Robert Walters · Leon Trakman
Bruno Zeller

Data Protection Law

A Comparative Analysis of Asia-Pacific and European Approaches

Springer

Data Protection Law

Robert Walters • Leon Trakman • Bruno Zeller

Data Protection Law

A Comparative Analysis of Asia-Pacific and European Approaches

European Union
Singapore
Australia
India
Indonesia
Malaysia
Thailand
Japan

Springer

Robert Walters
Victoria University
Melbourne, VIC, Australia

Bruno Zeller
University of Western Australia
Crawley, WA, Australia

Leon Trakman
Faculty of Law
University of New South Wales
Kensington, NSW, Australia

ISBN 978-981-13-8109-6 ISBN 978-981-13-8110-2 (eBook)
https://doi.org/10.1007/978-981-13-8110-2

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Foreword

This book provides a comparison and practical guide for academics, students and business communities grappling with the current day data protection laws across the Asia Pacific (Australia, Singapore, India, Indonesia, Japan, Malaysia and Thailand) and the European Union. During the course of researching this book, the original proponent of the World Wide Web, Sir Tim Berners-Lee, published a letter raising serious concerns over the development and use of the Internet today.[1] Below is an excerpt from his letter of 12 March 2017.

Today marks 28 years since I submitted my original proposal for the World Wide Web. I imagined the web as an open platform that would allow everyone, everywhere to share information, access opportunities and collaborate across geographic and cultural boundaries. In many ways, the web has lived up to this vision, though it has been a recurring battle to keep it open. But over the past 12 months, I've become increasingly worried about new trends, which I believe we must tackle in order for the web to fulfill its true potential as a tool which serves all of humanity. "We've lost control of our personal data".

The current business model for many websites offers free content in exchange for personal data. Many of us agree to this – albeit often by accepting long and confusing terms and conditions in documents – but fundamentally we do not mind some information being collected in exchange for free services. But, we're missing a trick. As our data is then held in proprietary silos, out of sight to us, we lose out on the benefits we could realise if we had direct control over this data and chose when and with whom to share it. What's more, we often do not have any way of feeding back to companies what data we'd rather *not* share – especially with third parties. This widespread data collection by companies also has other impacts. Through collaboration with – or coercion of – companies are also increasingly watching our every move online, and passing extreme laws that trample on our rights to privacy. It creates a chilling effect on free speech and stops the web from being used as a space to explore important topics, like sensitive health issues, sexuality or religion.

[1] World Wide Web Foundation, https://webfoundation.org/2017/03/web-turns-28-letter, accessed 17 December 2017

This is a complex problem, and the solutions will not be simple. We must work together with web companies to strike a balance that puts a fair level of data control back in the hands of people, including the development of new technology like personal "data pods" if needed and exploring alternative revenue models like subscriptions and micropayments. We must push back against misinformation by encouraging gatekeepers to continue their efforts to combat the problem, while avoiding the creation of any central bodies to decide what is "true" or not. We need more algorithmic transparency to understand how important decisions that affect our lives are being made, and perhaps a set of common principles to be followed.

Sir Tim Berners-Lee's letter cannot be underestimated. The point about transparency and a common set of principles has to function across the entire data chain. Doing so creates and establishes a level of trust and certainty in technology and a law protecting people's personal data. That data chain needs to be framed in light of a definition of personal data that is both legally defensible and economically sustainable. That data chain also needs to encompass such diverse elements as the collection, consent, use, analysis, disclosure, retention and limitation of data, along with the backend systems that collect and store the data and to acknowledge the importance of government and industry regulation of data. It needs to go along with definitions of personal data, including inevitable tensions between them. These issues are no different to those faced by any other industry. Transparency is about knowing the unknown, because technology is no different to polluting the ocean, and, therefore, providing a level of trust in the systems. What is under the ocean is out of sight and thus out of mind. The authors, in writing this book, seek to stimulate the reader and respond to Sir Tim Berners-Lee's concerns. There are fundamental questions that need to be considered. What is possibly the solution to promote greater legal convergence and harmonisation in data protection law and policy? Does the current co-regulatory approach adopted by governments and industry work effectively? Will it safeguard personal data into the future? What is the best regulatory model? Is there yet a different way forward? This book will examine competing approaches towards data protection, based on the three models that have been identified. The models identified in this book include the European, Singaporean and Australian approaches to data protection and privacy over the Internet. This book calls for a different approach to redress their deficiencies and build on their strengths through an international model. It also highlights other areas of the law where personal data is being considered such as intellectual property, anti-trust, transnational contracts and cybersecurity.

Preface

The free flow of personal data as a tradable commodity is becoming an important part of the global economy. Personal data is transcending human rights, antitrust law, intellectual property, transnational contracts, cybercrime and criminology, among many other areas of law.

Largely emerging out of developments in the European Union (EU), data protection law is considered as new area of law in the contemporary digital economy. With the recent implementation of the EU's General Data Protection Regulation (GDPR), the EU is arguably influencing the development of data protection and privacy law across the world. Therefore, this book is timely, coming 1 year after the implementation of the GDPR.

The book is the first of its kind, comparing the data protection laws of the EU to the divergent laws across Asia and the Pacific. The time is also right for the governments around the world to consider how to formulate policies and to develop laws that embrace the new digital economy, while protecting individuals from the potential harmful use of their personal data. The national and regional responses to this data revolution have been diffused. Some jurisdictions, such as the EU and Australia, have had data protection and privacy laws in place since the 1980s. For other countries in Central, Southeast and East Asia, these laws are a recent phenomenon. For example, Singapore, Malaysia and Japan have all established data protection laws that, while differing from one another, are no more than a decade old. India and Indonesia, in turn, have adopted a sectorial approach and are in the process of developing specific data protection laws.

Despite the attempts by some jurisdictions and international organisations to establish a baseline of concepts and principles that can be found in most data protection laws, the approach to data protection remains fragmented and inconsistent in both law and policy. The challenges for the government are not easily addressed as technology changes at a rapid rate and legal systems are often slow to respond. This slow legal and policy response is epitomised in the perpetuation of a general focus on regulating data use, such as regulating data controllers and processors. However, there is little to no government regulation of the actual Internet systems, platforms, servers and infrastructure. With the expansion of big data, practice-based data

analytics, blockchain and development of quantum technology, the collection of personal data will only increase. At issue, the security framework to protect this data is far from fully understood. Moreover, the regulatory and policy framework underpinning the management of data is fragmented, requiring greater vigilance by nation states to ensure the appropriate policy and legal response are developed for the future. Thus, there is the potential for criminal activity arising from the misuse of personal data, which is likely to result in privacy breaches increasing.

Equally important is the need for more pervasive international responses to improve data protection law(s), including the need to redress tensions across regional and national institutions, and bodies responsible for regulating the use of personal data. With the internationalisation of the Internet and technology, there is also a growing need for both resources and information to fill the gaps in the legal and policy responses to these deficiencies. Complicating these international aspirations is the absence of an agreed best model or combination of models that adequately provide a balance between the many competing and conflicting areas of law and policy pertaining to data. In other words, as people become more aware of how organisations are using their personal data for monetary or some other gains, they may call for more regulation or less regulation. At this point in time, the current models that have emerged see the EU version taking a greater focus on human rights, while Singapore has implemented a business-friendly model. Australia, on the other hand, sits somewhere between the two. Therefore, this book calls for greater legal and policy convergence and harmonisation, at an international level, in data protection law and in the many other areas of law that pervades. It must be noted that it is out of scope if this book to examine other possible models for data protection, such as, North America, China or the Middle East.

Thanks to the Springer publisher team.

Melbourne, VIC, Australia Robert Walters
Kensington, NSW, Australia Leon Trakman
Crawley, WA, Australia Bruno Zeller

Acknowledgements

A special acknowledgement and great thanks go to Associate Professor Dr. Sinta Dewi Rosadi, Cyber Law Center, Faculty of Law, Padjadjaran University, Indonesia, who has coauthored journals with the authors of this book, for providing a specialist advice on Indonesian data protection law. The work continues today in this complex but important area of law.

The authors would also like to thank Professor Marc Bungenberg, Director of the Europa-Institut Saarbrücken, European Law and Public International Law at Saarland University in Germany, for his advice on technical matters within the GDPR.

Further acknowledgement and thanks go out to Dr. A. Nagarathna, Associate Professor and Coordinator, Advanced Centre on Research, Development and Training in Cyber Law and Forensics, National Law School of India University, for providing valuable comments on the draft Indian chapter and input into the Indian component in relation to cybercrime/security.

Thanks to Dr. Sonny Zulhuda, Assistant Professor, International Islamic University, Malaysia, for his review of the Malaysia chapter. Without his wise counsel, the Malaysian chapter would not have been completed.

A special thanks also goes out to Dr. Jompon Pitaksantayothin (PhD), Lecturer, Department of Society and Health, Faculty of Social Sciences and Humanities, Mahidol University, Thailand, for providing valuable input and assistance in relation to the current status of data protection law in Thailand.

The authors would also like to acknowledge the work of Professor Dr. Graham Greenleaf and Professor Dr. Simon Chesterman in the area of data protection and privacy throughout Asia and Australia.

The book would not have come to publish without the assistance of many individuals and organisations from the various countries.

Chia Swee Yik – Chia, Lee & Associates, Advocates & Solicitors, Kuala Lumpur, Malaysia
Dr. Nilubol Lertnuwat, Assistant Professor of Law, Thammasat University, Bangkok, Thailand
Amber Sinha, Senior Programme Manager, The Centre for Internet and Society and Practicing Lawyer, India
Linklaters – DLA Piper – International Comparative Legal Guide

Contents

About the Authors

Robert Walters Dr. Robert Walters is a Lecturer of Law, Victoria University, Melbourne, Australia; is an Adjunct Professor with the European Faculty of Law, The New University, Slovenia, Europe. Dr. Walters is a Member of the ASEAN Law Association, Singapore, and of the United Nations Commission on International Trade Law Coordination Committee for Australia.

A very special thanks and enormous gratitude go to the coauthors of this book, Professor Dr. Bruno Zeller and Professor Dr. Leon Trakman, for allowing Dr. Walters the fortunate opportunity to work with them in this complex but, ever increasingly, important area of law and public policy. Without their combined wise counsel, this book would not have been completed.

This book is a dedication to his late father, Mr. Gordon Walters, and mother, Pam Walters. Special thanks to his wife, Catherine Tan-Walters, who provided him the space and support to complete this work.

Since completing his PhD, Dr. Walters legal research areas now include data protection, artificial intelligence, technology, cybercrime/security law, and international trade, finance and investment law with a particular focus on Australia, Asia Pacific (APEC and ASEAN countries), including Europe. Dr. Walters is admitted as an Australian Lawyer.

Leon Trakman Professor Trakman is former Dean (2002–2007) and currently Professor of Law, Faculty of Law, University of New South Wales, and Director, Masters in Dispute Resolution. He is also Academic Disability Advisor at the UNSW. His appointments include the following: Distinguished Visiting Professor, University of California, Davis (1999–2000); Professor of Law, Schulich School of Law at Dalhousie University (1975–1999); Visiting Professor, University of Wisconsin Law School (1992–1993); Visiting Professor of Law, University of Cape Town (1990); Bora Laskin National Fellow in Human Rights, Canada (1997–1998); Killam Professor, Killam Foundation (1986); Visiting Professor, Tulane University School of Law (1983), and Bolton Visiting Professor, McGill University Faculty of Law (1982).

Professor Trakman specialises, inter alia, in contracts, international commercial arbitration, trade and investment law. He is an author of 8 books and over 100 articles in international recognised journals in his areas of specialty and has been Lead Chief Investigator on a Discovery Grant from the Australian Research Council (2014–2018). In addition, he has received significant fellowships including a Harvard Doctoral Fellowship, a Bora Laskin National Fellowship (one awarded annually across all disciplines in Canada), a Killam Senior Fellowship and various grants from the Canada Council and the Social Sciences and Humanities Research Council of Canada.

Trained as an International Commercial Arbitrator and Mediator, he has served as Presiding Arbitrator or Arbitrator in more than 100 international disputes and as mediated in over 30 disputes. These have included disputes in the fields of contracts, sales, construction, IP, sales, franchise, insurance law and executive remuneration, among others. He also chairs or has chaired and serves on various panels, boards and associations devoted to arbitration and mediation on four continents.

Bruno Zeller Professor Zeller, who has finished his PhD, BCom and BEd at the University of Melbourne and Master of International Trade Law at Deakin University, is a Professor of Transnational Commercial Law at the University of Western Australia; an Adjunct Professor at Murdoch University, Perth; a Fellow of the Australian Institute for Commercial Arbitration, Panel of Arbitrators, MLAANZ; and a Visiting Professor of the Institut fur Anwaltsrecht, Humboldt University, Berlin, and Stetson University College of Law, Florida. His areas of expertise are international trade law, international arbitration, conflict of laws and maritime law. He has published extensively on the CISG, arbitration law, harmonisation of contract law and carbon trading.

List of Diagram

Part I

Chapter 1
Problem Definition, Structure and Methodology

Abstract This Chapter begins by outlining the problem in defining and understanding the interrelationship between privacy and data protection law in Australia, India, Indonesia, Japan, Malaysia, Singapore, Thailand and the European Union. This Chapter will demonstrate and discuss how the concept of privacy is considered an important feature of the modern era. In other words, it is argued that there has been wide acceptance and a convergence of privacy that now transcends, government, countries, cultures religion over the Internet. This convergence of the concept of privacy, has resulted in nation states adopting to varying degrees, data protection and privacy laws. However, it will be highlighted that the current day approach needs further development and greater convergence and harmonization of data protection law and policy at the international level. This will be important as the trade in personal data continues to grow.

It will be argued in this Chapter that the privacy and data protection law of these jurisdictions is far from settled. It is further argued that data protection and privacy law has two dimensions. First, is to protect personal data and information of individuals, as a human right. Second, is balancing the protection of personal data with current and future economic activity (trade) of personal data. Moreover, data protection and privacy cannot be restricted to a single country or region of the world. It is international, and has been underpinned by Internet technology and infrastructure that knows no [national] borders. Thus, these laws, while being developed by nation states for their own particular sovereign needs, the internationalization of the Internet poses significant challenges to the future law and policy in this area. They are likely to continue to be challenged and require reviewing and updating, as technology continues to change. Being a recent addition to the law, data protection is also challenging and is arguably in conflict with other areas of the law, such as intellectual property, competition, transnational commercial contract law, and cybercrime-security law. This Chapter also highlights the structure of the overall book in recognizing and responding to these differences in data protection and privacy law. It argues that data protection is a tool of Internet privacy. At the recent June 2019 meeting of the G20, the leaders' declaration called for respect of national and international regulation of data and technology. The importance of this declaration highlights the importance for governments to balance innovation with protection of personal data. To achieve this, the book reinforces the G20 leaders position,

R. Walters et al., *Data Protection Law*,
https://doi.org/10.1007/978-981-13-8110-2_1

and goes a step further, by recommending that an international Model Law be developed, similar to international trade law. Also, consideration to an international treaty or convention will support any model law and go some way to closing the gaps and tensions between country data protection law. Thus, this book calls for greater legal convergence and harmonization in this emerging and complex area of law and policy. The book also identifies that personal data being afforded an intellectual property right. It also highlights the tension between data protection and competition law and cybersecurity/crime law. It will also be argued that data protection can fall within the current transnational international contract legal framework. Adopting data protection within these areas of law, provide valuable tools to strengthen the governance, control and regulation of personal data.

1.1 Problem Definition

1.1.1 Privacy

Privacy and data protection mean different things to industry, governments and the general community. Unlike other areas of law that have well settled legal concepts, norms and principles, it is an area of law that currently is far from settled. More than 40 years ago, Zelman Cowan stated that a man without privacy is a man without dignity.[1] However, privacy and data protection pose a significant challenge for government, society and industry. This challenge is even more pronounced than ever in the new digital economy, with millions of people accessing the Internet daily, and not knowing whether their personal privacy is being infringed.

Privacy has been described in three ways. Firstly, privacy in making certain significant self-defining choices. Secondly, privacy of personal information; and thirdly, privacy as it relates to an individual's personal space and body.[2] Arguably, someone's privacy is compromised when others obtain information about an individual, pay attention to him or her, or, gain physical access. Privacy has therefore protected secrecy, anonymity and solitude.[3] Simon Chesterman suggests that this definition may be too broad, because it would include rights not to be punished. The other element to privacy is through the principal of dignity, which has been expressed as a fundamental human right by the European Union 2000 Charter of Fundamental Rights. However, if privacy is to be solely viewed as a right, the tension with other societal interests such as national security and the economy, arguably dilutes privacy to some degree.[4] That tension becomes even more evident between

[1] Cowan Z *The Private Man* 24 Inst Pub Affairs Rev 26 (1970).

[2] Kang J (1998) *Information Privacy in Cyberspace Transactions*, Stanford Law Review, 1998, pp. 1201–04.

[3] Chesterman S (2012) *After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012*, Singapore Journal of Legal Studies, p 396.

[4] Ibid.

commercial activity and human rights, more generally. This is because personal data defined by the law has become a tradable commodity. Nonetheless, Chesterman believes that the sphere in which privacy relating to personal data can be insulated is the physical confines of one's home, with temporal limits determined by the moment at which one's telecommunication devices are switched off or out of range.[5] However, the ability to insulate one's privacy online is questionable, because most people have very little idea as to the footprint they have personally created when surfing the Internet. Thus, technology focusses on information privacy. It is difficult to define when it relates to personal data, given that data can come in many different forms.

Privacy can also mean different thing to different people. Richard Clarke, [6] believes that privacy can be conceived philosophically,[7] psychologically,[8] sociologically[9] and economically.[10] Clarke goes on to categorize privacy as being interpreted broadly by the individual as a form of personal behavior,[11] personal communication,[12] and personal data, which is often referred to as data privacy and information privacy.

The problem with the contemporary theory of privacy is that it has many deficiencies. Its focus on information means that it excludes many areas widely held to be basic to privacy. These include, but not limited to, the ability to make fundamental decisions about one's personal and family life; insofar as it suggests that personal control is limited to the individual who is the subject of that information.[13] Nevertheless, as a framework through which to view what is loosely termed privacy, the focus on information accurately highlights the overlapping but discrete subject of data protection.[14] Simon Chesterman notes that throughout Asia, in particular, many jurisdictions now embrace data protection laws even in the absence of any formal protection of a more abstract right to privacy. The theory of privacy is also set to evolve and change as technology changes. From its beginning, the scope of

[5] Ibid.

[6] Clarke R *What's 'Privacy'?,* Workshop at the Australian Law Reform Commission on 28 July (2006) http://www.cse.unsw.edu.au/~cs4920/resources/Roger-Clarke-Privacy.pdf, accessed 19 April 2018.

[7] Ibid, in Europe, people are regarded as being very important for their own sake. The concepts of 'human dignity' and integrity play a significant role in some countries, as do the notions of individual autonomy and self determination and human rights.

[8] Ibid, people need private space. This applies in public as well as behind closed doors and drawn curtains.

[9] Ibid, people need to be free to behave, and to associate with others, subject to broad social mores, but without the continual threat of being observed.

[10] Ibid, people need to be free to innovate. International competition is fierce, and countries with high labour-costs need to be clever if they want to sustain their standard-of-living.

[11] Ibid, referred to as 'bodily privacy', is concerned with the integrity of the individual's body.

[12] Ibid, including what is sometimes referred to as interception privacy.

[13] Chesterman S (2012) *After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012*, Singapore Journal of Legal Studies, 2012, p. 396.

[14] Ibid.

privacy has evolved to include most elements of modern technology. Thus, privacy can be best described as being culturally sensitive. It can also be described as being culturally biased and is based on Western thought and the Western Liberal Tradition. According to the Western Liberal Legal Tradition, privacy, while considered a principle of data protection, is a fundamental right within itself, and is associated with protecting a person's identity.[15] Privacy has evolved from its traditional notion of the right to be left alone. As a concept it engages the protection of human rights buttressed against the promotion of economic development. In early times, the law gave a remedy only for physical interference with life and property, which has been well understood to be trespass.[16] However, as countries respond to data protection differently the very concept of a privacy right has not been fully accepted, over the Internet. The concept of privacy has meant something different to states outside the Western Liberal Tradition to their counterparts in Western Democratic states.

The challenge is to evaluate how different cultures and legal traditions within the selected nation states influence and regulate these conceptions of privacy. How these concepts are regulated is fundamentally important in the modern world. Indeed, it determines whether a country or region studied in this book is seen as having a competitive disadvantage when compared to other countries or regions that enjoy cultural and legal traditions that are differently attuned to, not only to the development of technology and the Internet, but also in regulating them. The competitive advantage is not only economical, but also operates at a personal level in protecting a person's human rights. One example of the differences in privacy, can in part be summarized when comparing Western thought with other religions in Central Asia, such as Buddhism. Charles Ess states:

> In those countries such as Japan and Thailand where Buddhism plays a central role in shaping cultural values and identity, the Buddhist emphasis on "no-self" (Musi in Japanese) directly undermines Western emphases on the autonomous individual as the most important reality (at least since Descartes), the source of morality (in Kant), the foundation of democratic polity, and in all these ways the anchor of Western emphases on individual privacy. As Buddhism stresses instead the importance of overcoming the ego as the primary illusion at the root of our discontent—it thus provides a philosophical and religious justification for doing away with "privacy" altogether, as in the example of Japanese Pure Land Buddhism (Jodo-shinsyu), which inspires some authors to move towards salvation by voluntarily betraying private, even shameful personal thoughts.[17]

Buddhism is also a major religion, along with Hinduism throughout India. The understanding of privacy in India dates back to 1960s case of *Kharak Singh v. State of UP*[18] where the court noted that privacy was not a fundamental right laid out in the constitution. However, privacy in the law of India is nevertheless a central part of the right to personal liberty, especially as it concerns privacy against arbitrary

[15] Hildebrandt M (2006) *Privacy and Identity*. In: Claes E, Duff A and Gutwirth S (eds) Privacy and the Criminal Law, Oxford, United Kingdom Hart, 2006, pp. 43–60.

[16] Samuel D, Brandeis L (1890) *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, pp. 193–220.

[17] Ess C (2005b) *Lost in translation*. Ethics Inf Technol 7, 1 2005b, pp. 1–6.

[18] *Kharak Singh v. State of UP*, (1964) 1 SCR 332, 359 (India).

intrusion. Nonetheless, India's perception of 'privacy' as a concept has been traditionally viewed as subjective in terms of personal space and depends on one's culture, environment and economic condition.[19] It is not about the economic value of that information.[20] However, that view is slowly changing in India. In December 2017, the Indian Government released a White Paper to study various issues relating to data protection. The white paper makes specific suggestions on principles underlying data protection and privacy. India is particularly concerned about the growth in the digital economy, and the need to balance the protection of its citizen's personal data.[21] The committee of experts had not conclusively reviewed community submissions at the time of writing this book. Nonetheless, the development justifies maintaining a watching brief, particularly to see how the committee reacts to those submissions and whether it adopts community concerns selectively.

Viewed broadly, privacy can include protecting all forms of personal communications; the personal body (biometrics and medical)[22]; personal data and personal information (name and address; personal possession such as property).[23] However, the definition of privacy within national and supranational law is rarely defined. It is rather the information that constitutes personal data that is defined. Moreover, the conception of privacy in Islam is worth highlighting. Both Indonesia and Malaysia are predominantly Islamic countries, and privacy has been viewed by many Muslim scholars as a fundamental human right.[24] Privacy stems from the *Maqasid al Shariah,* from which personal rights *(haqq)* are derived. According to the Maqasid, all individual rights are God-given and by their nature not absolute.[25] Even so, there are some exceptions such as witnesses are allowed to give testimony for purposes of law enforcement and the imposition of punishment, even if this means intruding upon another's privacy.[26] In the exercise of such rights, the state is guided by two main functions: *al amr,* or the promotion of certain positive conduct, and *al nahy,* or the prohibition of negative conduct.[27] The establishment of rules and institutions such as the institution of *hisbah* serve as machinery to promote positive conduct. Essential to the prohibition of negative conduct is the creation of a list of offences such as outraging modesty, spying, *'ghibah'* (revealing embarrassing details about

[19] Basu S (2010) *Policy-Making, Technology, and Privacy in India*, INDIAN J.L. & TECH. vol 6. p. 66.

[20] Ibid.

[21] White Paper of the Committee of Experts on a Data Protection Framework for India, December 2017.

[22] Westin A (1967) *Privacy and Freedom.* New York: Atheneum, p. 351.

[23] Neethling J, Potgieter M, Visser J (1996) *Neethling's law of personality*, Butterworths. pp. 35–36.

[24] Kamali, H. (2007) *The Right to Life, Security, Privacy and Ownership in Islam* (Cambridge, Islamic Texts Society); Mahmood, T. (ed.) (1993) *Human Rights in Islamic Law* (New Delhi, Institute of Objective Studies).

[25] Madieha Azmi I, *Personal Data Protection Law: The Malaysian Experience*, 16 Info. & Comm. Tech. L. 125 (2007) pp. 130.

[26] Ibid.

[27] Ibid.

others), disclosing matrimonial secrecy, defamation and trespass to property.[28] Therefore, the right of privacy comes in two normative frameworks: the prohibition of intrusion into other's privacy, and instructions and guidance for keeping secrets.[29] Personal privacy (a person is free to conduct their own affairs without interference from outsiders) is guaranteed in the Qur'an in *Surah al Taubah: 105, Surah Fussilat:* 40 and *Surah Saba: 11*. All conduct of a person deserves the highest respect in terms of privacy and secrecy. Any attempt to collect information on their activities would amount to spying ('tajassus'), a conduct forbidden in Islam.[30] Furthermore, Berween argues that privacy is both a very important societal and legal concept to Islam. For Berween, privacy constitutes one of the most precious freedoms, most comprehensive and respected of rights. In Islam, privacy and good manners in public contribute to the highest virtues, and are parts of a Muslim's duty. The right to privacy in Islam includes:

1. the right for every individual to be left alone in their private life;
2. the right to be free from governmental surveillance and intrusion;
3. the right not to have an individual's private affairs made public without their permission;
4. the protection of persons, and places where they live from searches and seizures;
5. the protection of knowledge and thoughts from compulsory self-incrimination; and
6. the right to keep all personal information confidential.[31]

More recently, there has been a hybridization of privacy in which the elements of the West and the East have converged.[32] That convergence has not been by accident. Rather, there has been deliberate attempts at convergence in response to globalization, regionalization, the movement of goods, and services and people in which legal frameworks, concepts, principles and norms require more cohesion. Nonetheless, privacy constitutes a human right, or at least the appropriate use of someone's personal data and information.[33] The level of privacy afforded to an individual is still determined by the national laws of each country or regional entities such as the European Court of Human Rights and the Court of Justice of the European Union. However, the nature if privacy remains divergent across these institutions.[34]

---

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Berween M *"The Fundamental Human Rights: An Islamic Perspective"* The International Journal of Human Rights 61 (2002) pp. 70–74.

[32] Ess C (2005b) *Lost in translation*. Ethics Inf Technol 7, 12005b, pp. 1–6.

[33] International Association of Privacy Professionals, https://iapp.org, accessed 20 December 2017. Article 7 and 8 Charter of Fundamental Rights of the European Union C 326/12.

[34] Case −28/08 P *Commission/Bavarian Lager* [2010] ECR I–6055, para. 60.

The ways in which people create, safeguard and enhance their privacy, and the extent to which they exhibit a desire for privacy, vary from culture to culture according to a complex array of factors.[35] In societies which provide little opportunity for physical or spatial solitude, human beings seem to adopt various strategies for cultivating other forms of social distance.[36] Barrington believes that the need for privacy is socially created and is complex, with a strongly felt division between the private realm and public sphere. Privacy, to date, is minimal where technology and social organization is concerned.[37] It has resulted in what can be best described in some regions of the world as a patchwork of law and policy to address privacy issues – on the run. This is certainly true in the contemporary world, where people who operate in the technology sphere are unaware of whether their privacy is being intruded upon. Furthermore, the protection of privacy has a tendency to manifest itself, after the fact, namely, when it is too late to protect privacy that has been violated. It is practically impossible to predict the consequences or the level of harm arising from a violation of a privacy right, notably the misuse of personal data, especially in today's information society.[38] Meg Leta Ambrose and Jef Ausloos argue that privacy is abstract because harms are often concerned with societal and psychological issues. They are distant because many of the consequences will only reveal themselves after a series of reactions to their practical application in specific cases. The impact of privacy breaches is also uncertain because such breaches might never occur, or at least, not occur in a foreseeable way, due to the lack of understanding of the platforms and infrastructure used to capture personal data.[39]

1.1.2 The Modern History of the Right to Privacy

The right to privacy itself is not new. In 1890 Samuel Warren and Louis Brandeis wrote an essay titled, "The Right to Privacy," which was published in Harvard Law Review.[40] They proposed recognition of an individual's "right to be let alone" and argued that this right should be protected by existing law, as a matter of human rights. The right has (in Western Liberal Tradition) arisen significantly from the relationship between the individual, society and the nation state. This liberal thought is something that Hobbes and Locke described as protecting rights derived from the

[35] Altman I (1977) *Privacy Regulation: Culturally Universal or Culturally Specific?,* Journal of Social Issues, vol. 33, pp. 66–84.

[36] Barrington M (1987) *Privacy: Studies in Social and Cultural History*, American Journal of Sociology, vol 92, 1987.

[37] Ibid, p. 276.

[38] Ambrose M, Ausloos J *The Right to Be Forgotten Across the Pond,* Journal of Information Policy, Vol. 3 (2013), pp. 1–23.

[39] Ibid.

[40] Samuel D, Brandeis L (1890) *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, pp. 193–220.

'state of nature' of mankind, and as forming the basis of the ideals of freedom and liberalization that underpinned the French Revolution.[41] However, scholars have attempted to provide a solid theoretical foundation to the right to privacy. De Boni and Prigmore argue for the protection of a right to privacy from an idealistic, neo-Hegelian philosophy point of view. They see privacy, not as a "human right", but as the logical consequence of the Hegelian idea of free will.[42] This thought is based on traditional Anglo-Saxon philosophy and does not consider the wider world. In particular, it does not consider traditional Central or South East Asian thought.

The right to privacy began to take hold following WWII, when the United Nations had to consider privacy in the context of ideological differences along North–South and East–West ideological lines.[43] Countries in the South-East camp, including mostly developing countries, emphasized the socio-economic benefits of scientific and technological discoveries. In contrast, those in the North-West bloc—mainly industrial nations—argued that priority be given to the negative impact that these technological discoveries may have on human rights, particularly the right to privacy. These divisions could be seen partly as reverberations from a broader debate on the generation of human rights. The resulting effect saw states divided between those that argued for prioritizing civil and political rights, and those that focused on socio-economic and cultural rights. Richard Clayton and Hugh Tomlinson categorize privacy as the:

1. Misuse of personal information. A right to restrict the use of "personal" or "private" information about an individual is central to the right to privacy.
2. Intrusion into the home. The right of the individual to respect for the home is fundamental to any notion of privacy. Unreasonable searches and seizures trigger privacy issues.
3. Photography, surveillance and telephone tapping. The "private sphere" is invaded not only by physical intrusion into the home.
4. Other privacy rights. There is a range of other privacy rights which covers all forms of interference in the "private sphere" including appropriation of a person's image, interference with private sexual behaviour and questions of the sexual identity of transsexuals.[44]

The position taken by Clayton and Tomlinson arguably captures the various cultural, religious and legal thought of privacy in the modern period. Nonetheless, according to Daniel Solove privacy" as a legal concept is challenging at best, and

[41] Hobbes T (1981) *Leviathan*, C. B. Macpherson (Editor), Penguin. Locke J (1986) Second Treatise of Government, Prometheus.

[42] De Boni M, Prigmore M (2001) *A Hegelian basis for information privacy as an economic right*, in Roberts M, Moulton M, Hand S, Adams C. (eds) Information systems in the digital world, Proceedings of the 6th UKAIS conference, Manchester, UK, Zeus Pres.

[43] Micheal Yilma K, *The United Nations data privacy system and its limits*, International Review of Law, Computers & Technology (2018).

[44] Clayton R., Tomlinson H *The Law of Human Rights* (2 Ed, Oxford University Press, 2009) [The Law of Human Rights] at 1005.

appears to be about everything, and yet it also appears to be about nothing.[45] On the other side, James Whitman is of the view that our conception of privacy reflects our knowledge of, and commitment to, the basic legal values of our culture and values.[46] Another dichotomy that has arisen in the West, is the view that privacy constitutes an important element of liberty.[47] For instance, the right to freedom from intrusions by the state.[48] Moreover, traditionally, many nation states privacy laws from Western societies have tended to focus on the freedom to control access to one's private life. It is an approach by which one can consent to the loss of privacy. A good example is the entry to one's private property by another, without consent. Importantly, the concept of consent in privacy has been long established, and has also emerged in the modern technological (the Internet) period to also provide a level of control over one's personal data. The resulting effect is that there is a level of privacy protection over the Internet. Yet, the European concept of privacy, by comparison, views it as an aspect of dignity.[49] This subtle difference arguably has little baring on privacy in the context of data protection and the Internet. This has been reinforced by Whitman who argues that privacy today is closely aligned with data protection. However, it is our view that data protection is merely a tool that goes some way to protect privacy over the Internet.

The conceptualization of privacy, along with data protection, is also not subject to a consistent method of expression, or to a particular thought or emotion about the ambit of privacy regulation. This inconsistency arose because the right to privacy could relate to a host of factors, such as signs, paintings, sculpture, music, newspapers,[50] and in the contemporary world, the use of the mobile phone and

[45] Solove, D *A Taxonomy Of Privacy,* University of Pennsylvania Law Review, (2006), pp. 477–564.

[46] Whitman, J *The Two Western Cultures of Privacy: Dignity versus Liberty*. Yale Law School (2004) p. 1160.

[47] Ibid. The word 'liberalism' has been used, since the eighteenth century, to describe various distinct clusters of political positions, but with no important similarity of principle among the different clusters called liberal at different times. The roots of liberalism rest in the classical interpretation, that there ought to exist a certain minimum area of personal freedom, which must never be violated. Liberty in this sense is the condition in which an individual has immunity from the arbitrary exercise of authority. It presupposes some frontiers of freedom that nobody should be permitted to cross, and requires the minimum, and demanded a maximum degree of noninterference compatible with the maximum demands of social life.

[48] Ibid.

[49] Ibid. Human dignity plays a role both at the international and state levels. On the international level, the Universal Declaration of Human Rights opens with the statement that "recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world." Other prominent international documents and covenants rely upon human dignity as a leading value. The concept of human dignity also plays a significant role in the debate over the 'universalism' or 'relativism' of human rights. In the contemporary human rights discourse within the international arena, human dignity is highly visible. At the national level, human dignity became a central concept in many modern constitutions. The concept of human dignity now plays a central role in the law of human rights, there is surprisingly little agreement on what the concept actually means.

[50] Ibid.