycle (Capgemini Consulting IoT Security Report, 2014, p.11).

### *Step Two: Embed Security with Early Product Development Stages*

A privacy and security risk analysis should happen while thinking of a product or system design. The full privacy audit should consider all privacy threats throughout the IoT product or solution lifecycle.



**Figure 15 - Revamp IoT Product Development Process to Address Privacy & Security Issues**

(Capgemini Consulting IoT Security Report, 2014)

Such early-stage analysis will gain lots of value and credibility if the team managed to include an analysis of the financial impact of any privacy or security threat. Quantifying the potential risks is considered a highly effective way for PbD to gain proper executive support from the vendor (Capgemini Consulting IoT Security Report, 2014, p.11).

### *Step Three: Secure the Product and System Design*

Security and privacy standards need to apply to both the software and the hardware component of an IoT system. Thus, comprehensive security testing needs to be applied to the entire IoT system. (Capgemini Consulting IoT Security Report, 2014, p.11).

### *Step Four: Secure the Intangibles; Securing the System Computer Code*

IoT's rely on information technology and digital codes to operate. Hence, security has to be implemented at the code level. IoT developers need to observe industry accepted security coding and privacy best practices while writing the initial IoT operating code (Capgemini Consulting IoT Security Report, 2014, p.11).

### *Step Five: Closing the Privacy & Security Loop by Performing a Security Evaluation Process*

Hackers find new ways to bypass security measures and break security codes daily. With that said in mind, IoT developers need to improve their privacy and security measures daily and involve the entire organization into becoming a privacy-centric learning organization (Earnest & Young Cybersecurity and IoT Report, 2015, p.11).

### *Step Six: Educate and Train End users on Security & Privacy Best Practices*

Training users is the most effective way to ensure sustainable privacy and security practice at the individual level.

### *Step Seven: Clarify Security & Privacy Policies with better Transparency*

The privacy and security policies of IoT systems and devices need to be easy to comprehend and read by the end users. This goes to include simplifying the language and all other nuances of written privacy and security policies (Privacy Risk Summit Preview by Truste, 2016).

#### *Step Eight: Minimize Data Collection*

It goes without saying that the more data an IoT system collects, the higher the privacy and security risk the end-user will face. It should come as no surprise that to ensure customers' privacy and security, IoT vendors should only collect data deemed to be highly relevant to the purposes for which consent was originally given by the end-user (Privacy Risk Summit Preview by Truste, 2016). Thus, if a piece of data is not mission-critical it shouldn't be collected.

#### *Step Nine: Secure Communication From and To the IoT Device & System*

Authentication and encryption are keys in IoT since most IoT devices operate remotely with little or no supervision. Hence, securing the communication network for IoT is essential for the security and privacy of the entire IoT network (Frahim Jazib, Pignataro Carlos, Apcar Jeff, 2016).

#### *Step Ten: Know the Environment in which the IoT will be used within*

IoT's are smart because they interact with their environment, and through situational awareness, they make sense of how their users utilize them on a daily basis. Accordingly, privacy has to have a deep level of situational analysis to comprehend the bigger scope of the threat landscape to prevent privacy and security attacks (Earnest & Young Cybersecurity and IoT Report, 2015, p.11).

#### *Step Eleven: Align Privacy & Security with Tangible Business Objectives*

Cyber security risks and challenges need to be addressed at the organization's broad level. Senior leadership needs to be aware of the quantifiable impact of poor security and privacy measures. Like any sustainable strategy, senior leadership commitment is a key pillar for it to succeed (Earnest & Young Cybersecurity and IoT Report, 2015, p.11).

*Step Twelve: Rethink Security from Considering it as a Cost Center to be Viewed as a Value Adding & Key Differentiator Center*

The privacy and security in an IoT device or system should not be looked at as a mandatory burden that the company has to spend resources to attain. Instead, it should be considered as a value-added process that hones consumers' trust in the brand and smart system (Earnest & Young Cybersecurity and IoT Report, 2015, p.12).

*Step Thirteen: Reassess Privacy & Security Measures throughout the IoT Product & Service Lifecycle*

This would be a comprehensive risk-based assessment approach to address privacy and security measures within IoT. In these 360 degrees assessments, organizations need to pursue a complete evaluation of the inventory of the numerous personal data it collects from and about its end-users. This will open the door for the thorough understanding of end-to-end information lifecycle flows of any personal data (Privacy Risk Summit Preview by Truste, rgiev 2016).

*Step Fourteen: Shift Focus from Product to People (End Users)*

Technological-based security and privacy measures have limitations, henceforth, it is absolutely important to address end-users' behavioral impact on maintaining the privacy and security of an IoT device or system. People have to be trained on using their smart and connected devices in a safe and secure way. For example, Gartner recently advocated a new people-centric privacy and security vision called, "*People-centric security*," which as it implies emphasizes the role of the individual user's accountability and trust over traditional defensive security measures (Firstbrook, 2015; Scholtz, 2015).

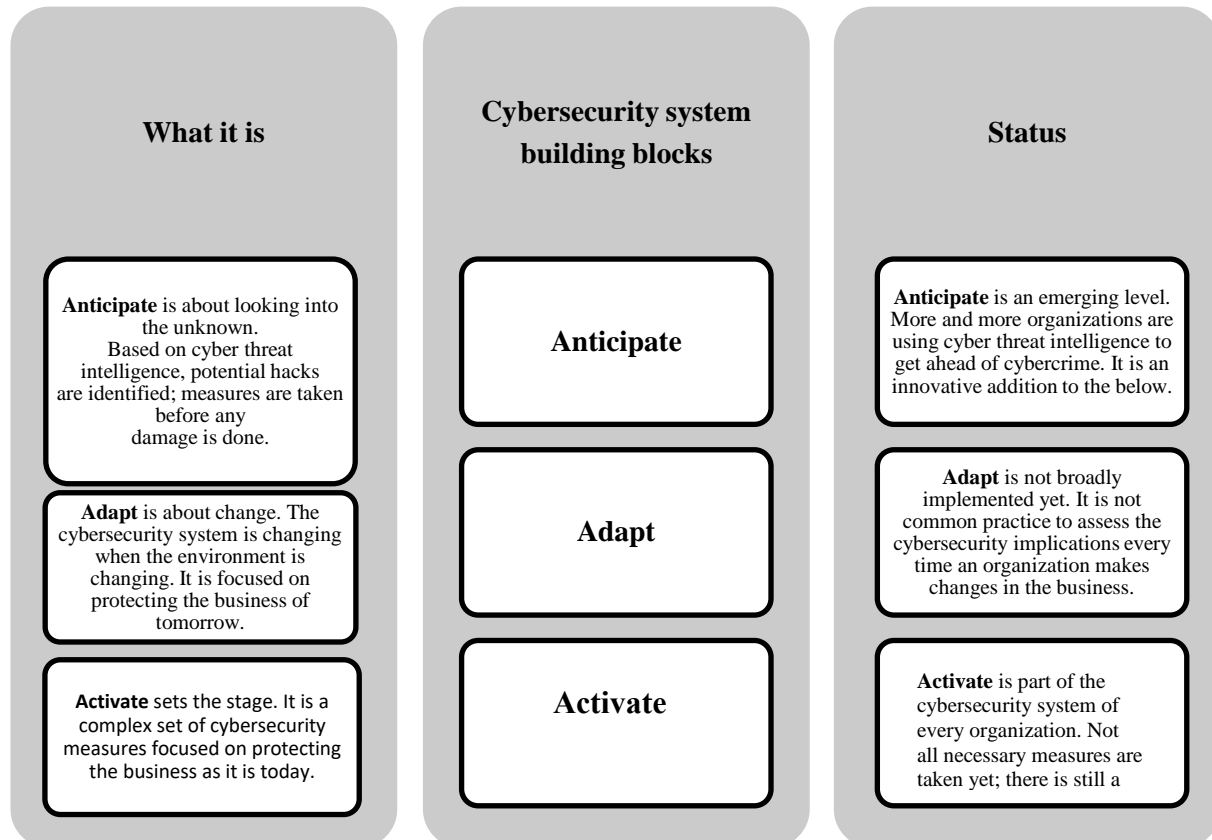




**Figure 16 - A Framework for People-Centric Security as proposed by Tom Scholtz from Garter**

(Scholtz, 2015)

*Step Fifteen: Triple A; Activate, Adapt, and Anticipate*



**Figure 17 - The Three Stages of Cybersecurity Maturity Responses — Activate, Adapt and Anticipate (the three As)**

(Earnest & Young Cybersecurity and IoT Report, 2015, p.12)

## *Conclusion*

This research paper aims to provide the non-technical reader a quick overview of the world of Internet of Things (IoT) and Privacy by Design. Throughout the four different chapters, it provided a snapshot of current security and privacy challenges associated with the proliferation of the IoTs and suggested a comprehensive fifteen step to rethinking privacy within the IoT space. Privacy by Design (PbD) is a breakthrough and a new way of thinking about privacy. The framework was proposed and developed by Dr. Ann Cavoukian, three-term Privacy Commissioner of Ontario, to protect the privacy of end users in today's digital age by embedding thoughtful privacy protective measures into the early stages of a system or device design within the world of information technology and corporate operations. Due to the potential of PbD in changing the way companies regard privacy, it was unanimously passed as an international framework for privacy and data protection in 2010 (CAVOUKIAN, 2015).

It is fundamental to keep in mind that as more smart devices and associated platforms and networks connect to the world wide web in real-time, it becomes a priority for all stakeholders to make sure that their participation in the IoT era bears the minimum amount of risk for their privacy and security. There is no doubt that the most successful IoT-era active contributors – programmers of the smart code, telecommunication providers, IoT devices vendors, research and development, policy makers and end users – will be those that put PbD as top of mind while thinking of the design and realization of the next big new smart "Connected Thing". Therefore, in order to keep pace with the lightning speed at which technology advances and the speed and creativity in which hackers find ways to threaten our security, and privacy, experts and advocates need to keep developing a PbD-centric framework to cover the products, systems, and infrastructure of today's connect world.

## References

- Akyildiz, I., Challal, Y., Natalizio, E., Sen, S., & Vegni, A. M. (2014). Special Issue on Internet of Things security and privacy: design methods, detection, prevention and countermeasures - Call for Papers - Elsevier. Retrieved from <http://www.journals.elsevier.com/ad-hoc-networks/call-for-papers/special-issue-on-internet-of-things-security-and-privacy>
- Allan, K. (2015). Cybersecurity and the Internet of Things Insights on governance, risk and compliance.
- Al-Shakhouri, N. S., & Mahmood, A. (2009). Privacy in the digital world: Towards international legislation. *First Monday*, 14(4).
- Aurora, V. (2012). Lifetimes of cryptographic hash functions. Retrieved from <http://valerieaurora.org/hash.html>
- BARAJAS, O. (2014). How the Internet of Things (IoT) Is Changing the Cybersecurity Landscape. Retrieved from <https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/>
- BBC. (2014). Edward Snowden: Leaks that exposed US spy programme. Retrieved from <http://www.bbc.com/news/world-us-canada-23123964>
- Bob Violino. (2013). What the Internet of Things means for security. Retrieved from <http://www.csoonline.com/article/2134066/mobile-security/what-the-internet-of-things-means-for-security.html>
- Bradbury, D. (2015). How can privacy survive in the era of the internet of things? | Technology | The Guardian. Retrieved from <https://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things>
- Brendan O'Brien. (2014). Why the "Internet of Things" Is Important. Retrieved from

<http://insights.wired.com/profiles/blogs/why-the-internet-of-things-is-important#axzz4E356LqS0>

Britt, P. (2016). IoT Security Begins with Risk Assessment. Retrieved from <http://www.esecurityplanet.com/network-security/iot-security-begins-with-risk-assessment.html>

businessdictionary.com. (2014). Definition of Privacy. Retrieved from <http://www.businessdictionary.com/definition/privacy.html>

Capgemini Consulting IoT Security Report. (2014). *Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT The Internet of Things Opportunity Hinges on Security*. Retrieved from [https://www.capgemini.com/resource-file-access/resource/pdf/securing\\_the\\_internet\\_of\\_things\\_opportunity\\_putting\\_cyber\\_security\\_at\\_the\\_heart\\_of\\_the\\_iot.pdf](https://www.capgemini.com/resource-file-access/resource/pdf/securing_the_internet_of_things_opportunity_putting_cyber_security_at_the_heart_of_the_iot.pdf)

caroleloomis, & hpecom. (2015). Internet of things research study: 2015 report. Retrieved from <http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf>

Cavoukian, A. (2011a). Privacy by Design Curriculum 2.0. Retrieved from [https://www.ipc.on.ca/site\\_documents/1b-Privacy by Design An Introduction-Instructor Resources.pdf](https://www.ipc.on.ca/site_documents/1b-Privacy%20by%20Design%20An%20Introduction-Instructor%20Resources.pdf)

Cavoukian, A. (2011b). *The 7 Foundational Principles*. Retrieved from <https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf>

CAVOUKIAN, A. (2015). Why privacy must be baked into the Internet of Things. Retrieved from <http://www.theglobeandmail.com/report-on-business/rob-commentary/how-we-can-maintain-privacy-in-the-era-of-the-internet-of-things/article24700062/>

Cavoukian, A., & Jonas, J. (2009). *Privacy by Design From Rhetoric To Reality*. Toronto.

Retrieved from <https://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>

Cavoukian, A., & Popa, C. (2016). Embedding Privacy Into What's Next: Privacy by Design for the Internet of Things.

Chase, J. (2013). *The Evolution of the Internet of Things*. Retrieved from <http://www.ti.com/lit/ml/swrb028/swrb028.pdf>

Chou, H.-T. G., & Edge, N. (2012). "They Are Happier and Having Better Lives than I Am": The Impact of Using Facebook on Perceptions of Others' Lives. *Cyberpsychology, Behavior, and Social Networking*, 15(2), 117–121. <http://doi.org/10.1089/cyber.2011.0324>

Cía, J. F. (2015). The future of the wearables and the Internet of Things depends on the investment in cybersecurity. Retrieved from <https://bbvaopen4u.com/en/actualidad/future-wearables-and-internet-things-depends-investment-cybersecurity>

CLARK, B. (2016). "I have nothing to hide" is killing the privacy argument. Retrieved from <http://thenextweb.com/opinion/2016/02/11/i-have-nothing-to-hide-is-killing-the-privacy-argument/#gref>

Clarke, R. (2013). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Retrieved from <http://www.rogerclarke.com/DV/Intro.html>

Cohn, J. (2015). The importance of Internet of Things data security and privacy | IBM Big Data & Analytics Hub. Retrieved from <http://www.ibmbigdatahub.com/blog/importance-internet-things-data-security-and-privacy>

Coraggio, G. (2015a). GLOBAL – Internet of Things needs privacy by design. Retrieved from <http://blogs.dlapiper.com/privacymatters/internet-of-things-needs-privacy-by-design/>

Coraggio, G. (2015b). IoT in 2016: Privacy by design is the only way. Retrieved from

<http://inform.tmforum.org/features-and-analysis/featured/2015/12/iot-in-2016-privacy-by-design-is-the-only-way/>

Council, A., Healey, J., Pollard, N., & Woods, B. (2015). THE HEALTHCARE INTERNET OF THINGS REWARDS AND RISKS in partnership with.

Crews, B. C., & Mangal, S. (2016). *IOT AND IT'S IMPACT ON TESTING*. Mexico City.

Retrieved from <http://www.getzephyr.com/resources/whitepapers/iot-and-its-impact-testing>

Dennedy, M. F., Fox, J., & Finneran, T. R. (2014). Technology Evolution, People, and Privacy.

In *The Privacy Engineer's Manifesto* (pp. 3–24). Berkeley, CA: Apress.

[http://doi.org/10.1007/978-1-4302-6356-2\\_1](http://doi.org/10.1007/978-1-4302-6356-2_1)

Diehn, S. A., & Goebel, N. (2012). “Internet of Things” holds promise, but sparks privacy concerns. Retrieved from <http://www.dw.com/en/internet-of-things-holds-promise-but-sparks-privacy-concerns/a-15911207>

Doherty, R. (2016). Why privacy is important, and having “nothing to hide” is irrelevant. Retrieved from <https://robindoherty.com/2016/01/06/nothing-to-hide.html>

Earnest & Young Cybersecurity and IoT Report. (2015). Cybersecurity and the Internet of Things Insights on governance, risk and compliance. Retrieved from [http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/\\$FILE/EY-cybersecurity-and-the-internet-of-things.pdf](http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf)

Emanuele Angelidis. (2015). The internet of things is as important as the world wide web.

Retrieved from <https://www.theguardian.com/media-network/2015/jan/09/internet-of-things-important-world-wide-web>

Facilitiesnet.com. (2015). Survey Suggests Many BAS Could Be Vulnerable To Hackers.

Retrieved from <http://www.facilitiesnet.com/buildingautomation/article/Survey-Suggests->

Many-BAS-Could-Be-Vulnerable-To-Hackers--15561?source=part

Firstbrook, P. (2015). The Six Principles of Resilience to Manage Digital Security. Retrieved from <http://www.gartner.com/smarterwithgartner/the-six-principles-of-resilience-to-manage-digital-security/>

Frahim Jazib, Pignataro Carlos, Apcar Jeff, M. M. (2016). Securing the Internet of Things: A Proposed Framework. Retrieved July 11, 2016, from <http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html>

FTC Staff Report. (2015a). *Privacy & Security in a Connected World FTC Staff Report*. Retrieved from <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

FTC Staff Report. (2015b). *Privacy & Security in a Connected World FTC Staff Report*. Retrieved from <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

Gartner Information Technology Glossary. (2016). Retrieved from <http://www.gartner.com/it-glossary/internet-of-things/>

Grau, A. (2016). IOT SECURITY STANDARDS – PAVING THE WAY FOR CUSTOMER CONFIDENCE. Retrieved from <http://www.standardsuniversity.org/e-magazine/march-2016/iot-security-standards-paving-the-way-for-customer-confidence/>

Green, C. (2016). Securing the digital persona: how we entered the age of the digital avatar. Retrieved from <http://www.information-age.com/it-management/strategy-and-innovation/123461602/securing-digital-persona-how-we-entered-age-digital-avatar>



Guillemin, P., Berens, F., Carugi, M., Barthel, H., Dechamps, A., Rees, R., ... Friess, P. (2014).

IERC Cluster Book 2014 Ch.3 SRIA WEB.

Hannah Becker. (2013). What is the Internet of Things and Why is it Important? Retrieved from

<http://www.technologyguide.com/feature/internet-of-things/>

Hern, A. (2015). Samsung rejects concern over “Orwellian” privacy policy. Retrieved from

<https://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy>

Hernandez, D., & Appleby, J. (2014). How Your Pacemaker Will Get Hacked. Retrieved from

<http://www.thedailybeast.com/articles/2014/11/17/how-your-pacemaker-will-get-hacked.html>

HOWARTH, F. (2015). The Damage of a Security Breach: Financial Institutions Face Monetary,

Reputational Losses. Retrieved from <https://securityintelligence.com/the-damage-of-a-security-breach-financial-institutions-face-monetary-reputational-losses/>

iaap, T. I. A. of P. P. (2016). What does privacy mean? Why it matters? Privacy v.security..

Retrieved from <https://iapp.org/about/what-is-privacy/>

ico.org.uk. (2016). Privacy by design. Retrieved July 16, 2016, from [https://ico.org.uk/for-](https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/)

[organisations/guide-to-data-protection/privacy-by-design/](https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/)

Information and Privacy Commissioner of Ontario. (2016). Introduction to PbD. Retrieved from

<https://www.ipc.on.ca/english/privacy/introduction-to-pbd/>

Intel. (2016). Internet of Things Applications Across Industries. Retrieved from

<http://www.intel.com/content/www/us/en/internet-of-things/industry-solutions.html>

Jadoul, M. (2015). The IoT: The next step in internet evolution. Retrieved from

<https://techzine.alcatel-lucent.com/iot-next-step-internet-evolution>

- Johnson, E. (2016). 6 IoT Security Dangers To The Enterprise. Retrieved from <http://www.darkreading.com/endpoint/6-iot-security-dangers-to-the-enterprise/d/d-id/1325140>
- Joshi, N. (2016). Security Risks and Challenges to IoT devices. Retrieved from <https://www.linkedin.com/pulse/security-risks-challenges-iot-devices-naveen-joshi>
- Jyoti Kundu, B. (2015). Internet of Things (IoT)-Implication in Logistics- A Report. Retrieved from <https://www.linkedin.com/pulse/internet-things-iot-implication-logistics-report-bhaskar-jyoti-kundu>
- Kenyon, H. (2015). Privacy By Design: Protect User Data From “Get-Go.” Retrieved from <http://www.informationweek.com/government/cybersecurity/privacy-by-design-protect-user-data-from-get-go/d/d-id/1318437>
- Kevin Ashton. (2009). That “Internet of Things” Thing. Retrieved from <http://www.rfidjournal.com/articles/view?4986>
- Kolkowska, E., & Kristofferson, A. (2016). Privacy by Design Principles in Design of New Generation Cognitive Assistive Technologies (pp. 384–397). [http://doi.org/10.1007/978-3-319-33630-5\\_26](http://doi.org/10.1007/978-3-319-33630-5_26)
- Libelium. (2016). 50 Sensor Applications for a Smarter World. Retrieved from [http://www.libelium.com/resources/top\\_50\\_iot\\_sensor\\_applications\\_ranking/](http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/)
- Lopez Research LLC. (2013). “*An Introduction to the Internet of Things (IoT)*.” Retrieved from [http://www.cisco.com/c/dam/en\\_us/solutions/trends/iot/introduction\\_to\\_IoT\\_november.pdf](http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf)
- Maddox, T. (2016). The dark side of wearables: How they’re secretly jeopardizing your security and privacy. Retrieved from The dark side of wearables: How they’re secretly jeopardizing your security and privacy

- MCSWEENY, T. (2015). Security Is a Must for the Internet of Things. Retrieved from <http://www.recode.net/2015/1/27/11558088/security-is-a-must-for-the-internet-of-things>
- Middleton, P., Kjeldsen, P., & Tully, J. (2013). *Forecast: The Internet of Things, Worldwide, 2013*. Retrieved from <https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide->
- O'Connor, C. (2015). The future of security and privacy for Internet of Things systems. Retrieved from <http://www.ibmbigdatahub.com/blog/future-security-and-privacy-internet-things-systems>
- Office of the Privacy Commissioner of Canada. (2010). *Privacy, Trust and Innovation — Building Canada's Digital Advantage*. Retrieved from <https://www.ic.gc.ca/eic/site/028.nsf/eng/00431.html>
- Ozimek, A. (2013). Will Big Data Bring More Price Discrimination? Retrieved from <http://www.forbes.com/sites/modeledbehavior/2013/09/01/will-big-data-bring-more-price-discrimination/#2173d6ad792d>
- Pandhi, R., & Hanson, J. (2015). *The 10 Challenges of Securing IoT Communications*. Retrieved from <https://www.pubnub.com/blog/2015-05-04-10-challenges-securing-iot-communications-iot-security/>
- Pemberton Levy, H. (2015). How the Internet of Things Is Changing Cybersecurity. Retrieved from <http://www.gartner.com/smarterwithgartner/how-the-internet-of-things-is-changing-cybersecurity/>
- Privacy Risk Summit Preview by Truste. (2016). Privacy Risk Summit Preview: Privacy by Design for IoT. Retrieved from <http://www.truste.com/blog/2016/05/23/privacy-risk-summit-preview-privacy-design-iot/>

- PTC Cloud Services. (2015). *Securing the Internet of Things: Seven Steps to Minimize IoT Risk in the Cloud*. Retrieved from [https://www.ptc.com/~media/Files/PDFs/Services/PTC\\_IoT\\_CloudSecurity\\_WP.ashx?la=en](https://www.ptc.com/~media/Files/PDFs/Services/PTC_IoT_CloudSecurity_WP.ashx?la=en)
- PwC 6th Annual Digital IQ. (2014). *Sensing the future of the Internet of Things*. Retrieved from <https://www.pwc.com/us/en/increasing-it-effectiveness/assets/future-of-the-internet-of-things.pdf>
- ROMANOSKY, S. (2011). Privacy vs. Security vs. Anonymity. Retrieved from <http://concurringopinions.com/archives/2011/01/privacy-vs-security-vs-anonymity.html>
- Samani, R. (2014). 3 key security challenges for the Internet of Things. Retrieved from <https://blogs.mcafee.com/business/3-key-security-challenges-internet-things/>
- Santucci, G., & Lange, S. (2008). Internet of Things in 2020 A ROADMAP FOR THE FUTURE  
RFID WORKING GROUP OF THE EUROPEAN TECHNOLOGY PLATFORM ON  
SMART SYSTEMS INTEGRATION (EPOSS).
- Scholtz, T. (2015). Lessons in How to Implement People-Centric Security. Retrieved from <http://www.gartner.com/smarterwithgartner/lessons-in-how-to-implement-people-centric-security/>
- Shanzhi Chen, S., Hui Xu, H., Dake Liu, D., Bo Hu, B., & Hucheng Wang, H. (2014). A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective. *IEEE Internet of Things Journal*, 1(4), 349–359. <http://doi.org/10.1109/JIOT.2014.2337336>
- Siegel, B. (2016). What is the difference between privacy and security? | CIO. Retrieved from <http://www.cio.com/article/3075023/privacy/the-difference-between-privacy-and-security.html>

- Solove, D. J. (2014). 10 Reasons Why Privacy Matters. Retrieved from <https://www.linkedin.com/pulse/20140113044954-2259773-10-reasons-why-privacy-matters>
- Sondergaard, P. (2014). Securing the Internet of Things. Retrieved from <http://www.forbes.com/sites/gartnergroup/2014/09/25/securing-the-internet-of-things/#6a6f0f261eb0>
- sourceLink. (2012). What Does Privacy Mean to You? Retrieved from <http://www.sourcelink.com/blog/rob-singh-latulipe/2012/06/22/what-does-privacy-mean-to-you->
- Tamarov, M. (2015). Intel, Cisco pushing for enhanced security communication, integration. Retrieved from <http://searchsecurity.techtarget.com/news/4500250845/Intel-Cisco-pushing-for-enhanced-security-communication-integration>
- Techopedia. (2015). Internet of Things (IoT). Retrieved from <https://www.techopedia.com/definition/28247/internet-of-things-iot>
- Thorne, E. (2015). Protecting our rights to privacy and digital dignity. Retrieved from <http://phys.org/news/2015-04-rights-privacy-digital-dignity.html>
- Turner, M. (2015). How to secure the internet of things. *Computerweekly.com*. Retrieved from <http://www.computerweekly.com/opinion/How-to-secure-the-internet-of-things>
- Vael, M. (2015). Advantages of privacy by design in IoE. Retrieved from <http://www.slideshare.net/markieturbo/advantages-of-privacy-by-design-in-ioe>
- Valerio, P. (2014). Why IoT Security & Privacy Are Critical. Retrieved from <http://www.networkcomputing.com/data-centers/why-iot-security-privacy-are-critical/1362672471>

- Ward, M. (2014). Smart meters can be hacked to cut power bills. Retrieved from <http://www.bbc.com/news/technology-29643276>
- Weitzner, D. J. (n.d.). Beyond Secrecy: New Privacy Protection Strategies for the World Wide Web.
- Wessing, T. (2015). Privacy by design – essential for the growth of the Internet of Things? Retrieved from [http://united-kingdom.taylorwessing.com/globaldatahub/article\\_internet\\_of\\_things.html](http://united-kingdom.taylorwessing.com/globaldatahub/article_internet_of_things.html)
- West, kimberly. (2015). The Future of Cyber Security: IoT Creates Entirely New Set of Risks and Organizations Embrace “Active Defense.” Retrieved from <http://www.boozallen.com/media-center/press-releases/2015/04/the-future-of-cyber-security--iot-creates-entirely-new-set-of-ri>
- Zanolli, L. (2015). Welcome To Privacy Hell, Also Known As The Internet Of Things. Retrieved from <http://www.fastcompany.com/3044046/tech-forecast/welcome-to-privacy-hell-otherwise-known-as-the-internet-of-things>
- Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2013). Privacy in the Internet of Things: Threats and Challenges. <http://doi.org/10.1002/sec.795>