THE INTERNET OF THINGS:
LEGAL ANALYSIS OF PRIVACY, SECURITY AND DATA OWNERSHIP IN MALAYSIA

BY

SIDI MOHAMED SIDI AHMED

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy in Law

Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia

APRIL 2021

ABSTRACT

The rapid development of technology has left its imprint on all aspects of modern life including the norm and systems that people depend on to regulate their conducts and protect their interests. The Internet of Things (IoT) is one of those successive technological waves that are widely being used by individuals, organisations and governments around the world. Based on this, the thesis examines the effect of IoT on the existing legal framework of Malaysia through highlighting challenges of this technology to the legal rules related to security, privacy and ownership of data. The discussion of privacy of data focuses on pointing out threats facing information privacy in the IoT environment and the challenges of complying with personal data protection principles in this electronic environment. In the security aspect, the thesis highlights threats of cyberspace to security of private and public entities with especial concentration on national security and assesses the ability of the existing legal framework of the country to efficiency deal with those threats. In addition to aspects of privacy and security, the thesis also discusses ownership of data and investigates the so-called 'propertization of data' (dealing with data as property) from economic, academic and legal perspectives. Moreover, the research also discusses the Shariah (Islamic law) view on security, privacy and ownership of data. The researcher uses the analytical method for finding relevant legal rules and examining the effectiveness of such rules in dealing with data flowing in the IoT environment. He also employs the comparative method for comparing laws pertaining to data in different aspects. The study uses both primary and secondary sources. Statutes and court-cases referred to in this thesis are mostly taken from Malaysia and sometimes from other jurisdictions. The study concluded that the current legal framework governing privacy and security in Malaysia provides considerable protection to information privacy and vital interests of the country. However, there is a need to improve and enhance such framework to enable it to efficiently cope with countless threats associated with cyberspace. For data propertization, the research found that dealing with data as property is a new idea, but it can theoretically be accepted by the existing legal system in Malaysia and elsewhere. The best legal models to be followed thereof are data protection law which grants various rights to data subjects and IP law which also gives an assortment of rights to data in its scope. As for the Shariah side, the thesis found that *Fiqh* rulings related to privacy, security and ownership can apply to data in the IoT environment.

خلاصة البحث

التطور السريع للتكنولوجيا ترك بصماته على جميع جوانب الحياة الحديثة بما في ذلك القواعد والأنظمة التي يعتمد عليها الناس لتنظيم سلوكهم وحماية مصالحهم. وإنترنت الأشياء (Internet of Things) تعتبر واحدة من موجات التكنولوجيا المتعاقبة التي تستخدم على نطاق واسع من قبل الأفراد والمنظمات والحكومات حول العالم. تبحث هذه الدراسة تأثير إنترنت الأشياء على الإطار القانوني القائم في ماليزيا حاليا من خلال إبراز تحديات هذه التكنولوجيا للنظم القانونية المتعلقة بأمن وخصوصية وملكية البيانات. يركز نقاش خصوصية البيانات على إبراز التهديدات التي تواجه المعلومات الشخصية في بيئة إنترنت الأشياء والتحديات المتعلقة بتطبيق قواعد حماية المعلومات الشخصية في هذه البيئة الرقمية. وفي ما يتعلق بالجانب الأمني، تلقى الدراسة الضوء على التهديدات السيبرانية التى تواجه أمن الكيانات الخاصة والعامة مع التركيز على التهديدات التي تواجه الأمن الوطني، وتقيم الدراسة قدرة الإطار القانوني الحالي على التعامل بكفاءة مع تلك التهديدات. بالإضافة إلى جانبي الخصوصية والأمن، تناقش الرسالة أيضا ملكية البيانات وتبحث ما يسمى ب"مالية البيانات" (التعامل مع البيانات على أنها مال) من وجهة نظر اقتصادية وأكاديمية وقانونية. وزيادة على ذلك، تناقش الرسالة أيضا وجهة نظر الشريعة الإسلامية في أمن وخصوصية وملكية البيانات. استعمل الباحث المنهج التحليلي لتحليل الأحكام القانونية المتعلقة بموضوع البحث ومعرفة فاعليتها في التعامل مع البيانات المتدفقة في بيئة إنترنت الأشياء. ووظف كذلك المنهج المقارن من أجل مقارنة تلك الأحكام المتعلقة بالبيانات في جوانب مختلفة. استعملت الدراسة كلا من المصادر الأولية والثانوية. وأغلب التشريعات وأحكام المحاكم التي اعتمدت عليها الدراسة أخذت من ماليزيا وقد استندت الدراسة أيضا إلى تشريعات وأحكام قضائية من دول أخرى. توصلت الدراسة إلى أن النظام القانوني الحالي الذى يحكم الخصوصية والأمن في ماليزيا يقدم حماية معتبرة للبيانات الشخصية ويوفر كذلك حماية لمصالح الدولة الأساسية. ومع ذلك، وجدت الدراسة أن هذا النظام يحتاج إلى تحسين وتعزيز ليتمكن من التعامل بكفاءة مع التهديدات المقترنة بالفضاء السيبراني والتي لا حصر لها. وفي مسألة مالية البيانات، وجدت الدراسة أن فكرة التعامل مع البيانات كمال فكرة جديدة ولكنها يمكن أن تقبل قانونا في ماليزيا وفي غيرها؛ لعدة أسباب منها أن قوانين حماية البياتات الشخصية تمنح حقوقا مختلفة لأصحاب البيانات الشخصية وقانون الملكية الفكرية يمنح أيضا أنواعا أخرى من الحقوق للبيانات التي تدخل في نطاقه. ومن ناحية أخرى، وجدت الدراسة أن أحكام الفقه الإسلامي المتعلقة بالخصوصية والأمن والملكية يمكن أن تنطبق على البيانات في بيئة إنترنت الأشياء.

APPROVAL PAGE

The thesis of Sidi Mohamed Sidi Ahmed has been approved by the following:

____
Sonny Zulhuda
Supervisor

____
Duryana Bt Mohamed
Co-Supervisor

____
Ida Madieha Bt. Abdul Ghani Azmi
Co-Supervisor

____
Juriah Abd Jalil
Internal Examiner

____
Nazura Binti Abdul Manap
External Examiner

____
Zainal Amin bin Ayub
External Examiner

____
Roslina Bt. Othman
Chairman

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Sidi Mohamed Sidi Ahmed

Signature .... Date ....27 / 04 / 2021....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

THE INTERNET OF THINGS: LEGAL ANALYSIS OF PRIVACY, SECURITY AND DATA OWNERSHIP IN MALAYSIA

I declare that the copyright holder of this thesis is owned by Sidi Mohamed Sidi Ahmed.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Sidi Mohamed Sidi Ahmed

……..………………………..	27 / 04 / 2021 ………………………..
Signature	Date

This thesis is dedicated to:

My beloved mother Khadijah

My late father Mohamed, May Allah have mercy upon him and make him one of the inheritors of the Garden Bliss

My sisters, brothers and others relatives and friends who offered me unflinching support during the course of the study.

ACKNOWLEDGEMENTS

بسم الله الرحمن الرحيم

Praise be to Allah, the Lord of the world who says “It is He Who brought you forth from the wombs of your mothers when you knew nothing; and He gave you hearing and sight and intelligence and affections: that you may give thanks (to Allah) (Surah al-Nahl: 78). All thanks to Allah and peace be upon the Prophet Mohamed (S.A.W) who says “he who does not thank people, does not thank Allah” (Tirmidhi).

I am greatly indebted to my supervisor Assoc. Prof. Dr. Sonny Zulhuda for his supervision, guidance and unflinching support from the early stages of the research to its end. My gratitude and appreciation are also directed to my co-supervisors Assoc. Prof. Dr. Duryana Mohamed and Prof. Dr. Ida Madieha Abdul Ghani Azmi for their constructive comments, advice and support which all led to the accomplishment of the study. May Allah reward, bless, guide my supervisors, improve their condition and admit them to the Garden.

I would also like to express my sincere gratitude and appreciation to those who examined the thesis: Prof. Dr. Nazura Binti Abdul Manap, Assoc. Prof. Dr. Juriah Abd Jalil and Assoc. Prof. Dr. Zainal Amin bin Ayub.

My gratitude and appreciation also go to the whole IIUM community especially my teachers in CELPAD, lecturers of AIKOL, friends, colleagues, the staff of AIKOL Postgraduate Office, IIUM Library, CPS and all of those who helped me to complete the study.

In the end of the acknowledgments, I would like to say, “All praise is due to Allah, by whose favor good deeds are accomplished.”

TABLE OF CONTENTS

Abstract ii
Abstract in Arabic iii
Approval Page iv
Declaration v
Copyright Page vi
Dedication vii
Acknowledgements viii
Table of Contents ix
List of Tables xiii
List of Cases xiv
List of Statutes xv
List of Abbreviations xvi

CHAPTER ONE: INTRODUCTION 1
1.1 Background of the Study 1
1.2 Statement of the Problem 8
1.3 Hypothesis 14
1.4 Objectives of the Research 14
1.5 Research Questions 15
1.6 Scope and Limitation of the Research 15
1.7 Literature Review 17
1.7.1 IoT and Data Protection 21
1.7.2 Security Challenges 25
1.7.3 Data Ownership 29
1.7.4 The Islamic Approach to IoT 33
1.8 Research Methodology 35

CHAPTER TWO: THE IOT CONCEPT AND CHALLENGES 37
2.1 Introduction 37
2.2 IoT Definitions 38
2.2.1 IoT Technical Definition 40
2.2.2 IoT Functional Definition 41
2.2.3 IoT Legal Definition 42
2.3 Development of IoT 44
2.3.1 IoT in Global and Regional Levels 45
2.3.2 Development of IoT in Malaysian 54
2.4 Social Benefits of IoT 55
2.4.1 IoT Usage in Commercial Aspects 56
2.4.2 IoT and Public Sector 57
2.4.3 IoT and Citizens Lifestyle 59
2.5 IoT Policies and Standards 60
2.5.1 International Industrial Standards 61
2.5.2 EU Perspective 63
2.5.2.1 Technical Standards 63
2.5.2.2 Regulatory Standards and Policies 64

2.5.3 The Malaysian Side 66
2.6 IoT and Law 68
2.6.1 IoT and Privacy 70
2.6.2 IoT and Security Challenges 72
2.6.3 IoT and Data Ownership 74
2.7 Concluding Remark 76

CHAPTER THREE: IOT AND PERSONAL DATA PROTECTION 78
3.1 Introduction 78
3.2 Nature of Data Protection Law 82
3.2.1 Data Protection and Privacy 82
3.2.1.1 Definition of Privacy 83
3.2.1.2 Definition of Personal Data 87
3.2.1.3 Chosen Definition 91
3.2.2 Data Protection around the World 93
3.2.3 The Right to Privacy 97
3.2.4 The Need for Data Protection 100
3.3 Data Protection in the European Union 104
3.4 Data Protection in Malaysia 108
3.4.1 PDPA 2010 (Act 709) 112
3.4.2 Torts 113
3.5 IoT and Personal Data Protection Principles 115
3.5.1 IoT and Data Processing 117
3.5.1.1 How Are Data Processed in the IoT Environment? 118
3.5.1.2 What Is Legally Required for Processing Personal Data? 121
3.5.1.3 Challenges of Compliance with Data Protection Principles in IoT 133
3.5.2 IoT and Data Security 145
3.5.3 IoT and Trans-Border Data Transfer 151
3.6 Concluding Remarks 155

CHAPTER FOUR: IOT AND SECURITY CHALLENGES 156
4.1 Introduction 156
4.2 Nature and Scope of Security 159
4.2.1 National Security 162
4.2.1.1 The National Cybersecurity Policies 166
4.2.2 Security of Private Entities 170
4.2.2.1 Security and the CIA Objectives 172
4.2.2.2 Security of IoT Technology 172
4.3 Threats in Cyberspace 175
4.3.1 Cyberattack and Its Impact on States 175
4.3.1.1 Cyberwar 178
4.3.1.2 Hacktivism 179
4.3.1.3 Cyber-espionage 182
4.3.1.4 Cybercrime 183
4.3.1.5 Malaysian Legal Response to Cyber Threats 186
4.3.2 Cyberattacks in the IoT Era 188
4.3.3 Critical Information Infrastructure 192
4.3.3.1 Definition of CII 192

4.3.3.2 CII in the IoT Era....196
4.3.3.3 CII Threats....197
4.3.3.4 Protection of CII in Malaysia....201
4.4 IoT and Prevention of Crime and Terrorism....210
4.5 Intelligence and Surveillance in the IoT Era....216
4.5.1 IoT and State Intelligence....216
4.5.1.1 How Intelligence Services Work....217
4.5.1.2 IoT and Intelligence Services Agencies....218
4.5.1.3 Legal Response to Intelligence Activities....220
4.5.2 IoT and Surveillance....224
4.5.2.1 The Definition of Surveillance....224
4.5.2.2 Advantages and Disadvantages of Surveillance....226
4.5.2.3 Surveillance from the Legal Viewpoint....228
4.5.2.4 Surveillance from the Viewpoint of Data Protection Law231
4.6 Concluding Remarks....233

CHAPTER FIVE: IOT AND DATA PROPERTY....235
5.1 Introduction....235
5.2 Definitions....238
5.2.1 Data....238
5.2.2 Ownership....240
5.2.3 Property....241
5.2.4 Ownership and Property of Data....244
5.3 Data as a Valuable Thing....245
5.4 Data and Law....253
5.4.1 Protecting Data as Creation of Mind....254
5.4.1.1 Copyright Act 1987....256
5.4.1.2 Data as Databases....260
5.4.2 Data as a Secret....264
5.4.2.1 Confidential Information Law....265
5.4.2.2 Official Secrets Law....267
5.4.2.3 Computer Crimes Act 1997....269
5.4.3 Data as a Right....270
5.4.3.1 The Right to Control Self-information....271
5.4.3.2 Freedom of Information....272
5.5 Property Right as a New Mechanism for Protecting Data....274
5.5.1 The Nature of Data Property....276
5.5.2 Data Property in Light of Existing Legislation....279
5.5.2.1 Statutory Law and Data Propertization....280
5.5.2.2 Data Property in the Judiciary Sphere....282
5.6 Propertization of Data in the IoT Era....287
5.6.1 Ownership of Pure Personal Data....298
5.6.2 Ownership of Mixed Data....300
5.7 Concluding Remarks....301

CHAPTER SIX: AN ISLAMIC APPROACH TO PRIVACY, SECURITY AND PROPERTY OF DATA....303
6.1 Introduction....303
6.2 Privacy from the Shariah Perspective....305

6.2.1 Privacy and its Meaning 306
6.2.2 Physical and Territorial Privacy 308
6.2.2.1 Physical Privacy 308
6.2.2.2 Territorial Privacy 311
6.2.3 Informational Privacy 313
6.2.3.1 Inquiring Private Information 314
6.2.3.2 Disclosure of Secret Information 316
6.3 Security from the Shariah Perspective 321
6.3.1 Using Information as a Security Means 322
6.3.2 Protection of Data in the Shariah Viewpoint 327
6.4 The Shariah Approach to Data Ownership 331
6.4.1 The Concept of Ownership in the Shariah 332
6.4.2 Scope of Property 335
6.4.3 Propertization of Data 338
6.4.3.1 Propertization of Data in Light of the Hanafi View 338
6.4.3.2 Propertization of Data in Light of the Majority View 339
6.4.3.3 Propertization of Data in the View of Contemporary Researchers 340
6.5 Concluding Remarks 341

CHAPTER SEVEN: CONCLUSION AND RECOMMENDATIONS 343
7.1 Introduction 343
7.2 Summary 344
7.3 Recommendations 352
7.3.1 Recommendations for Data Protection Improvement 352
7.3.1.1 Expanding the Scope of PDPA 353
7.3.1.2 Clarifying the Position of Those Who Process Personal Data in the IoT Era 353
7.3.1.3 Providing a Clear Guideline on How to Implement Data Protection Principles in the IoT Sphere 354
7.3.1.4 Establishing a Right to Compensation and Liability 355
7.3.2 Recommendations for Security Improvement 355
7.3.2.1 Creating Comprehensive Cybersecurity Legislation 356
7.3.2.2 Amending Some Existing Legislation 357
7.3.2.3 Establishing Practical Steps to Mitigate Impact of Implementation of Security Law on Human Rights 358
7.3.3 Recommendations Related to Data Propertization 358
7.3.3.1 Studying the Idea of Data Propertization in Light of the Existing Legal System in Malaysia 359
7.3.3.2 Taking IP and Data Protection Law as Models for any Movement in Propertization of Data 359
7.3.3.3 Ownership of Data Shall not be an Absolute Right 360
7.3.4 Recommendations Based on the Islamic Law Viewpoint 360
7.4 Final Remarks 361

REFERENCES 363

LIST OF TABLES

Table No. Page No.

3.1 The 7 Principles of PDPA 2010 134

4.1 Reported General Incidents of 2017, 2018 and 2019 201

LIST OF CASES

Coco v, A. N. Clark (Engineers) Ltd. [1969] R.P.C. 41

Electro Cad Australia Pty Ltd & Ors v Mejati Rcs Sdn Bhd & Ors [1998] 3 MLJ 422,

International news Service v Associated Press- (1918) 245 US 215

Jonathan Dixon v the Queen [2015] NZSC 147 Courts of New Zealand,

Lee Ewe Poh v Dr Lim Teik Man & Anor [2011] 1 MLJ 835.

Lew Cher Phow @ Lew Cha Paw & Ors v Pua Yong Yong & Anor - [2011] MLJU 1195

Oxford v Moss (1979) 68 Cr App Rep 183

Phipps v Boardman [1966] 3 All ER 721

PDPA 2012 v. Actxa Pte. Ltd. [2018] SGPDPC 5 Case No DP-1611-B0320

Radion Trading Sdn Bhd v Sin Besteam Equipment Sdn Bhd & Ors [2010] 9 MLJ 648

Riley v. California 573 U. S. (2014), Supreme Court, of the United States

*Sivarasa Rasiah v. Badan Peguam Malaysia & Ano*r, [2010] 3 CLJ 507 (FC).

Stewart v the Queen [1988] 1 S.C.R. 963

The Oxford v Moss (1978) 68 Cr App Rep 183, [1979] Crim LR 119

The Riley v. California 573 U. S. (2014), Supreme Court,

Ultra-Dimension Sdn Bhd v Kook Wei Kuan [2001] MLJU 751

Ultra-Dimension Sdn Bhd v Kook Wei Kuan [2004] 5 CLJ 285

UsedSoft GamH v Oracle International Corp, case no. C-128/11 [2012]

LIST OF STATUTES

Charter of Fundamental Rights of the European Union 2012
Communications and Multimedia Act 1998
Computer Crimes Act 1997
Constitution of the Islamic Republic of Mauritania 1991
Council of Europe Convention for the Protection of Individual with regard to Automated Processing of Personal Data 1981
Council of Europe Convention on Cybercrime 2001
Deoxyribonucleic Acid (DNA) Identification Act 2009
Electronic Commerce Act 2006
EU Directive 96/9/EC on the legal protection of databases 1996
EU Regulation 2016/679/EU on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data 2016
European Convention for the Protection of Human Rights and Fundamental Freedoms 1950
International Covenant on Civil and Political Rights 1966
Malaysian Federal Constitution
Mauritanian Law of Cybercrime 2016 (Law no. 007 of 2016)
Official Secrets Act 1972
Penal Code (Revised- 1997)
Personal Data Protection Act 2010
Prevention of Terrorism Act 2015
Security Offences (Special Measures) Act 2012
Singaporean Cybersecurity Act 2018
The UK Data Protection Act 2018
Theft Act 1968
Trademarks Act 1976
UN General Assembly Resolution No. 217 Universal Declaration of Human Rights 1948
UN General Assembly Resolution No. 45/95 Guidelines for the Regulation of Computerized Personal Data Files 1990

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
CCA	Computer Crimes Act
CIA	Confidentiality, Integrity and Availability
CI	Critical infrastructure
CII	Information infrastructure
CJEU	Court of Justice of the European Union
CMA	Communications and Multimedia Act
CNII	Critical National Information Infrastructure
EDR	Event Data Recorders
EU	European Union
FOI	Freedom of information
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
ICS	Industrial control systems
ICT	Information Communications Technology
IDC	International Data Corporation
IERC	European Research Cluster on Internet of Things
IIC	Industrial Internet Consortium
IMDA	Singapore Infocomm Media Development Authority
IoT	Internet of Things
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MCMC	Malaysian Communications and Multimedia Commission
MOSTI	Minister of Science, Technology and Innovation
MyCERT	Malaysian Computer Emergency Response Team
NCSP	Malaysian National Cyber Security Policy
NSA	National Security Agency of USA
OECD	Organisation for Economic Co-operation and Development
OEMs	Original equipment manufacturers
P2P	Peer-to-peer systems
PDPA	Personal Data Protection Act
PER	Private information retrieval
PET	Privacy enhancing technologies
P-FOIE	Penang Freedom of Information Enactment 2010
PMDs	Personal Medical Devices
RTI	Right to information
SCADA	Supervisory Control and Data Acquisition
S-FOIE	Selangor Freedom of Information Enactment 2011
SRIA	Strategic Research and Innovation Agenda
TLS	Transport layer security
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UNODC	United Nations Office of Drugs and Crime
UN	United Nations
USA	United States of America

VPN	Virtual private networks
WP29	Article 29 Data Protection Working Party
ZB	Zettabytes

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Technology has made people's lives better and easier and has provided them with myriad of benefits. This improvement is pervasive in the economic, health, educational, social sectors and so on. The Internet of Things (IoT) is one of the successive waves of technology that promise unprecedented benefits and at the same time pose challenges. It has been described as an Internet evolution "driven by an extension of the Internet through the incorporation of physical items."[1] The whole idea of IoT revolves around connecting objects with the Internet and with each other and enabling them to process, generate, send, receive, etc., information about themselves and the things they are attached to. IoT is perceived differently from different people in different sectors. For example, while it in the consumer perspective means "wearable technology and "smart" appliances, such as thermostats and televisions," it means "autonomous machines and sensorized equipment" in the industrial sector.[2] To simply understand IoT, consider it as "things or objects that connect to the Internet and each other."[3] The term IoT may also be used to refer to the specific time when the number of connected objects outnumber people in the earth.[4] Currently there are many things connected to the Internet including ordinary and everyday objects. For example, in 2010, around 12.5

[1] Syed Abdul Moeed and A. Arun Kumar, "Internet of Things (IoT) - Internet Evolution", *International Journal of Engineering Trends and Technology (IJETT),* (– Special Issue – April 2017): 50.

[2] Shawn DuBravac and Carlo Ratti, "The Internet of Things: Evolution or Revolution?," American International Group (AIG), https://www.aig.com/content/dam/aig/america-canada/us/documents/insights/aig-iot-evolution-or-revolution.pdf (accessed 15 Aug, 2020).

[3] Samuel Greengard, *The Internet of Things*, (Massachusetts Institute of Technology, 2015), 15.

[4] Dave Evans, "The Internet of Things – How the Next Evolution of the Internet is Changing Everything," Cisco, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed 15 Aug, 2020).

billion devices were estimated to be connected to the Internet and such number increased dramatically to 25 billion in 2015.[5] In 2019 there were 26.66 billion IoT devices and such number was expected to exceed 75 billion by 2025.[6] According to Gartner, consumer applications represented 63% of IoT applications (5.2 billion units) used in 2017.[7] In fact, the connected devices will affect different aspects of life and such effects will be good and bad at the same time.

IoT technologies have captured people's attention, imagination and efforts for about a decade and it is likely to do so in the future as it is still one of the top emerging technologies. For example, IoT is considered among technologies enabling business trends side by side with other emerging technologies such as Artificial Intelligence (AI), blockchain and such like.[8] Moreover, Gartner has counted IoT legal, social and ethical issues among top IoT ten trends for 2019 to 2023.[9] All these indicate or necessitate dealing with IoT as a reality and providing legal solutions to its challenging issues. IoT is being used in various domains such as transport, logistics, energy, smart environment, agriculture, etc.[10] IoT promoters are claiming that when it is fully employed, the gap between poor and rich people will be closed or at least minimised as resources and

[5] Dave Evans, "The Internet of Things – How the Next Evolution of the Internet is Changing Everything," Cisco,https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed 15 Aug, 2020).

[6] Ana Bera, "80 IoT Statistics (Infographic)," Safeatlast, https://safeatlast.co/blog/iot-statistics/ (accessed 15 Aug, 2020).

[7] Gartner, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016," Gartner-Newsroom, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 (accessed 15 Aug, 2020).

[8] GS1, "Trend Research 2018-2019," GS1, https://www.gs1.org/docs/innovation/GS1-Trend-Research-Paper-070219.pdf (accessed 15 Aug, 2020).

[9] Nick Jones, "Top Strategic IoT Trends and Technologies Through 2023," Gartner, https://www.gartner.com/en/documents/3890506 (accessed 15 Aug 2020).

[10] Louis Coetzee and Johan Eksteen, "The Internet of Things – Promise for the Future?: An Introduction," CITESEERX, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.8816&rep=rep1&type=pdf (accessed 15 Aug, 2020).

services will reach the needy.[11] In the healthcare sector, for instance, IoT could enable health professionals to serve more patients and detect diseases.[12] As an illustration, a patient who needs close observation can be monitored via "using IoT-driven, non-invasive monitoring" where sensors are used to collect physical information from the patient without the need for the presence of health professionals to "check the patient's vital signs."[13]

Regardless of the above, however, IoT has a cost especially when it comes to security and privacy of individuals. Data stored and collected about individuals has great values and the same could be said about data collected from inanimate things (cars, houses, offices). Moreover, many might be interested in gathering information via IoT or using it as a means of surveillance for various purposes. It can be used by governmental intelligent services agencies,[14] intruders, criminals and other malicious parties. As insecure IoT systems and devices can be used and deployed to generate and store sensitive private information about individuals and things, human dignity, privacy as well as their safety might be at risk in the IoT age. Thus, data protection becomes an urgent issue in the IoT era where everything could reveal everything.

Nowadays, expressions such as smart environments, smart homes and smart cities become on everybody's lips. Therefore, IoT applications can be found in almost all domains such as smart grids, environmental monitoring and logistics, intelligent

[11] Dave Evans, "The Internet of Things – How the Next Evolution of the Internet is Changing Everything,"Cisco,https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed 15 Aug, 2020).

[12] David Niewolny, "How the Internet of Things Is Revolutionizing Healthcare," NXP, https://www.nxp.com/docs/en/white-paper/IOTREVHEALCARWP.pdf (accessed 15 Aug, 2020).

[13] David Niewolny, "How the Internet of Things Is Revolutionizing Healthcare," NXP, https://www.nxp.com/docs/en/white-paper/IOTREVHEALCARWP.pdf (accessed 15 Aug, 2020).

[14] Sam Thielman, "The Internet of Things: How Your TV, Car and Toys Could Spy on You," The Guardian, http://www.theguardian.com/world/2016/feb/10/internet-of-things-surveillance-smart-tv-cars-toys (accessed 15 Aug, 2020).

transportation systems, e-health, etc.[15] IoT devices that could collect information related to persons include, among others, smartwatch, fitness tracker, smart eyewear, smart clothing, wearable medical device and wearable camera.[16] As an illustration, among wearable devices that can collect personal information are the followings[17]: (1) Health and fitness devices sensors- such as countertop devices, wearable, intimate and implantable sensors. There are many types of personal health devices -range from least physically invasive to most invasive- that can generate and store valuable and intimate personal information about users (this information includes: how much and how fast you eat, steps taken each day, heart rate, skin temperature, breathing patterns, blood pressure, weight scale, etc.). (2) Automobile sensors (black boxes) -such as Event Data Recorders (EDR), and consumer's automobile sensors. These sensors can collect enormous amounts of information about vehicles and drivers' behaviour. (3) Home and electricity sensors- such as the smart home and the smart grid. These are types of IoT devices that provide information to the home-dwellers and let them control home-appliances remotely but at the same time they can generate, transmit, and store huge information about homes and people stay in them. (4) Employee sensors. The purpose of these sensors is to enable the employers to monitor their employees in the workplace and to know what they are doing and whether they act in accordance with employment rules or not. However, these sensors could create problems if employers try to access and collect personal and private information about the employees. (5) Smartphone

[15] River Publishers Series in Communication, *Internet of Things- From Research and Innovation to Market Development*, ed. by Ovidiu Vermesan and Peter Friess, (Aalborg: River Publisher, 2014), 243-4.

[16] Mokhinabonu Mardonova and Yosoon Choi, "Review of Wearable Device Technology and Its Applications to the Mining Industry," *Energies,* vol. 11, no. 3 (2018): 547.

[17] Scott R. Peppet, "Regulation of the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", *Texas Law Review*, vol. 93 no. 1 (2014): 85, Mostafa Haghi, MSc, Kerstin Thurow, Ing. Habil, Regina Stoll and Med. Habil, "Wearable Devices in Medical Internet of Things: Scientific Research and Commercially Available Devices," *Healthcare Informatics Research*, vol. 23 no. 1 (2017): 4.

sensors. Sensors embedded in smartphones can be considered one of the most ubiquitous new sensors technologies.[18] These sensors can detect physical orientation, track the phone movement in space, and so forth.

From the above, it becomes obvious that IoT systems and devices have the power to generate, transmit and store enormous information about users' habits, activities, characteristics and personalities as well as about their surrounding environment. Since most of data streaming in the IoT environment might include personal information, concern about misusing such valuable information is justifiable. In the legal view, serious questions related to data streaming in the IoT sphere need to be answered: What information does the Internet of Things collect? Who owns and controls data generated, processed and stored in IoT environment? Who should be responsible in case of negligence? Is IoT a secured place in the meaning of data protection law? It could be true that calling for an IoT specific law at this stage may be premature or undesirable as IoT is still in its infancy. Nonetheless, examining and investigating the phenomenon in light of the existing legal frameworks are important because IoT technology is penetrating in almost all aspects of modern life in a way that can negatively and positively affect people. Therefore, the law has to keep an eye on it in order to take its advantages and avoid its disadvantages.

As an emerging topic, IoT has been addressed and discussed by researchers who come from different disciplines from different aspects (technical, social, economic and legal aspects, etc.). Data protection, security, and privacy are at the forefront of legal concerns. The issue of ownership of data and responsibility for a damage or injury to property or persons that may be caused by this technology are also other challenges.

[18] Peppet, 85.

From here, this research attempts to contribute to the foregoing discussions by examining and judging IoT from security, privacy and data ownership in Malaysia from a legal perspective.

Recently, IoT became an important issue in the national agenda of many countries. For example, in the European Union (EU) region there is an assortment of projects and research about IoT and its impacts. In 2009, the European Research Cluster on Internet of Things (IERC) created with the aim of establishing policy frameworks in the IoT field. Following that, an Expert Group on IoT has investigated IoT from various aspects such as governance, architecture, standards, security and privacy in addition to other ethical issues.[19] The IERC seeks, among other things, to : (1) establish a cooperation platform and develop a research vision for IoT activities in Europe and become a major entry and contact point for IoT research in the world, (2) define an international strategy for cooperation in the area of IoT research and innovation and have an overview of the research and innovation priorities at the global level, (3) coordinate the cooperation activities with other EC Clusters and ICT projects, (4) coordinate and align the SRIA (Strategic Research and Innovation Agenda) agenda at the European level with the developments at the global level, and (5) organise debates/workshops leading to a better understanding of IoT and Future Internet, 5G, cloud technology, and adoption.[20] As Ron Davies mentioned, the rapid growth of IoT is anticipated to bring tangible benefits to the EU citizens, businesses and governments.[21] Moreover, the Article 29 Data Protection Working Party (WP29)

[19] Ângela Guimarães Pereira; Alice Benessia and Paula Curvelo, "Agency in the Internet of Things" CORE, https://core.ac.uk/download/pdf/38627181.pdf (accessed 15 Aug, 2020).

[20] ERC-European Research Cluster on the Internet of Things, IERC, http://www.internet-of-things-research.eu/about_ierc.htm (accessed 15 Aug, 2020).

[21] Ron Davies, "The Internet of Things Opportunities and challenges, "European Parliamentary Research Service Blog, https://epthinktank.eu/2015/05/21/the-internet-of-things-opportunities-and-challenges/ (accessed 15 Aug, 2020).

acknowledged that IoT has already met the needs of the EU citizens in general and it is going to create significant economy growth that will benefit both large and small innovative and creative businesses working in the field. However, the WP29 asserts that IoT advantages should not lead to ignore its disadvantages like challenges related to security and privacy.[22]

Another manifest of IoT policy initiative is found in Malaysian context. In 2014, the Minister of Science, Technology and Innovation (MOSTI) published the country's first National Internet of Things (IoT) Strategic Roadmap.[23] The Roadmap provides an overview of Malaysian mission and vision towards IoT. Apart from IoT definition and megatrends, the Roadmap discussed the importance of IoT and readiness of the country to join the IoT caravan. The IoT economic potential for Malaysia is forecast to reach RM9.5 billion in 2020 and the growth will continue to RM42.5 billion thereafter. IoT was also estimated to create more than 14000 high-skilled employment opportunities by 2020. It could also serve the research community and help them commercialise R&D outputs. Regarding readiness of the country for IoT, the Roadmap mentioned that Malaysia has a suitable environment for IoT and a strong ground in terms of technical, political and societal aspects. Nevertheless, the Roadmap highlights some obstacles that can hamper implementation of IoT in Malaysia such as security, privacy and others concerns. This hindrance will be discussed later on in the coming chapters of this present study.

[22] Article 29 Data Protection Working Party (WP29), "Opinion 8/2014 on the on Recent Developments on the Internet of Things," EC.EUROPA.EU, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (accessed 15 Aug, 2020).

[23] See, Ministry of Science, Technology and Innovation (MOATI)), *National Internet of Things (IoT) Strategic Roadmap*, (Kuala Lumpur: MIMOS Berhad, 2014).