

**Protecting Liberty and Nurturing Prosperity
in the Propertization of Digital Footprint
in the Age of Surveillance Capitalism**

By Ma. Angela Teresa G. Sebastian

Foundation for Liberty and Prosperity
2019-2020 Dissertation Writing Contest

DEDICATION

“Every work which he began in the service of the house of God in law and in commandment, seeking his God, he did with all his heart and prospered.”

2 Chronicles 31:21

ABSTRACT

In the age of surveillance capitalism, data is the new currency, whereby the digital footprints of consumers are commodified and made the subject of analysis and sale. The economic interests of knowledge-based, data-driven enterprises involving the collection and processing of data runs the risk of undermining and violating the right to privacy and right to data protection of every *Juan*. Hence, the study poses the following question: How can the right to privacy and the right to data protection be effectively enforced in a way that promotes liberty and nurtures prosperity for the everyday Filipino?

The author proposes a hybridized approach to the treatment of digital footprint in the context of property and property rights: In treating certain *personal information as outside the commerce of man*, human dignity is extended not just to the natural or physical body, but the extensions thereof in the digital; whereas treating certain *personal information as within the commerce of man* but as the exclusive property of the user provides an opportunity for financial prosperity, to enjoy the use and the fruits of one's digital footprint. An application of this proposed hybridized approach brings back to the individual the full power and control over his or her digital footprints.

Whether in the form of taxing the digital economy directly, or requiring the payment of revenues into an account divided among data subjects, or direct-to-consumer payout mechanisms for those who elect to sell their personal information, the overall effect is a more equitable redistribution of the wealth of the digital economy, leading to liberty and economic prosperity truly felt and experienced by every *Juan*.

OUTLINE

Chapter I shall provide an overview of the research, starting with an analysis of the current digital landscape and culminating in the exposure of the (mis)use of digital footprints by knowledge-based, data-driven enterprises.

Chapter II shall provide the current legal framework in international and domestic law of the two rights under attack by such (mis)use of digital footprints: the right to privacy and right to personal data protection.

Chapter III shall provide the theoretical justifications for the hybridized approach in the treatment of personal data, in the nature of an expansion from the traditional privacy protection regime to one under property law.

Chapter IV shall provide the basis for the treatment of personal information in the first tier as outside the commerce of man, and the treatment of personal information in the second tier as within the commerce of man, and the implications of such treatment on the various contracts entered into and by knowledge-based, data-driven enterprises.

Chapter V shall provide the remedies of the data subject in case of unlawful processing of personal information outside and within the commerce of man, and the various ways that the wealth of the digital economy may be more equitably distributed.

Chapter IV shall emphasize the role of this hybridized approach to digital footprint in more actively protecting the rights of individuals in the wake of persistent abuses to the right to privacy and data protection, and proposes an application of this proposed hybridized approach to bring back to the individual the full power and control over his or her digital footprints, leading to liberty and economic prosperity truly felt and experienced by every *Juan*.

TABLE OF CONTENTS

I.	Commodification of personal data.....	6
	A. Background.....	6
	B. Research question and thesis statement.....	9
	C. Objectives.....	10
	D. Significance.....	10
	E. Research methodology.....	10
	F. Scope and limitations.....	11
II.	Right to privacy and the right to personal data protection.....	12
	A. Right to privacy.....	12
	1. Right to privacy in international law.....	12
	2. Right to privacy in Philippine law.....	16
	a) Right to privacy in the 1987 Philippine Constitution.....	16
	b) Right to privacy in the NCC.....	17
	c) Right to privacy in the RPC.....	17
	d) Right to privacy in Special Laws.....	18
	B. Right to data protection.....	18
	1. Right to data protection in international law.....	18
	2. Right to data protection in Philippine law.....	20
	a) Data Privacy Act.....	20
	b) Other special laws.....	21
III.	Theoretical justifications.....	23
	A. Personal information outside the commerce of man.....	23
	1. Personhood theory justifications.....	23
	B. Personal information within the commerce of man.....	24
	1. Incentive theory justifications.....	24
	2. Natural rights justifications.....	24
IV.	Dual approach to the treatment of personal information.....	26
	A. Personal information outside the commerce of man.....	26
	1. Conflict of laws.....	26
	2. Domestic laws.....	26
	a) Personal information outside commerce of man.....	26
	b) Effect on contracts.....	30
	B. Personal information within the commerce of man.....	33

1.	Conflict of laws.....	33
2.	Domestic laws.....	35
a)	Personal information within commerce of man.....	35
b)	Effect on contracts.....	38
V.	Exacting accountability from data driven enterprises.....	43
A.	Remedies for unlawful processing of personal information outside the commerce of men.....	43
1.	Conflict of laws.....	43
2.	Special laws.....	44
3.	Article 19 of the New Civil Code.....	44
4.	Article 20 of the New Civil Code.....	45
5.	Article 26 of the New Civil Code.....	45
B.	Remedies for unlawful processing of personal information within the commerce of men.....	46
1.	Conflict of laws.....	46
2.	Breach of contract.....	46
3.	Special laws.....	46
4.	Article 19 of the New Civil Code.....	46
5.	Article 20 of the New Civil Code.....	47
6.	Article 21 of the New Civil Code.....	47
7.	Article 26 of the New Civil Code.....	47
C.	Way forward: Wealth distribution.....	48
1.	Unjust enrichment.....	48
2.	Taxing the digital economy.....	49
3.	Direct to consumer profit-sharing mechanisms.....	50
VI.	The role of the paradigm shift in strengthening liberty and prosperity under the rule of law.....	52

There are certain truths that transcend sovereignties, territories, ideologies and legalities. And one of those truths is this: The best way to conquer poverty, to create wealth and to share prosperity is to unleash the entrepreneurial genius of people by granting them the freedom and the tools to help themselves and society.

- Former Chief Justice Artemio V. Panganiban¹

I. THE COMMODIFICATION OF PERSONAL DATA

A. Background

Data is the new currency² in the age of surveillance capitalism.³ This currency takes the form of digital footprints - “every shred of digital data - every movement, every transaction, every record - woven together into a single virtual database”.⁴ Through surveillance capitalism, digital footprint is commodified and made the subject of analysis and sale.⁵ Data constitutes the very foundation and arguably, the primary capital stock of the current knowledge-based,

¹ Artemio V. Panganiban, *Unleashing Entrepreneurial Ingenuity*, 12th General Assembly of the Asean Law Association, Makati Shangri-la Hotel, Makati City, February 26, 2015, available at <https://cjpanganiban.com/2015/02/26/unleashing-entrepreneurial-ingenuity/> [accessed 10 March 2020]

² Eggers, W.D., Hamill, R., and Ali, A. (2013). Data as the new currency: Government’s role in facilitating the exchange. *Deloitte Review* (2013) 13, 18-31.

³ Zuboff, S. (2015). *Big other: Surveillance capitalism and the prospects of an information civilization*. *Journal of Information Technology* (2015) 30, 75-39

⁴ Garfinkel, S., and Cox, D., (2009). *Finding and archiving internet footprint*. Presented at the first Digital Lives Research Conference. London, England; John, Spacey. 2016. 6 types of digital footprint. *Simplicable*, November 24. <https://simplicable.com/new/digital-footprint>.

⁵ Angwin, J. (2014). *Dragnet Nation: A quest for privacy, security, and freedom in a world of relentless surveillance*, New York: Times Books.

data-driven economy,⁶ founded on a simple yet powerful proposition:

“If the product is free, the product is you.”⁷

The aftermath of the Facebook-Cambridge Analytica scandal has brought to the forefront the power Big Data holds in determining the relations between public and private entities, and correspondingly, the data privacy and data protection rights of individuals.⁸ The need to strengthen data privacy and data protection rights of Filipinos is apparent, especially due to the strong digital media consumption of Filipinos.

According to the *Digital in 2019* report of social media firms Hootsuite and We Are Social, the Philippines ranks high in global internet usage, both in breadth and in depth.

Of the 108 million population, 79 million Filipinos are internet users, resulting in an internet penetration rate of 73.1%.⁹ The Philippines ranks 12th in the world among those with the highest number of internet users.¹⁰ Filipino users spend an average of 10 hours and 2 minutes per day using the internet on any device, ranking first in the world.¹¹ Filipino users rank first in the world for daily social media use at an average of 4 hours and 12 minutes per day¹², across 10.4 social accounts per person.¹³

⁶ Ciuriak, D. (2017). *The Knowledge-Based and Data-Driven Economy: Quantifying the Impacts of Trade Agreements*. CIGI Paper No. 156. Waterloo, ON: CIGI. www.cigionline.org/publications/knowledge-based-and-data-driven-economy-quantifying-impacts-trade-agreements.

⁷ Goodson, S. (2012). If you're not paying for it, you become the product. *Forbes*, available at <https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/#2d66dceb5d6e> (last visited December 22, 2019)

⁸ Ciuriak supra note 6

⁹ Internet World Statistics, *Philippines internet usage, population statistics and Facebook subscribers*, available at <https://www.internetworldstats.com/asia.htm#ph> (last visited 4 January 2020) [IWS - PH]

¹⁰ Internet World Statistics, *Top 20 countries with the highest number of internet users*, available at <https://www.internetworldstats.com/top20.htm> (last visited 3 January 2020) [IWS - Global]

¹¹ *Id.*, at 40.

¹² *Id.*, at 77.

¹³ *Id.*, at 79.

In order to reach consumers, knowledge-based, data-driven enterprises employ advertising and marketing strategies on social media platforms. In the Philippines, the total advertising audience on Facebook is 75 million; on Instagram, 11 million; and on Twitter, 5.08 million.¹⁴ Hence, there is a strong incentive for advertisers and marketers to channel their efforts online.¹⁵ 25% of Facebook pages use paid media to boost their content.¹⁶ By 2020, the digital advertising expenditure share of total media ad spending in the Philippines is estimated to be 24.2% of total media ad spending.¹⁷

The prevalence of advertisements has resulted in the desire to insulate oneself from the reach of advertising, as 50% of Filipino internet users use ad-blocking tools to prevent the display of advertising content.¹⁸ 38% of Filipino users employ the use of Virtual Private Networks (VPN).¹⁹ Growing concerns on fake news, hacking, privacy, and the misuse of data lead to a decrease in consumer trust in social media and an increase in consumer trust in experts, journalists and immediate circles on social media.²⁰

While businesses and other large institutions do indeed have economic interests involved in the collection and processing of data, the danger is in unduly encroaching on the right to privacy and right to data protection.²¹ Hence, a proper balance must be struck between such interests.²² Under the current framework of personal data, there

¹⁴ We are Social, *Digital in 2019 Philippines report*, available at <https://www.slideshare.net/DataReportal/digital-2019-philippines-january-2019-v01>, at 34 (last visited 8 January 2020)

¹⁵ We Are Social, *Digital in 2019 global report*, available at <https://wearesocial.com/uk/digital-2019>, at 37 (last visited 2 January 2020)

¹⁶ *Id.*, at 39

¹⁷ Sanchez, M.J. (2019). *Digital advertising expenditure share of total media ad spending in the Philippines from 2015-2020*, available at <https://www.statista.com/statistics/771570/digital-ad-spending-share-of-total-media-ad-spending-philippines/> (last visited 4 January 2020)

¹⁸ We are Social *supra* note 14, at 58

¹⁹ *Id.*, at 29.

²⁰ *Id.*, at 145; Hootsuite, *Social media trends 2019*, available at <https://www.digitalmarketingcommunity.com/researches/social-media-trends-2019-hootsuite/> (last visited 8 January 2020)

²¹ McFarland, M. (2012). *Privacy and balancing institutional power with individual freedom*. Markkula Center for Applied Ethics, Santa Clara University, available at <https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/privacy-and-balancing-institutional-power/> (last visited 8 January 2020)

²² European Union Agency for Fundamental Human Rights, *Handbook on European Data Protection Law 2018 Edition*, available at <http://fra.europa.eu/en/publication/2018/handbook-european->

is an imbalance in favor of knowledge-based, data-driven enterprises, and against individual rights, which now necessitates a new approach in providing legal protection - from the traditional privacy protection regime to a wider, expanded protection under property law.²³

A review of literature shows there are two perspectives: Those who advocate the use of property rights to protect privacy online²⁴, and those who oppose the propertization of personal information²⁵. The study proposes a two-tiered approach to personal information, an approach that harmonizes the two viewpoints. The first tier involves *personal information outside the commerce of man*; hence, not property which may be contracted out. The second tier involves *personal information within the commerce of man*; hence, property which may be contracted out.

B. Research Question and Thesis Statement

Given that the proper balance must be struck between business interests and individual privacy,²⁶ the study poses the following:

In the age of surveillance capitalism, how can the right to privacy (and corollarily, the right to data protection) be effectively enforced in a way that promotes liberty and nurtures prosperity for the everyday Filipino?

The author submits the following hypothesis:

Data-protection-law, at p. 79 (last visited 8 January 2020) [Handbook on European Data Protection]

²³ Karanasiou, A.P and Douilhet, E., (2016). *Never mind the data: The legal quest over control of information and the networked self*. 100-105. 10.1109/IC2EW.2016.39.

²⁴ Kenneth C. Laudon, *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept. 1996, at 92; Lessig, L., *Code and Other Laws of Cyberspace*, 142-63 (1999); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, II BERKELEY TECH. L.J. 1, 26-41 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2385 (1996);

²⁵ Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423-28 (2000); Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 750-57 (1999); Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1551 (2000); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. s, 92-97

²⁶ Handbook on European Data Protection supra note 23, at p. 79

To approach digital footprint in the context of property and property rights, in that the everyday Filipino is adequately compensated for his or her privacy loss and the wealth of the digital economy is more equitably distributed

C. Objectives

In the course of the research, this paper aims to achieve the following:

1. To compare and contrast the right to privacy and right to data protection
2. To classify digital footprints using relevant and existing laws and cases
3. To establish a legal framework in approaching the two tiers of digital footprints in the context of commerce

D. Significance

The current paradigm of data consumption is dominated by knowledge-based, data-driven enterprises, which have, for the most part, profited from the (mis)use of the digital footprints, bringing to the fore concerns on violations of the right to privacy and right to data protection of digital natives and digital immigrants alike.

The author submits that the paradigm shift proposed in this research as a combination of the two approaches to digital footprint has a concrete role in strengthening liberty and prosperity under the rule of law.

E. Research Methodology

The following sources and research methods shall be employed to achieve the objectives:

1. To survey existing laws and cases related to the right to privacy and the right to data protection

2. To survey existing laws and cases to establish legal framework in approaching the two tiers of digital footprints in the context of property
3. To survey existing laws and cases to exact accountability from knowledge-based, data-driven enterprises

F. Scope and Limitations

The focus of this study is the right to privacy and the right to personal data protection, in the context of economic prosperity. Hence, it will not delve into the corollarily topics of freedom of expression in its relation with the right to privacy and right to data protection online. Moreover, this study focuses on the relationship of individuals with commercial enterprises, and not with state actors.

II. RIGHT TO PRIVACY AND RIGHT TO PERSONAL DATA PROTECTION

A. Right to privacy

1. Right to privacy in international law

In 1948, the United Nations General Assembly adopted the Universal Declaration of Human Rights (UNDR)²⁷, a landmark document which enshrines the fundamental human rights that must be universally protected.²⁸

Privacy is defined as “a private sphere with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals”.²⁹ Corollary to privacy are the concepts of privacy, security, and anonymity of communications.³⁰

International human rights law provides the legal framework by which interferences with the right to privacy is assessed.³¹ The right to privacy is a fundamental human right, enshrined in various declarations and treaties:³²

1. Article 12 of the Universal Declaration of Human Rights³³
2. Article 17 of the International Covenant on Civil and Political Rights³⁴

²⁷ UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at: <https://www.refworld.org/docid/3ae6b3712c.html> [accessed 22 December 2019] [UDHR]

²⁸ Conrad, A. (2018). *The right to privacy under Philippine and international law*, available at <https://www.privacyph.net/2018/06/12/the-right-to-privacy-under-philippine-and-international-law/> (last visited 10 January 2020)

²⁹ United Nations Human Rights Council. *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 30 June 2014, A/HRC/27/37, para. 22 [30 June 2014 Right to Privacy Report]

³⁰ UN Human Rights Council, *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17 April 2013, A/HRC/23/40, para. 23

³¹ 30 June 2014 Right to Privacy Report supra note 30, para. 12.

³² *Id.*, para. 20.

³³ UDHR supra note 28, art. 12

³⁴ UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: <https://www.refworld.org/docid/3ae6b3aa0.html> [accessed 13 January 2020] [ICCPR]

3. Article 16 of the Convention on the Rights of the Child³⁵
4. Article 14 of the International Convention on the Protection of All Migrant Workers and Members of Their Families³⁶
5. Article 8 of the European Convention on Human Rights³⁷; and
6. Article 11 of the American Convention on Human Rights³⁸

Article 12 of the Universal Declaration of Human Rights provides: *"No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."*³⁹

As the UNDR is not legally binding on state parties⁴⁰, two treaties were created for the purpose of codifying human rights: the International Covenant on Civil and Political Rights (ICCPR)⁴¹ and the International Covenant on Economic, Social and Cultural Rights (ICESCR).

In almost identical phraseology with the UDHR, the right to privacy is enshrined in Article 17 of the ICCPR:

³⁵ UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, available at: <https://www.refworld.org/docid/3ae6b38f0.html> [accessed 14 January 2020]

³⁶ UN General Assembly, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, 18 December 1990, A/RES/45/158, available at: <https://www.refworld.org/docid/3ae6b3980.html> [accessed 14 January 2020]

³⁷ Council of Europe: European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life*, 31 December 2016, available at: <https://www.refworld.org/docid/5a016ebe4.html> [accessed 21 December 2019] [ECHR Guide]

³⁸ Organization of American States (OAS), *American Convention on Human Rights, "Pact of San Jose"*, Costa Rica, 22 November 1969, available at: <https://www.refworld.org/docid/3ae6b36510.html> [accessed 22 December 2019] [ACHR]

³⁹ UDHR supra note 28, art. 12

⁴⁰ Tomuschat, C. (2008). *International Covenant on Civil and Political Rights*. United Nations Audiovisual Library of International Law, available at https://legal.un.org/avl/pdf/ha/iccpr/iccpr_e.pdf (last visited 10 January 2020)

⁴¹ ICCPR supra note 35, art 17.

“No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Everyone has the right to the protection of the law against such interference or attacks.”⁴²

General Comment No. 16⁴³ provides that the negative obligation in paragraph 1 of Article 17 consists in “a duty themselves not to engage in interferences inconsistent with Article 17 of the Covenant”,⁴⁴ while the positive obligation in paragraph 2 consists in guaranteeing that the right is respected⁴⁵, and providing the legislative framework prohibiting interferences.⁴⁶

The right to privacy is a qualified right⁴⁷, hence a two-tiered evaluation must first be made: first, whether or not the interference involves a right within the coverage of Article 17⁴⁸; and second, whether or not the interference is arbitrary or unlawful⁴⁹.

Similar to the limitations tests in the right to freedom of movement⁵⁰ and the right to freedom of expression⁵¹, any interference with the right to privacy, must comply accordingly:

⁴² *Ibid.*

⁴³ UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation, 8 April 1988, available at: <https://www.refworld.org/docid/453883f922.html> [accessed 21 December 2019] [General Comment 16]

⁴⁴ *Ibid* at para 9.

⁴⁵ *Ibid* at para 2.

⁴⁶ *Ibid* at para 9.

⁴⁷ American Civil Liberties Union. (2014). *Privacy rights in the digital age: A proposal for a new General Comment on the right to privacy under Article 17 of the International Covenant on Civil and Political Rights*, available at <https://www.aclu.org/other/human-right-privacy-digital-age> [accessed 13 January 2020] [ACLU Report]

⁴⁸ *Ibid.*

⁴⁹ ACLU Report, *supra* note 47 at p. 4.

⁵⁰ UN Human Rights Committee (HRC), CCPR General Comment No. 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9, available at: <https://www.refworld.org/docid/45139c394.html> [accessed 14 January 2020] [General Comment 27]

⁵¹ UN Human Rights Committee (HRC), CCPR General Comment No.34: Article 19 (Freedom of opinion and expression), 21 July 2011, available at: <https://www.refworld.org/docid/4e38efb52.html> [accessed 14 January 2020]

1. Any restrictions must be provided by the law⁵²
2. The essence of a human right is not subject to restrictions⁵³
3. Restrictions must be necessary in a democratic society⁵⁴
4. Any discretion exercised when implementing the restrictions must not be unfettered⁵⁵
5. It must be necessary for reaching the legitimate aim⁵⁶
6. Restrictive measures must conform to the principle of proportionality⁵⁷

Article 16 of the Convention on the Rights of the Child is a faithful reproduction of Article 17 of the ICCPR.⁵⁸ Article 14 of the International Convention on the Protection of All Migrant Workers and Members of Their Families is likewise substantially similar to Article 17 of the ICCPR.⁵⁹

The right to privacy also appears in regional declarations and treaties. Specifically, Article 8 of the European Convention on Human Rights (ECHR) provides:

“Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of his right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”⁶⁰

⁵² General Comment 27 supra note 51

⁵³ *Ibid*, at para 13

⁵⁴ *Ibid*, at para 11

⁵⁵ *Ibid*, at para 13

⁵⁶ *Ibid*, at para 14 [

⁵⁷ *Ibid*, at paras 14-15

⁵⁸ UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, available at: <https://www.refworld.org/docid/3ae6b38f0.html> [accessed 14 January 2020]

⁵⁹ UN General Assembly, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, 18 December 1990, A/RES/45/158, available at: <https://www.refworld.org/docid/3ae6b3980.html> [accessed 14 January 2020]

⁶⁰ Bygrave, L.A. (1998). *Data protection pursuant to the right to privacy in human rights treaties*. *International Journal of Law and Information Technology*, volume 6, pp. 247-284; *Deklerck v*

Similar to Article 17 of the ICCPR, Article 8 is divided into two parts. The first paragraph of Article 8 sets out the precise rights, while the second paragraph provides the grounds for interference.⁶¹ Hence, Article 8 of the ECHR involves a two stage inquiry, of whether the right is protected by Article 8, and whether the interference of such right is permissible.⁶²

Article 11 of the Inter-American Convention on Human Rights is similarly phrased with the ICCPR, while the right to privacy does not feature in the African Charter of Human and Peoples' Rights.⁶³

a. Right to privacy in Philippine law
i. Right to privacy in the 1987 Philippine Constitution

The right to privacy enshrined in Article 17 of the ICCPR, ratified by the Philippines in 1986, form part of municipal law through the doctrine of incorporation, as per Section 2, Article II of the 1987 Philippine Constitution.⁶⁴ The right to privacy is also protected under Section 11, Article II of the Constitution, which provides that "the State values the dignity of every human person and guarantees full respect for human rights".⁶⁵

The right to privacy of communication and correspondence is enshrined in the Constitution, under Article III, Section 3(1), which provides: "*The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.*"⁶⁶

Belgium (1980), Application No 8307/78, 21 Decisions and Reports of the European Commission of Human Rights, 116, 124.

⁶¹ Kirkelly, U. (2003). *The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights*. Human Rights Handbook Series of the Council of Europe, p. 6.

⁶² *Ibid*, at p. 9.

⁶³ Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), available at: <https://www.refworld.org/docid/3ae6b3630.html> [accessed 21 December 2019]

⁶⁴ CONST. (1987), art. 2, sec. 2.

⁶⁵ CONST. (1987), art. 2, sec. 11

⁶⁶ CONST. (1987), art. 3, sec. 1, par (3)

Surveillance of communications may be limited by Section 10, Article XVI of the Constitution, which provides that “the State shall provide the policy environment for the full development of Filipino capability and the emergence of communication structures suitable to the needs and aspirations of the nation”.⁶⁷

2. Right to privacy in the New Civil Code

Under Article 26 of the New Civil Code of the Philippines (NCC), the act of meddling with or disturbing the private life of another produces a cause of action in the form of damages, prevention and other relief.⁶⁸ Article 723 of the NCC provides that letters and other private communications in writing can only be published or disseminated with the consent of the writer or his heirs, or with the authorization of the court for their publication or dissemination on the grounds of public safety or the interest of justice.⁶⁹

3. Right to privacy in the Revised Penal Code

Article 229 of the Revised Penal Code (RPC) holds criminally liable any public officer who reveals any secret known to him or wrongfully delivers papers or copies of papers of which he may have charge and which should not be published.⁷⁰ Article 280 of the RPC criminalizes the entering of the dwelling of another against the latter’s will.⁷¹ Article 290 of the RPC provides that any private individual who seizes papers or letters to reveal the contents is criminally liable.⁷² Article 291 of the RPC criminalizes the revelations of the secrets of the principal or master.⁷³ Article 292 of the RPC criminalizes the revelation of the industrial secrets of the owner of any manufacturing or industrial establishment.⁷⁴

⁶⁷ CONST. (1987), art. 16, sec. 10

⁶⁸ CIVIL CODE, art. 26

⁶⁹ CIVIL CODE, art. 723

⁷⁰ REV. PEN. CODE, art 229

⁷¹ REV. PEN. CODE, art 280

⁷² REV. PEN. CODE, art 290

⁷³ REV. PEN. CODE, art 291

⁷⁴ REV. PEN. CODE, art 292

4. Right to privacy in special laws

Section 35 of the Electronics Engineering Law of 2004 (RA 9292) provides that registered electronics engineers and technicians may be imprisoned, or fined, or both for involvement in forms of unauthorized and malicious electronic eavesdropping and/or the use of any electronic devices.⁷⁵

Section 1 of RA 4200 or the Anti-Wiretapping Act of 1965 penalizes the wiretapping of any device done by any person to secretly overhear, intercept, or record any private communication or spoken word of another person or persons without the authorization of all the parties to the communication⁷⁶, except when pursuant to a court order and compliant with all conditions under the law.⁷⁷

Other special laws sanction the surveillance of communications for narrowly tailored circumstances, such as in Section 16(g) of the Expanded Anti-Trafficking in Persons Act of 2012 or Republic Act No. 9208, as amended by Republic Act No. 10364⁷⁸, Section 7 of Republic Act No. 9372 or the Human Security Act of 2007⁷⁹, and Section 9 of the Anti-Child Pornography Act of 2009 (RA 9775).⁸⁰

Rule 130, Sections 24⁸¹ and 25⁸² of the Rules of Court disqualifies certain privileged information from being admissible as evidence.

2. Right to data protection

a. Right to data protection in international law

Article 12 of the UDHR⁸³ and Article 17 of the ICCPR⁸⁴ protects everyone from arbitrary or unlawful interferences with their privacy,

⁷⁵ R.A. 9262, sec. 35

⁷⁶ R.A. 4200 or Anti Wiretapping Law, sec. 1

⁷⁷ R.A. 4200 or Anti Wiretapping Law, sec. 3

⁷⁸ R.A. No. 9208, as amended by R.A., 10364 or the Expanded Anti-Trafficking in Persons Act of 2012, Section 16(g)

⁷⁹ R.A. No. 9372 or the Human Security Act of 2007, sec. 7

⁸⁰ R.A. No. 9775 or Anti-Child Pornography Act of 2009, sec. 9

⁸¹ RULES OF COURT, Rule 130, sec 24

⁸² RULES OF COURT, Rule 130, sec 25

⁸³ UDHR supra note 28

⁸⁴ General Comment 16 supra note 44

family, home, or correspondence. While the right to data protection is not expressly provided in the ICCPR, it is however deemed an adjunct to the right to privacy.⁸⁵ The UN Human Rights Committee interprets the provisions on the right to privacy to include the right to data protection.⁸⁶

In contrast, Article 8 of the Charter of Fundamental Rights of the European Union (EU Charter) enshrines the right to data protection as a separate and distinct right⁸⁷:

“Everyone has the right to the protection of personal data concerning him or her.

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Compliance with these rules shall be subject to control by an independent authority.”⁸⁸

Superseding Data Protection Directive 95/46/EC⁸⁹, gold standard for data protection law is the General Data Protection Regulation, aiming to both unify data privacy and protection laws and give control to individuals over their personal data.⁹⁰ Article 4 of the GDPR provides that personal data means “information relating to

⁸⁵ *Ibid.*

⁸⁶ UN Human Rights Council, *The right to privacy in the digital age*, 24 March 2015, available at <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G15/061/64/PDF/G1506164.pdf?OpenElement> [accessed 14 January 2020]; ACLU Report *supra* note 47 at p. 31.

⁸⁷ Lynskey, O. (2014) “DECONSTRUCTING DATA PROTECTION: THE ‘ADDED-VALUE’ OF A RIGHT TO DATA PROTECTION IN THE EU LEGAL ORDER,” *International and Comparative Law Quarterly*. Cambridge University Press, 63(3), pp. 569–597. doi: 10.1017/S0020589314000244.

⁸⁸ European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, available at: <https://www.refworld.org/docid/3ae6b3b70.html> [accessed 14 January 2020]

⁸⁹ Directive 95/46/EC of 24 October 1995, European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995, p. 31

⁹⁰ Zuiderveen Borgesius, Frederik J. (April 2016). "Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection Regulation". *Computer Law & Security Review*. doi:10.1016/j.clsr.2015.12.013. ISSN 0267-3649;

an identified or identifiable natural person”⁹¹. Under the GDPR, the main actors include the data subjects, or those natural persons whose personal data are processed⁹², controllers, or those who determine the means and purposes of such processing of personal data⁹³, processors, or those who do something with respect to personal data for controllers, and data protection authorities⁹⁴.

b. Right to data protection in Philippine law.

1. Data Privacy Act

The Data Privacy Act of 2012 (DPA) is the Philippines’ first data privacy law.⁹⁵ The DPA requires entities to both observe the data privacy principles⁹⁶ as laid out in the law, and to uphold the rights⁹⁷ of the data subject.

Under the DPA, there are four general principles in the collection and processing of personal data: the principles of transparency⁹⁸, legitimate purpose⁹⁹, proportionality¹⁰⁰, and data quality¹⁰¹. Each data subject also has the following rights under the DPA: the right to be informed¹⁰², the right to object¹⁰³, the right to access¹⁰⁴, the right to rectification¹⁰⁵, erasure¹⁰⁶ or blocking¹⁰⁷, the right to damages¹⁰⁸, and the right to data portability¹⁰⁹.

⁹¹ GDPR, art 4(1)

⁹² GDPR art 4(1).

⁹³ GDPR art 4(7).

⁹⁴ GDPR art 4(8).

⁹⁵ RA 10173, Sec 2; Asian Business Law Institute. (2018). *Regulation of cross-border transfers of personal data in Asia: Jurisdictional report of the Republic of the Philippines*, p. 278, para 1.

⁹⁶ RA 10173, Sec 11

⁹⁷ RA 10173, Sec 16

⁹⁸ IRR of RA 10173, Sec 18(a)

⁹⁹ IRR of RA 10173, Sec 18(b)

¹⁰⁰ IRR of RA 10173, Sec 18(c)

¹⁰¹ IRR of RA 10173, Sec 19(c)

¹⁰² RA 10173, Sec 16(a); IRR of RA 10173, Sec. 34(a)

¹⁰³ IRR of RA 10173, Sec. 34(b)

¹⁰⁴ RA 10173, Sec 16(c); IRR of RA 10173, Sec. 34(c)

¹⁰⁵ RA 10173, Sec 16(d); IRR of RA 10173, Sec 34(d)

¹⁰⁶ RA 10173, Sec 16(e); IRR of RA 10173, Sec 34(e)

¹⁰⁷ RA 10173, Sec 16(e); IRR of RA 10173 Sec. 34(e)

¹⁰⁸ RA 10173, Sec 16(f); IRR of RA 10173, Sec 34(f)

¹⁰⁹ RA 10173, Sec 18; IRR of RA 10173, Sec 36

2. Other special laws

Section 13 of R.A. No. 2000 or the Electronic Commerce Act of 2000 authorizes data retention under specific grounds and tasks agencies to ensure the integrity and reliability of electronic documents.¹¹⁰

Section 1 of Memorandum Circular No. 04-06-2007 of the National Telecommunications Commission requires that public telecommunications entities retain the call data records on voice calls and similar records for non-voice traffic.¹¹¹

Republic Act No. 10175 or the Cybercrime Prevention Act authorizes the interception of communications¹¹², the disclosure¹¹³ of computer data, and the preservation¹¹⁴ of computer data.

Section 17 of Republic Act. No. 11055 or the Philippine Identification System Act prohibits the unlawful disclosure of information of registered individuals under the system, or giving access or copies of such information to third parties, except under specific circumstances under the law.

Other special laws in the financial sector, restrict the disclosure of certain types of information¹¹⁵, such as in Section 2 of Republic Act No. 1405 or the Law on Secrecy of Deposits¹¹⁶, Section 8 of Republic Act No 6426 or the Foreign Currency Deposit Act¹¹⁷, Rule 9.C.3 of the Revised Rules and Regulations Implementing Republic Act No 9160 or the Anti Money-Laundering Act of 2001¹¹⁸, Section 6 of Republic

¹¹⁰ RA 2000, sec. 13

¹¹¹ National Telecommunications Commission, Memorandum Circular No. 04-06-2007, sec. 1

¹¹² RA 10175, sec. 3(m)

¹¹³ RA 10175, sec. 14

¹¹⁴ RA 10175, sec. 13

¹¹⁵ Asian Business Law Institute Report supra note 97

¹¹⁶ RA 1405, Sec 2

¹¹⁷ RA 6426, Sec. 8

¹¹⁸ IRR of RA 9160, Rule 9.C.3

Act No 9510 or the Credit Information System Act¹¹⁹, Subsection X501.7 of the Manual of Regulations for Banks (2017),¹²⁰

¹¹⁹ RA 9510, Sec. 6

¹²⁰ Manual of Regulations for Banks, Sec. X501.7

III. THEORETICAL JUSTIFICATIONS

This study proposes a new approach in the treatment of personal data, in the nature of an expansion from the traditional privacy protection regime to one under property law. In light of this, this study proposes a two-tiered approach: The first tier involves *personal information outside the commerce of man*. The second tier involves *personal information within the commerce of man*.

A. Personal information as outside the commerce of man

1. Personhood theory justifications

The right to privacy is an adjunct to the right to be left alone, a right so fundamental and basic that it emanates from the person himself or herself.¹²¹ Focusing on the “intrinsic worth” of the human person, the person is “valuable above all price”.¹²² The principle of inviolate personality¹²³ posits that the right to privacy is one so interwoven with one’s personhood and inherent to human dignity.¹²⁴

An inviolate personality involves the independence, dignity, and integrity of the individual, which “defines man’s essence as a unique and self-determining being”¹²⁵ Any injury is a violation “of our individuality, of our dignity as individuals, and the legal remedy represents a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered.”¹²⁶

¹²¹ Florencio, Patrik S. and Ramanathan, Erik D. (2001). *Secret Code: The Need for Enhanced Privacy Protections in the United States and Canada to Prevent Employment Discrimination Based on Genetic and Health Information*. Osgoode Hall Law Journal 39.1: 77-116.

¹²² Rachels, J. (1986). *Kantian Theory: The Idea of Human Dignity*. *The Elements of Moral Philosophy*, 114-117, 122-123.

¹²³ Warren, S.D. and Brandeis, L.D.. (1890). *The Right to Privacy*. *Harvard Law Review*, Vol. 4, No. 5; 193-220.

¹²⁴ Craven, J.B. Jr., (1976). *Personhood: The Right to be Let Alone*. *Duke L.J.* 699; J.H. Reiman, (1977). *Privacy, Intimacy, and Personhood*. 6 *Phil. & Pub. Aff.* 26;

¹²⁵ Bloustein, E.J. (1964). *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*. 39 *N.Y.U. L. Rev.* at 971.

¹²⁶ *Ibid* at 1003.

B. Personal information within the commerce of man

i. Incentive theory justifications

Values in the form of incentives or reasons are the driving force for the engagement in a particular activity.¹²⁷ It is posited that “a right in personal information would not only grant more control over the use of information by companies to the individual but also lead to economic compensation for the use of that information”¹²⁸ In such a *quid pro quo* arrangement, personal information is disclosed and in exchange of which, there is monetary compensation for its disclosure commensurate to the loss of privacy.¹²⁹ Hence, individuals would be more willing to disclose certain personal information, leading to accelerated growth in the information market.¹³⁰

ii. Natural rights justification

Under the entitlement theory, a person’s holdings are just, if acquired through the following modes: (1) just original acquisition¹³¹ or (2) just transfer¹³² or (3) through rectification of injustices¹³³ to original acquisition or transfer.¹³⁴

Here, what is protected is the right of an individual to the product of one’s labour and the corollarily protection against unjust enrichment by competitors.¹³⁵ Hence, the harm contemplated the loss

¹²⁷ Lai, E.R. (2011). *Motivation: A Literature Review*. Research report, available at http://images.pearsonassessments.com/images/tmrs/Motivation_Review_final.pdf [accessed 2 February 2020]

¹²⁸ Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 *GEO. L.J.* 2381, 2385 (1996);

¹²⁹ Vishwajith, A.S. and Varanasi, S. (2012) *I am mine or am I? Analyzing the need for a property right in personal information*. *Indian Journal of Intellectual Property Law*. 5, 106, available at <http://www.commonlii.org/in/journals/INJIPLaw/2012+/9.pdf> [accessed 1 January 2020]

¹³⁰ Kenneth C. Laudon, *Markets and Privacy*, *COMMUNICATIONS OF THE ACM*, Sept. 1996, at 92; Lessig, L., *Code and Other Laws of Cyberspace*, 142-63 (1999)

¹³¹ *Ibid*, at 2

¹³² *Id*

¹³³ *Id*

¹³⁴ Salahuddin A (2018) *Robert Nozick’s Entitlement Theory of Justice, Libertarian Rights and the Minimal State: A Critical Evaluation*. *J Civil Legal Sci* 7: 234. doi: 10.4172/2169-0170.1000234

¹³⁵ Bloustein supra note 127

of control by the individual of his own personal information, in the form of unjust enrichment.¹³⁶

¹³⁶ Vishwajith, A.S. and Varanasi, S. *supra* note 131

IV: DUAL APPROACH TO THE TREATMENT OF PERSONAL INFORMATION

A. Personal information outside the commerce of man

1. Conflict of laws

Approaching digital footprint necessitates a discussion of what legal system should apply, considering the ubiquitous nature of cyberspace.¹³⁷ Conflict of laws is “that part of the law of each state or nation which determines whether, in dealing with a legal situation, the law of some other state or nation will be recognized, given effect, or applied”.¹³⁸ With regard to the first tier of personal information, the nationality principle applies, enshrined in Article 15 of the NCC.¹³⁹ Hence, regardless of where a Filipino might be, that Filipino will be governed by Philippine law.¹⁴⁰ The ability of a person to act with legal effect is determined by personal law, and such capacity attaches to such legal status follows the individual wherever the person goes.¹⁴¹ It is submitted that, in the context of personal information, the ability of an individual to act with legal effect is determined by Philippine law.

2. Domestic laws

a. Personal information outside the commerce of man

Section 3(j) of the Data Privacy Act of 2012 (DPA) provides that *personal data* “refers to all types of personal information”. DPA further classifies data into 3 types: personal information¹⁴², sensitive personal information¹⁴³, and privileged information¹⁴⁴. Section 3(g) of the DPA provides that *personal information* “refers to any information whether recorded in a material form or not, from which the identity

¹³⁷ Schau, Terry. *Internet Use: Here, There, and Everywhere*. Occupational Outlook Quarterly, v44 n4 p40-47 Win 2000-2001

¹³⁸ Coquia, J.R. and Aguilin-Pangalangan, E. (2000). Conflict of laws: Cases, materials and comments. Central Book Supply Inc. Quezon City

¹³⁹ CIVIL CODE; art. 15.

¹⁴⁰ Perez v. CA, G.R. No. 162580, January 27, 2006; Coquia, J.R. and Aguilin-Pangalangan, E. supra note 140

¹⁴¹ Perez v. CA, G.R. No. 162580, January 27, 2006

¹⁴² RA 10173, Sec 3(j)

¹⁴³ RA 10173, Sec 3(l)

¹⁴⁴ RA 10173, Sec 3(k)

of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual”.¹⁴⁵

While the DPA does not further classify personal information, the Cybercrime Prevention Act of 2012 (CPA) classifies personal information: subscriber information, traffic data, and content data. Section 3(o) of the CPA provides that *subscriber’s information* “refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which identity can be established.”¹⁴⁶

Section(p) of the CPA provides that *traffic data* or *non-content data* “refers to any computer data other than the content of the communication including, but not limited to, the communication’s origin, destination, route, time, date, size, duration, or type of underlying service”.¹⁴⁷

Section 3 of the IRR of the Cybercrime Prevention Act provides that *content data* is “the communication content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data”.¹⁴⁸

In the processing of personal information, Section 3(j) of the DPA provides that *processing* “refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data” (emphasis supplied). Section 12 of the DPA provides the criteria for lawful processing of *personal information*.¹⁴⁹ Section 13 of the DPA provides the exclusive cases

¹⁴⁵ RA 10173, Sec 3(g); IRR of RA 10173, Sec 3(l)

¹⁴⁶ R.A. No. 10175, Section 3(o)

¹⁴⁷ R.A. No. 10175, Section 3(p)

¹⁴⁸ IRR of RA 10175, Section 3

¹⁴⁹ RA 10173, Section 12

wherein processing of sensitive personal information and privileged information are permitted.¹⁵⁰ Hence, for these specific purposes, information of the abovementioned classifications may still be legally processed.

Specific to data enterprises, personal information is processed on the basis of contract through the acquisition of consent evidenced by assent to terms and conditions and the use of the platform. It is however submitted that certain types of personal information may not be processed on the ground of consent and cannot be contracted out, as by the very nature of such personal information, they are not strictly speaking property.

Property refers to a mass of things or objects which are useful to human activity and integral to human life.¹⁵¹ Things are only those which can give some good or utility to man and which can be the object of juridical relations.¹⁵² Hence, in order to be juridically considered as a *thing* or *property*, “an object must have the following requisites:

1. utility, or the capacity to satisfy human wants,
2. individuality and substance, or a separate and autonomous existence, and
3. susceptibility of being appropriated”.¹⁵³

The World Economic Forum 2016 report entitled “A Blueprint for Digital Identity” provides that *digital identity* is a collection of information that describes an entity, categorized into 3 main groups: *inherent attributes* or “attributes that are intrinsic to an entity and are not defined by relationships to external entities, such as age and date of birth”, *accumulated attributes* or “attributes that are gathered or developed over time, which may change multiple times or evolve throughout an entity’s lifespan, such as preferences and behaviors through telephone metadata”, and *assigned attributes* or “attributes

¹⁵⁰ RA 10173, Section 13

¹⁵¹ 2 Arturo M. Tolentino, Commentaries and jurisprudence on the Civil Code of the Philippines, 1, 1 (2004)

¹⁵² *Id*, at 2, 2 (2004)

¹⁵³ *Id*, at 3, 2 (2004)

that are attached to the entity, which can change and are reflective of relationships the entity holds with other bodies, such as telephone number and email address” (emphasis supplied).¹⁵⁴

Applying the elements of a thing, *inherent attributes* and *assigned attributes* do not comply with the requisites of individuality and susceptibility of being appropriated. *Inherent attributes* are intrinsic to a data subject and *assigned attributes* are attached to the data subject, more in accord with a state of being or an incident of such, and hence cannot have a separate and autonomous existence apart from the data subject. Moreover, both are not susceptible of appropriation because pursuant to the principle of inviolate personality¹⁵⁵, the integrity of a person makes certain rights so interwoven with one’s personhood that they are inherent to human dignity.¹⁵⁶ Our human senses are extended through technology and extends the various ways in which people may represent themselves.¹⁵⁷ Hence, just as a shovel may be an extension of one’s hands or a microscope extends one’s vision¹⁵⁸, *inherent attributes* and *attached attributes* may be seen as extensions of the human body itself or an expression of one’s personhood in online platforms.

The quintessential example of one which is not within the commerce of man is the living human body.¹⁵⁹ Upon death, the corpse becomes a thing, although it is not susceptible of appropriation and commerce by reason of public morality and cannot be the subject matter of an onerous contract.¹⁶⁰ Emphasizing the intrinsic worth of the human person, making them “valuable above all price”¹⁶¹, personal information in the form of *inherent* or *attached attributes* are not *things* or *property*.

¹⁵⁴ World Economic Forum 2016 Report. A Blueprint for Digital Identity, available at http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf [accessed 4 April 2020]

¹⁵⁵ Warren et al supra note 125

¹⁵⁶ Craven supra note 126

¹⁵⁷ Belk, R. (2016). Extended self and the digital world. *Current Opinion in Psychology*, volume 10, 55-54

¹⁵⁸ McLuhan, M. (1964). *The Medium is the Message: Understanding Media: The Extensions of Man*, <https://web.mit.edu/allanmc/www/mcluhan.mediummessage.pdf> [accessed 19 February 2020]

¹⁵⁹ *Id*, at 3, 4 (2004)

¹⁶⁰ *Id*, at , 4, 1 (2004)

¹⁶¹ Rachels supra note 124

2. Effect on contracts

A contract is an agreement on the declaration of a common will.¹⁶² Article 1305 of the NCC provides the definition of a contract in our jurisdiction.¹⁶³ Article 1318 of the Civil Code states that consent, object and cause are the essential requisites of a contract.¹⁶⁴ Hence, contracts involving personal information in the nature of *inherent attributes* and *attached attributes* are accordingly void for want of a valid object and cause.

The object of a contract is the thing, right, or service which is the object of the obligation itself.¹⁶⁵ In order for such thing to be the object of a contract, the following must concur:

1. Article 1347¹⁶⁶ provides that the object must be within the commerce of man
2. Article 1347 provides that it must be licit, or not contrary to law, morals, good customs, public policy or public order
3. Article 1348¹⁶⁷ states that it must be possible; and
4. Article 1349¹⁶⁸ states that it must be determinate as to its kind.¹⁶⁹

Personal information in the nature of *inherent attributes* and *attached attributes* do not comply with the requisite of being within the commerce of man, and being a licit object. As to object, Article 1347 of the Civil Code provides that things which are outside the commerce of men may not be the object of contracts.¹⁷⁰ *Things* or *property* outside the commerce of men are those which are not susceptible to appropriation or private ownership.¹⁷¹ Among those things which are

¹⁶² Edilberto Alcantara v Cornelio B. Rita, Jr., G.R. 136996, December 14, 2001

¹⁶³ CIVIL CODE, art. 1305

¹⁶⁴ CIVIL CODE, art. 1318

¹⁶⁵ 4 Arturo M. Tolentino, Commentaries and jurisprudence on the Civil Code of the Philippines, 520, 1 (2002)

¹⁶⁶ CIVIL CODE, art. 1347

¹⁶⁷ CIVIL CODE, art. 1348

¹⁶⁸ CIVIL CODE, art. 1349

¹⁶⁹ 4 Arturo M. Tolentino supra note 167, at 520, 2 (2002)

¹⁷⁰ CIVIL CODE, art. 1347

¹⁷¹ Land Bank v. Republic, G.R. No. 150824, February 4, 2008; Republic v. Court of Appeals, G.R. No. 126316, June 25, 2004;

outside the commerce of man are “services which imply an absolute submission by those who render them sacrificing their liberty, their independence, or beliefs or disregarding in any manner the equality and dignity of persons”.¹⁷² Falling into such classification, personal information of this nature falls outside the commerce of man.

Moreover, a contract is considered void if at the time the contract is entered into, it is illicit.¹⁷³ As earlier discussed, the intrinsic worth of the human person makes him or her valuable above all price¹⁷⁴, hence, personal information involving *inherent attributes* and *attached attributes* cannot be contracted out by reason of public policy.

Additionally, personal information involving *inherent attributes* and *attached attributes* cannot be contracted out, by want of a valid cause. The cause is the essential reason for the contracting parties to enter the contract¹⁷⁵, or the immediate, direct, and proximate reason which justifies the creation of an obligation.¹⁷⁶ Hence, the cause of a contract must exist, must be true, and must be licit.¹⁷⁷

As to cause, the cause is illicit or unlawful if it is contrary to law, morals, good customs, public order or public policy.¹⁷⁸ A contract is contrary to public policy if it contravenes some established interest of society or tends clearly to undermine the security of an individual’s rights.¹⁷⁹ In the same way that any alienation of a body part or a corpse is void for being contrary to public policy, the alienation of personal information of this nature, is unlawful for being contrary to public policy.

As to third party contracts (such as those entered by data controllers to advertisers and marketers) which have for its object personal information involving *inherent attributes* and *attached attributes*, they are also accordingly void. As per Article 1409 of the

¹⁷² *Id*, at 521, 2

¹⁷³ *Spouses Isagani Castro and Diosdada Castro v Angelina de Leon Tan, et al*, G.R. 168940, November 24, 2009; 4 Arturo M. Tolentino *supra* note 167, at 524, 3 (2002)

¹⁷⁴ *Rachels* *supra* note 124

¹⁷⁵ *Id*, at 529, 1 (2002)

¹⁷⁶ *General Enterprises, Inc. v Lianga Bay Logging Co.*, G.R. No L-18487, August 31, 1964

¹⁷⁷ 4 Arturo M. Tolentino *supra* note 167, at 531, 3 (2002)

¹⁷⁸ CIVIL CODE, art. 1352; *Liguez v Court of Appeals*, G.R. No. L-11240, December 18, 1957

¹⁷⁹ *Leal vs. Intermediate Appellate Court*, 155 SCRA 994 [1987]

Civil Code, a contract whose cause, object or purpose is contrary to law, morals, good customs, public order or public policy, or whose object is outside the commerce of men, is inexistent and void from the beginning.¹⁸⁰ Article 1422 of the Civil Code provides that a contract which is the direct result of a previous illegal contract, is also void and inexistent.¹⁸¹ Applying the same to contracts entered into by data controllers with advertisers and marketers, being the direct result of a previous illegal contract as aforestated, such third party contracts are also void.

¹⁸⁰ CIVIL CODE, art. 1409; *Arquero v. Hon. Flojo and RCPI*, G.R. No. 68111, December 20, 1988

¹⁸¹ CIVIL CODE, art. 1422; *Razon v. PPA*, G.R. No. 75197, 22 June 1987

B. Personal information within the commerce of man

1. Conflict of laws

Earlier on, it was discussed that approaching personal information necessitates a discussion of what legal system should apply.¹⁸² With regard to personal information involving *inherent attributes* and *attached attributes*, the nationality principle enshrined in Article 15 of the Civil Code¹⁸³ applies, in recognition of the fact that the ability of a person to act with legal effect is determined by personal law, and such capacity attached to such legal status follows the individual.¹⁸⁴ The same rationale may be applied involving the second tier of personal information in the form of *accumulated attributes* or “attributes that are gathered or developed over time, which may change multiple times or evolve throughout an entity’s lifespan, such as preferences and behaviors through telephone metadata”.¹⁸⁵

Similarly, even if the approach were taken from the perspective of choice of law in contracts, domestic law would still apply with respect to the intrinsic validity of such contracts.

As to extrinsic validity, our jurisdiction follows the principle of *lex loci celebrationis* in Article 17 of the NCC. Article 1319(2) of the NCC states: “Acceptance by letter or telegram does not bind the offerer except from the time it came to his knowledge. The contract in such case, is presumed to have been entered into the place where the offer is made.” It is submitted that as to Facebook, the place of the offer is Palo Alto, California, the seat of its corporate office and headquarters, while as to Google, the place of the offer is Mountain View, California, the seat of its corporate office and headquarters. A perusal of California Uniform Electronic Transactions Act provides under Article 1633.7 that a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.¹⁸⁶ Hence, California law provides that electronic terms and conditions are valid in form.

As to intrinsic validity, the following should be considered: “(a) the law chosen by the parties and in the absence thereof; (b) the place of contracting, (c) the place of negotiation of the contract, (d) the place of

¹⁸² Schau supra note 139

¹⁸³ CIVIL CODE; art. 15.

¹⁸⁴ Perez v. CA, G.R. No. 162580, January 27, 2006; Coquia, J.R. and Aguilin-Pangalangan, E. supra note 140

¹⁸⁵ World Economic Forum 2016 Report supra note 156

¹⁸⁶ California Uniform Electronic Transactions Act, art. 1633.7

performance; and (e) the domicile, residence, nationality, place of incorporation and place of business of the parties”.¹⁸⁷ The law intended by the parties or *lex loci intentionis* may be expressed in our jurisdiction through a provision in the contract itself.¹⁸⁸ Applying Article 1306¹⁸⁹ of the NCC, it is valid to stipulate that the contract be governed by a specific law, unless such choice of law provision is contrary to a policy of the forum.¹⁹⁰

A perusal of the Terms and Conditions of Facebook, there is an express provision on that domestic law will govern the parties:

*“If you are a consumer, the laws of the country in which you reside will apply to any claim, cause of action, or dispute you have against us that arises out of or relates to these Terms or the Facebook Products, and you may resolve your claim in any competent court in that country that has jurisdiction over the claim.”*¹⁹¹

The Terms and Conditions of Google have a similar provision:

“If you reside in one of those countries [that will not apply California law], then where California law is excluded from applying, your country’s laws will apply to such disputes related to these terms.

*If the courts in your country will not permit you to consent to the jurisdiction and venue of the courts in Santa Clara County, California, U.S.A., then your local jurisdiction and venue will apply to such disputes related to these terms.”*¹⁹²

Hence, Philippine law will apply concerning these contracts, pursuant to *lex loci intentionis*.

It is also worth stressing that the two special laws applicable in the treatment of personal information, the Data Privacy Act and the Cybercrime Prevention Act are in the nature of long arm statutes or statutes that specify the kind of contacts wherein jurisdiction will be

¹⁸⁷ Coquia, J.R. and Aguilin-Pangalangan, E. supra note 140, at 68, 2.

¹⁸⁸ *Ibid*, at 339, 2.

¹⁸⁹ CIVIL CODE, art. 1306

¹⁹⁰ *Ibid*, at 339, 2; Continental Micronesia, Inc. v. Joseph Basso, G.R. No. 178382-83, September 23, 2015

¹⁹¹ Facebook Terms and Conditions, available at <https://www.facebook.com/legal/terms/update> [accessed on 11 March 2020]

¹⁹² Google Terms and Conditions, available at <https://policies.google.com/terms?hl=en-US> [accessed 11 March 2020]

asserted.¹⁹³ Section 6 of the DPA provides the principle of extraterritorial application¹⁹⁴, while Section 21 of the same provides the principle of accountability for data controllers.¹⁹⁵ Meanwhile, Section 21 of the CPA outlines the jurisdiction.¹⁹⁶ Hence, even without such provision in the contract providing that the domestic law of the user will apply, Philippine law will still apply to those cases expressly enumerated under the law.

2. Domestic laws

a. Personal information within the commerce of man

The second approach under this framework treats certain types of personal information as property within the commerce of man.¹⁹⁷ This view is supported by existing literature due to the control it gives to the data subject over his or her personal information.¹⁹⁸ Applying the incentive theory, the treatment of personal data of this category may lead to economic compensation for the use of such personal data,¹⁹⁹ commensurate to the loss of privacy, resulting in accelerated growth in the information market.²⁰⁰

As discussed, Section 3(g) of the DPA provides the definition of personal information,²⁰¹ while the CPA further classifies personal information as subscriber information, traffic data²⁰², and content data.²⁰³ Following the digital identity framework provided by the World Economic Forum, *traffic data* and *content data* in the nature of *accumulated attributes* or “attributes that are gathered or developed over time, which may change multiple times or evolve throughout an entity’s lifespan, such as preferences and behaviors in the form of telephone metadata” are *things* or *property*.²⁰⁴

¹⁹³ Coquia, J.R. and Aguiling-Pangalangan, E. supra note 140, at 36, 2.

¹⁹⁴ CPA, sec. 6.

¹⁹⁵ *Id*

¹⁹⁶ RA 10173, sec. 21.

¹⁹⁷ World Economic Forum 2016 Report supra note 156

¹⁹⁸ McFarland supra note 22

¹⁹⁹ Jennifer Barrigar et al., Let’s not get psyched out of privacy: Reflections on withdrawing consent to the collection, use and disclosure of personal information, 44 Can. Bus. L.J. 54, 56 2006-2007

²⁰⁰ Vishwajith, A.S. and Varanasi, S. supra note 131

²⁰¹ RA 10173, Sec 3(g); IRR of RA 10173, Sec 3(l)

²⁰² R.A. No. 10175, Section 3(p)

²⁰³ IRR of RA 10175, Section 3

²⁰⁴ World Economic Forum 2016 Report supra note 156

As discussed, in order to be juridically considered as a thing or property, “an object must have the following requisites:

1. utility, or the capacity to satisfy human wants,
2. individuality and substance, or a separate and autonomous existence, and
3. susceptibility of being appropriated.”²⁰⁵

Applying the elements of a *thing* or *property*, *accumulated attributes* have all of the necessary requisites. First, they have utility or the capacity to satisfy human wants because of the value of such personal information to the data subject and the enterprises which seek to analyze such data.²⁰⁶ Information of this nature also has a separate and autonomous existence apart from the data subject, in that they are a direct result of behavior online through a “digital dossier”.²⁰⁷ Finally, they are susceptible to appropriation, due to the value of such data in facilitating commercial transactions.²⁰⁸ Accordingly, it is submitted that *traffic data* and *content data* are *things* or *property* in our jurisdiction.

The position that data subjects own their own data is supported in legal scholarship.²⁰⁹ Ownership is defined as “the independent and general power of a person over a thing for purposes recognized by law and within the limits established thereby”.²¹⁰ The attributes of ownership are *jus possidendi* or the right to possess, *jus utendi* or the right to receive from the thing what it produces²¹¹, *jus fruendi* or the right to the fruits, *jus abutendi* or the right to consume the thing by its use²¹², *jus disponendi* or the right to dispose²¹³, and *jus vindicandi* or the right to exclude from the possession of

²⁰⁵ 2 Arturo M. Tolentino supra note 153, at 3, 2 (2004)

²⁰⁶ Li, Chao, Li, Daniel Yang, Miklau, Gerome, and Suciu, Dan. A theory of pricing private data. Communications of the ACM, December 2017, Vol. 60 No. 12, 79-86
10.1145/3139457

²⁰⁷ Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083 (2002)

²⁰⁸ J. Brustein. Start-ups seek to help users put a price on their personal data. The New York Times, Feb 2012.

²⁰⁹ Kenneth C. Laudon, *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept. 1996, at 92

²¹⁰ 2 Arturo M. Tolentino supra note 153, at 45, 1 (2004)

²¹¹ 2 Arturo M. Tolentino supra note 153, at 5, 1 (2004)

²¹² *Ibid*, at 46, 1 (2004)

²¹³ *Ibid*, at 46, 2 (2004)

the thing owned by any other person to whom the owner has not transmitted such thing.²¹⁴

The DPA provides the various rights which a data subject, such as the right to be informed²¹⁵, the right to object²¹⁶, the right to access²¹⁷, the right to rectification²¹⁸, erasure²¹⁹ or blocking²²⁰, the right to damages²²¹, and the right to data portability²²². Specific rights under the DPA may be paralleled to the incidents of ownership in general property law.

Jus possidendi may be seen in the right to access under Section 16(c) of the DPA, which provides that the data subject has the right to reasonable access, upon demand, as regards information enumerated in the law.²²³

*Jus utendi*²²⁴ of the data subject may be paralleled to the right to data portability under Section 18 of the DPA, which states that the “the data subject shall have the right [...] to obtain from the personal information controller a copy of data undergoing processing [...] and allows for further use by the data subject”²²⁵

*Jus disponendi*²²⁶ is seen in section 34(b) of IRR of the DPA provides that “the data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling” and “the data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject”.²²⁷ The right to transform and destroy of the data subject may be seen in the right to rectification under Section 16(e) of the DPA, which states that the data subject has the right to “suspend, withdraw or order the blocking, removal or destruction of his or her personal information from

²¹⁴ *Ibid*, at 46, 3 (2004)

²¹⁵ RA 10173, Sec 16(a); IRR of RA 10173, Sec. 34(a)

²¹⁶ IRR of RA 10173, Sec. 34(b)

²¹⁷ RA 10173, Sec 16(c); IRR of RA 10173, Sec. 34(c)

²¹⁸ RA 10173, Sec 16(d); IRR of RA 10173, Sec 34(d)

²¹⁹ RA 10173, Sec 16(e); IRR of RA 10173, Sec 34(e)

²²⁰ RA 10173, Sec 16(e); IRR of RA 10173 Sec. 34(e)

²²¹ RA 10173, Sec 16(f); IRR of RA 10173, Sec 34(f)

²²² RA 10173, Sec 18; IRR of RA 10173, Sec 36

²²³ RA 10173, Sec 16(c); IRR of RA 10173, Sec. 34(c)

²²⁴ 2 Arturo M. Tolentino supra note 153, at 5, 1 (2004)

²²⁵ RA 10173, Sec 18; IRR of RA 10173, Sec 36

²²⁶ 2 Arturo M. Tolentino supra note 209, at 6, 2 (2004)

²²⁷ IRR of RA 10173, Sec. 34(b)

the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected".²²⁸

*Jus vindicandi*²²⁹ is in Section 16(f) of the DPA: "The data subject is entitled to be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information."

Hence, it is the submission of the researcher that other incidents of ownership such *jus fruendi* or the right to the fruits are also rights which the data subject is entitled to.

2. Effect on contracts

Having established that such personal information involving *accumulated attributes* may be contracted, for such information to be processed, it must be pseudonymized by the data controller and consent must be obtained from the data subject.

Pursuant to the concept of data protection by design, the GDPR encourages the pseudonymisation of data or "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual"²³⁰ While there is no express mention of the same in the DPA, the definition of personal information referring to information where the identity of an individual can be ascertained directly or indirectly when used with other information, may be used as basis for the application of a similar requirement for pseudonymisation in domestic law. Pseudonymisation is essential in reducing the risks of processing, while maintaining the utility of the data.²³¹

²²⁸ RA 10173, Sec 16(d); IRR of RA 10173, Sec 34(d)

²²⁹ 2 Arturo M. Tolentino supra note 209, at 46, 3 (2004)

²³⁰ GDPR, art 4(3b)

²³¹ Dove, E.S., *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*. Journal of Law Medicine and Ethics (December 2018). DOI: 10.1177/1073110518822003;

With this safeguard in place, the data subject has the right to make his or her personal information involving *accumulated attributes* the subject of contract. Article 1305 of the NCC provides the definition of a contract,²³² while the elements of a contract (consent, object and cause) under our jurisdiction are found in Article 1318 of the Civil Code.²³³

Consent is the concurrence of the offer and the corollary acceptance by the parties which expresses their intent in entering into such contract.²³⁴ Hence, any subsequent change must be made with the assent of both parties, and absent the mutual assent, the act has no effect under the law.²³⁵ Hence, it is thus within the discretion of the data subject to make personal information involving *accumulated attributes* such as *traffic data* and *content data* the subject of contract, or to otherwise not make it the subject of contract, pursuant to his or her right to object to the processing of his or her personal data, or the right to withdraw consent under Section 34(b) of the IRR of the DPA.²³⁶

As applied to contracts involving personal information of this nature, they may be validly contracted out, however it is submitted that certain provisions in existing contracts may be considered void. By way of example, this research focuses on two contracts from two of the biggest data-driven, knowledge-based enterprises: Facebook and Google. A perusal of the company information of Facebook shows that the technologies it owns are the Facebook application, Messenger, Instagram, Whatsapp, Oculus, Workplace, Portal, and Calibra.²³⁷ Meanwhile, Google owns 64 technologies for everyday users²³⁸, 55 technologies for businesses²³⁹, 391 technologies for developers,²⁴⁰ including YouTube, Waze, and Chrome. Hence, it is submitted that the pervasiveness of such technological platforms should be factored in and heavily appreciated in considering the unequal bargaining power of the contracting parties.

²³² CIVIL CODE, art. 1305;

²³³ CIVIL CODE, art. 1318

²³⁴ Yuchengco vs. Dacuycuy, 104 SCRA 668 [1981]

²³⁵ Phil. National Bank vs. Court of Appeals, 238 SCRA 20 [1994]

²³⁶ IRR of RA 10173, Sec. 34(b)

²³⁷ Facebook Company Information, available at <https://about.fb.com/company-info/> [accessed 3 March 2020]

²³⁸ Google Products for All, available at <https://about.google/products/> [accessed 3 March 2020]

²³⁹ Google Products for Businesses, available at <https://about.google/products/> [accessed 3 March 2020]

²⁴⁰ Google Products for Developers, available at <https://developers.google.com/products?hl=en> [accessed 3 March 2020]

A contract of adhesion is one wherein almost all of the provisions are drafted by one party, and the participation of the other party is limited to affixing his signature or his “adhesion” to the contract.²⁴¹ Hence, any ambiguity, obscurity or doubt in a contract of adhesion is construed or resolved strictly against the party who prepared it.²⁴² Article 24 of the NCC provides that a party who is disadvantaged because of ignorance, indigence, mental weakness, tender age, and other similar handicap must be protected.²⁴³ In some instances, the court has set aside prejudicial stipulations in an adhesion contract.²⁴⁴ Typically, the “take it or leave it” nature of contracts of adhesion still gives the option to users to not use the platform if one is not amenable to the terms and conditions thereof. However, considering the depth and breadth of these platforms and their inextricable link to modern daily life, opting out seems neither completely possible nor practical; hence, users should be protected in the construction of such provisions.

The validity or enforceability of the impugned contracts are determined by the peculiar circumstances in each case and the situation of the parties.²⁴⁵ As an example a perusal of the Facebook Terms and Conditions shows us that in using the Facebook platform, the user grants certain permissions in the form of permission to use content created and shared, permissions to use name, profile picture and information about actions with ads and sponsored content, and permission to update software used and downloaded.²⁴⁶ Section 12 of the DPA provides the criteria for lawful processing of personal information,²⁴⁷ and of those mentioned, Section 12(f) is the most relevant to the discussion:

“(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.” (emphasis supplied)

²⁴¹ Equitable PCI Bank v. Ng Sheung Ngor, G.R. 171545, December 19, 2007

²⁴² Spouses Panlilio v. Citibank, N.A., G.R. No. 156335, November 28, 2007

²⁴³ Ayala Corporation v. Ray Burton Development Corporation, G.R. No. 126699, August 7, 1998;

²⁴⁴ Sweet Lines, Inc. v. Teves, G.R. No. L-37750, May 19, 1978.

²⁴⁵ Cabunting v BPI Family Savings Bank, G.R. No. 201927, February 17, 2016

²⁴⁶ Facebook Terms and Conditions supra note 195

²⁴⁷ RA 10173, Section 12

The DPA itself provides that any collection and processing of information must yield to the power of the state to intervene where any terms are violative of Constitutional rights. In relation to this, of particular interest for the purposes of this research is the permission to use name, profile picture and information about actions with ads and sponsored content:

“You give us permission to use your name and profile picture and information about actions you have taken on Facebook next to or in connection with ads, offers, and other sponsored content that we display across our Products, without any compensation to you.”

The Google Terms and Conditions have a similar provision:

“When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute such content.”

The DPA requires that any and all processing be governed by the principles of transparency²⁴⁸, legitimate purpose²⁴⁹, proportionality²⁵⁰, and data quality²⁵¹. Hence, it is submitted that the abovementioned provisions are neither transparent nor proportionate to the legitimate aims pursued. First, it fails the principle of transparency because it fails to specify what types of personal information are being cascaded to third party entities and what purposes the data will be further processed for. Second, it fails the principle of proportionality, as disclosure for one purpose may not be proportionate for other purposes. Moreover, provisions do not allow the data subject to meaningfully consent to the further processing of his or her personal information, as such provision seems to imply blanket authority on the part of the data controller to enter into further contracts with third party processors and patrons, such as advertisers, marketers.

Additionally, the Facebook Terms and Conditions provide this proviso: *“This license will continue until the content has been fully deleted.”* Meanwhile, the Google Terms and Conditions contains a similar provision: *“This license continues even if you stop using our Services.”* It is submitted that

²⁴⁸ IRR of RA 10173, Sec 18(a)

²⁴⁹ IRR of RA 10173, Sec 18(b)

²⁵⁰ IRR of RA 10173, Sec 18(c)

²⁵¹ IRR of RA 10173, Sec 19(c)

such clauses are violative of the principle of legitimate purpose, as the entities may continue to collect and process such information even when the data subject discontinues use of the platform.

Moreover, the Google Terms and Conditions states: *“We reserve all rights not expressly granted to you.”* Such provision is contrary to public policy, as it seems to imply that the data controller may do anything in relation to the personal information of the data subject, if such has not been expressly granted to the data subject. While the parties do have the autonomy to contract one another, the demarcation and rightful hierarchy over a right and a restriction should be strictly reinforced; hence the norm (the data subject owns the information) and the exception (the data controller is given limited access) should not be reversed.²⁵²

Hence, any third party contracts (such as those entered by data controllers with advertisers and marketers) which spring from such alienation of personal information of this category, are also accordingly void. As per Article 1422 of the Civil Code, a contract which is the direct result of a previous illegal contract, is also void and inexistent.²⁵³ Applying the same to contracts entered into by data controllers with advertisers and marketers, such third party contracts are also void.

²⁵² Privacy International, *Guide to International Law and Surveillance 2.0* (February 2019), available at <https://privacyinternational.org/long-read/993/guide-international-law-and-surveillance-20> (accessed 1 February 2020)

²⁵³ CIVIL CODE, art. 1422

V. EXACTING ACCOUNTABILITY FROM DATA DRIVEN ENTERPRISES

1. Remedies for unlawful processing of personal information outside the commerce of men a. Conflict of laws

In order to exact accountability from data driven enterprises for the contractualization of personal information outside the commerce of man, the law on torts applies. Generally speaking, “a tort is an act or omission producing an injury to another without any previous existing lawful relation of which the act or omission may be said to be a natural outgrowth or incident”.²⁵⁴ However, at the outset, it must be determined what law should apply between foreign and forum law.

Conflict of laws is “that part of the law of each state or nation which determines whether, in dealing with a legal situation, the law of some other state or nation will be recognized, given effect, or applied”.²⁵⁵ One modern approach in determining the choice of law is the *most significant relationship approach*, which considers a plurality of factors.²⁵⁶ For actions for damages on general tort law, “the contacts to be taken into consideration are: the place where the injury occurred, the place where the negligent conduct occurred, the place the domicile, residence or nationality of the parties and the place where the relationship between the parties entered”²⁵⁷

Applying such framework, the tort is actionable domestically. In *Saudi Arabian Airlines v. CA*, the Court considered pragmatic considerations, including the convenience of the parties and the private interests of the litigant, including the enforceability of the judgment and the relative advantages and obstacles to a fair trial.²⁵⁸ While the determination of the connecting factors are matters of fact which should be looked into with respect to the peculiar circumstances of each case, it is

²⁵⁴ Coquia, J.R. and Aguilin-Pangalangan, E. supra note 140, at 407, 1

²⁵⁵ Agpalo, R., *Conflict of Laws (Private International Law)*, 2004 Ed

²⁵⁶ *Continental Micronesia, Inc. v. Joseph Basso*, G.R. No. 178382-83, September 23, 2015; Coquia, J.R. and Aguilin-Pangalangan, E. supra note 140, at 7, 1.

²⁵⁷ *Saudi Arabian Airlines v. CA*, G.R. 122191, October 8, 1998; Coquia, J.R. and Aguilin-Pangalangan, E. supra note 140, at 68, 1.

²⁵⁸ G.R. 122191, October 8, 1998

submitted that certain essential points of contact may be established in the Philippines, considering injury is personal and attaches to the person.²⁵⁹

There is also strong public policy that must be enforced in allowing an action to be brought in Philippine courts, namely, the protection of the data privacy rights of individuals.²⁶⁰ Otherwise, a claimant would have to file a tort action overseas wherever the information is collected and processed, leading not to inconvenience, expense, and injustice, considering that an individual stands at a profound disadvantage compared to entities such as Facebook and Google.

However, even assuming that such points of contact are deemed to be in another country, although there is no specific law governing the enforcement of claims for damages arising from foreign torts, the English rule may be followed in this jurisdiction, whereby a tort committed abroad may be actionable in either the country wherein it was committed and under Philippine law.²⁶¹

b. Special laws

The Data Privacy Act is in the nature of a long arm statute or a statute that specifies the kind of contacts wherein jurisdiction will be asserted.²⁶² Section 6 of the DPA provides the principle of extraterritorial application.²⁶³ Hence, Philippine law will apply to an action for damages in those cases expressly enumerated under the DPA, pursuant to Section 16(f) of the DPA which states that the data subject shall “be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information”.²⁶⁴

c. Article 19 of the New Civil Code

Article 19 of the NCC, which enshrines the principle of abuse of rights²⁶⁵ or the good faith principle²⁶⁶, provides that every person must, in

²⁵⁹ Agpalo, R., *Conflict of Laws (Private International Law)*, 2004 Ed;

²⁶⁰ *Philippine Export and Foreign Loan Guarantee Corporation v. V. P. Eusebio Construction, Inc.*, G.R. No. 140047, July 13, 2004

²⁶¹ Coquia, J.R. and Aguilin-Pangalangan, E. *supra* note 140, at 452, 5.

²⁶² *Ibid*, at 36, 2; Paras, E.L., *Philippine Conflict of Laws (6th Ed., 1984)*

²⁶³ RA 10173, sec. 6.

²⁶⁴ RA 10173, Sec 16(f); IRR of RA 10173, Sec 34(f)

²⁶⁵ *Globe Mackay v. CA*, G.R. No. 81262, 25 August 1989; *Albenson v. CA*, G.R. No. 88694, 11 January 1993

²⁶⁶ *Andrade v. CA*, G.R. No. 127932, 7 December 2001; Casis, R. 2012. *Analysis of Philippine Law and Jurisprudence on Torts and Quasi-delicts*, UP College of Law.

the exercise of his rights and in the performance of his duties, act with justice, give everyone his due, and observe honesty and good faith. In *UE v. Jader*, the Court stated that the rationale behind such principle is to “expand the concept of torts by granting adequate legal remedy for the untold number of moral wrongs”.²⁶⁷ In certain cases, the Court ruled that Article 19 is a mere declaration of principle²⁶⁸ and may not be the sole basis for an award of damages, however in certain instances, the Court granted an award of damages²⁶⁹ based solely on Article 19.²⁷⁰

d. Article 20 of the New Civil Code

Article 20 of the NCC provides that every person who, contrary to law, willfully or negligently causes damage to another shall indemnify the latter for the same. In *Garcia v. Salvador*, the Court explained that Article 20 is the “legal basis for the award of damages to a party who suffers damage whenever one commits an act in violation of some legal provision”.²⁷¹ Hence, to successfully bring an action under Article 20, all the elements of an actionable conduct must be present: “(1) duty, (2) breach, (3) injury, and (4) proximate causation”.²⁷²

e. Article 26 of the New Civil Code

Article 26 provides that every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons.²⁷³ Hence, a cause of action for damages, prevention and other relief may arise under this provision in case of breach of right to personal dignity, right to personal security, and right to privacy.²⁷⁴

²⁶⁷ G.R. No. 132344, 17 February 2000

²⁶⁸ *Sea Commercial Company v. CA*, G.R. No. 122823, 25 November, 1999

²⁶⁹ *UE v. Jader*, G.R. No. 132344, 17 February 2000

²⁷⁰ *Casis, R. supra* at note 272

²⁷¹ G.R. No. 168512, 20 March 2007

²⁷² *Garcia v. Salvador*, G.R. No. 168512, 20 March 2007; *Casis, R. supra* at note 272

²⁷³ *Gregorio v. CA*, G.R. No. 179799, 11 September 2009; *Casis, R. supra* at note 272

²⁷⁴ *Spouses Guanio v. Makati Shangrila*, G.R. 190601, 7 February 2011; *St. Louis v. CA*, G.R. L-46061, 14 November 1984

2. Remedies for unlawful processing of personal information within the commerce of man

a. Conflict of laws

As discussed, the Terms and Conditions of Facebook²⁷⁵ and Google²⁷⁶ both provide provisions that domestic law will govern the parties. Hence, such provisions show the intention or even accession of both Facebook and Google to be subjected to domestic law in all actions, such as breach of contract and torts.

b. Breach of contract

Article 1170 of the NCC provides that “those who in the performance of their obligations are guilty of fraud, negligence or delay, and those who in any manner contravene the tenor thereof are liable for damages”. Contravention of tenor of the obligation involves “violation of terms and conditions stipulated in the obligation”.²⁷⁷ In our jurisdiction, the law on contracts provides that “actionable injury inheres in every contractual breach”.²⁷⁸

c. Special laws

As discussed, under the DPA, an individual has the right to damages under Section 16(f) of the DPA which states that the data subject shall “be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information”.²⁷⁹

d. Article 19 of the New Civil Code

A data subject whose personal information has been processed unlawfully may file an action under Article 19 of the NCC or principle of abuse of rights.²⁸⁰ To successfully bring an action under Article 19, the data

²⁷⁵ Facebook Terms and Conditions supra note 195

²⁷⁶ Google Terms and Conditions supra note 196

²⁷⁷ De Leon, H.S. and de Leon, H.M., *The Law on Obligations and Contracts*, 2014 Revised Edition, Rex Bookstore: Quezon City, Philippines.

²⁷⁸ *Boysaw v. Interphil Promotions*, G.R. No. L-22590, 20 March 1987

²⁷⁹ RA 10173, Sec 16(f); IRR of RA 10173, Sec 34(f)

²⁸⁰ *Globe Mackay v. CA*, G.R. No. 81262, 25 August 1989

subject must present: “(1) legal right or duty, (2) exercise of bad faith, and (3) intent to prejudice or injure”.²⁸¹

e. Article 20 of the New Civil Code

Additionally, a data subject may file an action under Article 20 of the NCC. To successfully bring an action under Article 20, all the elements of an actionable conduct must be present: “(1) duty, (2) breach, (3) injury, and (4) proximate causation.”²⁸²

f. Article 21 of the New Civil Code

The data subject may also file an action under Article 21 of the NCC, which provides that any person who wilfully causes loss or injury to another in a manner that is contrary to morals, good customs, or public policy shall compensate the latter for the damages. The purpose of Article 21 is to provide a legal remedy for the untold number of moral wrongs which is impossible for human foresight to provide for specifically in the statutes.²⁸³ Hence, to successfully bring an action under Article 21, it must comply with the following: “(1) there is an act which is legal, (2) but which is contrary to morals, good customs, public order, or public policy, (3) and it is done with intent to injure”.²⁸⁴

g. Article 26 of the New Civil Code

The data subject may likewise file an action under Article 26, which provides that every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons.²⁸⁵ Hence, a cause of action for damages, prevention and other relief may arise under this provision in case of breach of right to personal dignity, right to personal security, and right to privacy.²⁸⁶

²⁸¹ Casis, R. supra at note 272, at p. 514

²⁸² Garcia v. Salvador, G.R. No. 168512, 20 March 2007; Casis, R. supra at note 272

²⁸³ Globe Mackay v. CA, G.R. No. 81262, 25 August 1989; Casis, R. supra at note 272, at p. 541-542

²⁸⁴ Albenson v. CAG.R. No. 88694, 11 January 1993; Casis, R. supra at note 272, at p. 544

²⁸⁵ Gregorio v. CA, G.R. No. 179799, 11 September 2009; Casis, R. supra at note 272

²⁸⁶ Spouses Guanio v. Makati Shangrila, G.R. 190601, 7 February 2011; Casis, R. supra at note 272, at p. 594

3. Way forward: Wealth distribution

a. Unjust enrichment

Under Article 22 of the NCC, "*every person who through an act of performance by another, or any other means, acquires or comes into possession of something at the expense of the latter without just or legal ground, shall return the same to him.*"²⁸⁷ The Court has pronounced in a number of cases that the principle of unjust enrichment has two conditions; first, a person must have been benefited without a real or valid basis or justification, and second, the benefit was derived at another person's expense or damage.²⁸⁸ With the rise of surveillance capitalism, it can be argued that corporations are unjustly enriching themselves at the expense of data subjects.

In April 2018, a class action lawsuit was filed in the U.S. District for the Northern District of California representing an estimated 70 million US Facebook users for the harvesting of data user information through the personality quiz Facebook application "*This is my digital life*" and the consequent siphoning off of such information to third party companies that bought such user data to influence voting in the US elections.²⁸⁹ Cambridge University researcher Aleksandr Kogan designed the personality quiz application which prompted users to give access to the user's information and the information of the user's Facebook friends, leading to the transfer of such information to GSL Elections and eventually to Cambridge Analytica.²⁹⁰ The complaint makes a case for unjust enrichment at the expense of its users in that "when users allowed Facebook access to their personal information in order to use the social network, they did so on the condition that it would be protected and shared only under the terms of the agreements and policies that protected it [hence] when Facebook skimmed on data protection to save money, thereby enhancing its profits, its users paid the price".²⁹¹ It provides that the platform "was unjustly enriched

²⁸⁷ CIVIL CODE, art. 22; *Elegir v. Philippine Airlines, Inc.*, G.R. No. 181995, July 16, 2012

²⁸⁸ *Locsin II v. Meken Food Corporation*, G.R. No. 192105, December 9, 2013;

²⁸⁹ Hagens Berman. (2018). Facebook hit with class action lawsuit following massive user data scandal, available at

<https://www.hbsslaw.com/cases/facebook-users-privacy/pressrelease/facebook-users-privacy-facebook-hit-with-class-action-lawsuit-following-massive-user-data-scandal> [accessed 3 April 2020]

²⁹⁰ Businesswire. (2018). Hagens Berman: Facebook hit with class action lawsuit following massive user data scandal, available at

<https://www.businesswire.com/news/home/20180409006426/en/Hagens-Berman-Facebook-Hit-Class-Action-Lawsuit-Massive> [accessed 1 April 2020]

²⁹¹ Hagens Berman *supra* note 297

when it used this data to make money from its advertising business, even as it was failing to protect it".²⁹² While as of the time of writing of this research, there has not been a final ruling on the matter, however it shows the movement towards greater accountability on the part of enterprises.

b. Taxing the digital economy

As of the time of this research, the Department of Finance and the Bureau of Internal Revenue of the Philippines are exploring methods to tax activities under the digital economy, in light of substantial tax leakages in the realm of online advertising and other online commercial activities.²⁹³ The need to capture online transactions for purposes of taxation is especially more pronounced in light of the COVID-19 pandemic of 2020 and the resultant projections of a global economic recession.²⁹⁴ The enforcement of lockdowns has resulted in a sharp spike in internet usage.²⁹⁵ Hence, capturing digital transactions can be a strong source of tax revenue that can translate to economic stimulus amid the challenging times.

The Philippine tax system has two primary broad bases for taxation, namely income and consumption.²⁹⁶ Taxation exposures of knowledge-based, data-driven economies may be through income tax and value added tax. As to income tax exposure, both Facebook and Google have established a presence in the country, namely Facebook Singapore doing business under the name and style of Facebook Philippines as a representative office, and Google Philippines, Inc. based in Taguig City for sales and marketing operations and Google Services, Inc. as a PEZA-registered entity for vendor operations. As to VAT, the worldwide trend is a shift to destination-based taxes and the liability of non-resident

²⁹² Businesswire supra note 298

²⁹³ Hulog, L. (2019). BIR studies ways on taxing digital economy in the Philippines, available at <https://ahccounting.com/bir-looks-methods-tax-digital-economy/> [accessed 1 April 2020]

²⁹⁴ New York Times (14 April 2020), IMF predicts worst downturn since the Great Depression, available at <https://www.nytimes.com/2020/04/14/us/politics/coronavirus-economy-recession-depression.html> [accessed 15 April]

²⁹⁵ ABS-CBN News (18 March 2020), PLDT, Globe gear for data demand as COVID-19 keeps millions in Philippines indoors, available at <https://news.abs-cbn.com/business/03/18/20/pldt-globe-gear-for-data-demand-as-covid-19-keeps-millions-in-philippines-indoors> [accessed 10 April 2020]

²⁹⁶ Reside, R.E. Jr and Burns, L. (2016). *Comprehensive Tax Reform in the Philippines: Principles, History, and Recommendations*. UP Diliman School of Economics Discussion Papers.

digital suppliers to VAT (cross-border digital services), in a bid to close taxation loopholes.²⁹⁷

Locally, Revenue Memorandum Circular (RMC) No. 55²⁹⁸ issued in 2013 establishes tax rules and obligations on online businesses, including a proviso mandating online shopping or retailing services, online intermediary services, online advertising or classified ads, and online auction services to register. Noncompliance with the said circular renders one subject to the imposition of penalties under the National Internal Revenue Code of 1997.

RMC 55-2013 provides that such entities conducting online transactions are mandated to “withhold required creditable/expanded withholding tax, final tax, tax on compensation of employees, and other withholding taxes, remit the same to the Bureau at the time or times required, [and] issue to the concerned payees the necessary Certificate of Tax Withheld”. However, despite the issuance of the said RMC No. 55 in 2013, tax leakages still abound, due in part to the difficulty in ensuring compliance among online businesses, including the taxation of foreign-supplied digital services.²⁹⁹

c. Direct to consumer profit-sharing mechanisms

The researcher submits that direct compensation schemes should be enforced in our jurisdiction, owing to the profound social media exposure of Filipinos.³⁰⁰ The current model for acquiring personal data offers free service and use of one platform in exchange of access to personal data, then monetizing the personal information by selling the data or information derived from data.³⁰¹ There is a strong movement now, however, to reevaluate this model in favor of a profit-sharing mechanism which allows users to be compensated directly, in light of the resulting loss of privacy on

²⁹⁷ Taxamo. (2020). Digital tax developments in South-east Asia, available at <https://blog.taxamo.com/insights/digital-tax-news-south-east-asia> [accessed 3 April 2020]; Taxamo. (2020). Digital trends: International plans to tax the digital economy, available at <https://blog.taxamo.com/insights/international-digital-tax-trends> [accessed 3 April 2020]

²⁹⁸ Revenue Memorandum Circular 55-2013: Reiterating taxpayers’ obligations in relation to online business transactions, 5 August 2013

²⁹⁹ Hulog, L. (2019). BIR studies ways on taxing digital economy in the Philippines, available at <https://ahccounting.com/bir-looks-methods-tax-digital-economy/> [accessed 1 April 2020]

³⁰⁰ We are Social, *Digital in 2019 Philippines report*, available at <https://www.slideshare.net/DataReportal/digital-2019-philippines-january-2019-v01>, at 34 (last visited 8 January 2020)

³⁰¹ Li et al supra note 210; A. Acquisti, L. John, and G. Loewenstein. What is privacy worth? In *Workshop on Information Systems and Economics*, 2009

the part of the user.³⁰² As of late, companies have developed the infrastructure for direct compensation by way of personal data vaults, and the data owners of such data vaults are adequately compensated for access to information contained therein.³⁰³

Legislation has also been proposed to address the widening income gap between giant technology companies and the data subjects, in the form of a *data dividend*, a direct-to-consumer payout for the use of personal data so consumers can “share in the wealth created from their data”.³⁰⁴ Direct-to-consumer wealth distribution legislation has been enforced as early as 1974 in Alaska; an oil company was mandated to transfer at least 25% of all annual oil royalties into a fund, for annual distribution to Alaskan residents, based on the proposition that “the natural resource belongs equally to all Alaskans”.³⁰⁵

Clearly, whether in the form of taxing the digital economy directly and distributing the wealth in the form of basic services³⁰⁶, or requiring the payment of a portion of revenues into a savings account divided among data subjects³⁰⁷, or direct-to-consumer payout mechanisms for those who elect to sell their personal information³⁰⁸, the growing trend globally is towards a more equitable redistribution of the wealth of the digital economy - one that should also be enforced in our own jurisdiction, to further promote liberty and economic prosperity.

³⁰² Holt, C.A., & Laury, S.K. (2002). Risk aversion and incentive effects. *American Economic Review*, 92, 1644-1655;

³⁰³ Personal data: The emergence of a new asset class. Report of the World Economic Forum, Feb 2011; Li et al supra note 210

³⁰⁴ Au-Yeung, A. (14 February 2020), California wants to copy Alaska and pay people a data dividend, available at <https://www.forbes.com/sites/angelauyeung/2019/02/14/california-wants-to-copy-alaska-and-pay-people-a-data-dividend--is-it-realistic/#3203bdd9222c> [accessed 30 March 2020]

³⁰⁵ Ulloa, J. (5 May 2019), *Newsom wants companies collecting personal data to share the wealth with Californians*, available at <https://www.latimes.com/politics/la-pol-ca-gavin-newsom-california-data-dividend-20190505-story.html> [accessed 10 March 2020]

³⁰⁶ Hulog, L. (2019). BIR studies ways on taxing digital economy in the Philippines, available at <https://ahccounting.com/bir-looks-methods-tax-digital-economy/> [accessed 1 April 2020]

³⁰⁷ Au-Yeung, A. (14 February 2020), California wants to copy Alaska and pay people a data dividend, available at <https://www.forbes.com/sites/angelauyeung/2019/02/14/california-wants-to-copy-alaska-and-pay-people-a-data-dividend--is-it-realistic/#3203bdd9222c> [accessed 30 March 2020]

³⁰⁸ Report of the World Economic Forum supra note 318; Li et al supra note 210

VI. THE ROLE OF THE PARADIGM SHIFT IN STRENGTHENING LIBERTY AND PROSPERITY UNDER THE RULE OF LAW

The paradigm shift proposed in this research as a combination of the two approaches to digital footprint has a concrete role in strengthening liberty and prosperity under the rule of law.

As to liberty, evidently, the combination of the approaches inherently recognizes the liberty of every *Juan* and by shifting the role of users in their own digital footprint. The approaches presented bring the power back to the digital community. Treating digital footprints in the first tier as beyond the commerce of man, human dignity is extended not just to the natural or physical body, but the extensions thereof in the digital; whereas treating digital footprints in the second tier as within the commerce of man, namely their own exclusive property, allows them to exercise and enjoy the full extent of their ownership rights as wide or narrow as they so please.³⁰⁹

As to prosperity, a combination of the two approaches results in prosperity for every *Juan*. The approaches hereof presented creates a more prosperous life for the whole digital community. Treating digital footprints in the first tier as beyond the commerce of man provides an avenue for prosperity in the form of an uplifted quality of life and well-being; whereas treating digital footprints in the second tier as within the commerce of man but as the exclusive property of the user provides an opportunity for financial prosperity, to enjoy the use and the fruits of one's digital footprint, in the form of compensation.³¹⁰

As to bringing both into the rule of law, a strong case has been made for the applicability of existing laws in the two approaches to digital footprint in a way that more actively protects the rights of individuals in the wake of persistent abuses to the right to data protection.

It is the author's fervent hope that an application of this proposed hybridized approach spearheads a paradigm shift in thinking, so as to finally bring back to the individual the full power and control over his or

³⁰⁹ Report of the World Economic Forum *supra* note 318; Li, C, Li, D.Y., Miklau, G., and Suci, D. (2013). *A theory of pricing private data*. ICDT 13: Proceedings of the 16th International Conference on Database Theory;

³¹⁰ Holt *supra* note 317

her digital footprints, leading to liberty and economic prosperity truly felt and experienced by every *Juan*.

BIBLIOGRAPHY

Primary Sources

Laws, Administrative Rules and Regulations, and Court Rules

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union, L 281, 23/11/1995 P. 0031 - 0050

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119/1-88, 4/5/2016

1987 Constitution of the Republic of the Philippines

Act No. 3815 or the Revised Penal Code of the Philippines

Republic Act no. 386 or the New Civil Code of the Philippines

Republic Act no. 1405 or Bank Secrecy Law

Republic Act no. 2000 or Electronic Commerce Act of 2000

Republic Act no. 4200 or Anti Wiretapping Law

Republic Act no. 6426 or Foreign Currency Deposit Act of the Philippines

Republic Act no. 9160 or Anti Money-Laundering Act of 2001

Republic Act no. 9208, as amended by Republic Act no. 10364 or the Expanded Anti-Trafficking in Persons Act of 2012

Republic Act no. 9262 or Electronics Engineering Law of 2004

Republic Act no. 9372 or the Human Security Act of 2007

Republic Act no. 9510 or Credit Information System Act

Republic Act no. 9775 or Anti-Child Pornography Act of 2009

Republic Act no. 10173 or Data Privacy Act

Republic Act no. 10175 or Cybercrime Prevention Act

Republic Act no. 11055 or Philippine Identification System Act

1997 Rules of Civil Procedure

2008 Manual of Regulations for Banks

Bureau of Internal Revenue, Revenue Memorandum Circular 55-2013: Reiterating taxpayers' obligations in relation to online business transactions, 5 August 2013

National Telecommunications Commission, Memorandum Circular No. 04-06-2007: Data log retention of telecommunications traffic

Treaties and International Conventions

European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, available at: <https://www.refworld.org/docid/3ae6b3b70.html> [accessed 14 January 2020]

Organization of American States (OAS), *American Convention on Human Rights*, "Pact of San Jose", Costa Rica, 22 November 1969, available at: <https://www.refworld.org/docid/3ae6b36510.html> [accessed 22 December 2019]

Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights* ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), available at:

<https://www.refworld.org/docid/3ae6b3630.html> [accessed 21 December 2019]

UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, available at: <https://www.refworld.org/docid/3ae6b38f0.html> [accessed 14 January 2020]

UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: <https://www.refworld.org/docid/3ae6b3aa0.html> [accessed 13 January 2020]

UN General Assembly, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, 18 December 1990, A/RES/45/158, available at: <https://www.refworld.org/docid/3ae6b3980.html> [accessed 14 January 2020]

UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at: <https://www.refworld.org/docid/3ae6b3712c.html> [accessed 22 December 2019] [UDHR]

United Nations. *Universal Declaration of Human Rights*, available at <https://www.un.org/en/universal-declaration-human-rights/index.html> (last visited 10 January 2020)

UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation*, 8 April 1988, available at: <https://www.refworld.org/docid/453883f922.html> [accessed 21 December 2019]

UN Human Rights Committee (HRC), *CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, 2 November 1999, CCPR/C/21/Rev.1/Add.9, available at:

<https://www.refworld.org/docid/45139c394.html> [accessed 14 January 2020]

UN Human Rights Committee (HRC), *CCPR General Comment No.34: Article 19 (Freedom of opinion and expression)*, 21 July 2011, available at: <https://www.refworld.org/docid/4e38efb52.html> [accessed 14 January 2020]

United Nations Human Rights Council. *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 30 June 2014, A/HRC/27/37

UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation*, 8 April 1988, available at: <https://www.refworld.org/docid/453883f922.html> [accessed 21 December 2019] [General Comment 16]

UN Human Rights Council, *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17 April 2013, A/HRC/23/40

Philippine Case Law

Albenson v. CA, G.R. No. 88694, 11 January 1993

Andrade v. CA, G.R. No. 127932, 7 December 2001;

Angeles v. Calasanz, G.R. No. 42283, March 18, 1985

Arquero v. Hon. Flojo and RCPI, G.R. No. 68111, December 20, 1988;

Arrieta v. National Rice and Corn Corporation, G.R. No. L-15645, 31 January 1964

Arroyo v Berwin, G.R. L-10551, March 3, 1917

Ayala Corporation v. Ray Burton Development Corporation, G.R. No. 126699, August 7, 1998

Baksh v. CA, G.R. No. 97336, 19 February 1993

Basic Books Philippines, Inc. v Lopez, et al, G.R. No. L-20753, February 28, 1966

Bough vs. Cantiveros, 40 Phil. 209 [1919]

Cabunting v BPI Family Savings Bank, G.R. No. 201927, February 17, 2016

Cadiz v. Brent, G.R. 187417, February 24, 2016

De los Santos v. Gorospe, et al., L12023, Apr. 29, 1959

Disini v. Secretary of Justice, G.R. No. 203335, February 11, 2014

Drilon v. CA, G.R. No. 107019, 20 March 1997

Edilberto Alcantara v Cornelio B. Rita, Jr., G.R. 136996, December 14, 2001

Elegir v. Philippine Airlines, Inc., G.R. No. 181995, July 16, 2012;

Equitable PCI Bank v. Ng Sheung Ngor, G.R. 171545, December 19, 2007;

Ferrazzini v. Gsell, G.R. No. 10712, August 10, 1916

Gabriel v. Monte de Piedad, et al, G.R. No. 47806, April 14, 1941,

Garcia v. Salvador, G.R. No. 168512, 20 March 2007

General Enterprises, Inc. v Lianga Bay Logging Co., G.R. No L-18487, August 31, 1964;

Globe Mackay v. CA, G.R. No. 81262, 25 August 1989

Gregorio v. CA, G.R. No. 179799, 11 September 2009

H.L. Carlos Construction, Inc. v. Marina Properties Corp., 466 Phil. 182, 197, 2004

Insular Life Assurance Co. vs. Assets Builders Corporation, 422 SCRA 148 [2004]

Land Bank v. Republic, G.R. No. 150824, February 4, 2008

Leal vs. Intermediate Appellate Court, 155 SCRA 994 [1987]

Liguez v Court of Appeals, G.R. No. L-11240, December 18, 1957

Locsin II v. Meken Food Corporation, G.R. No. 192105, December 9, 2013

Luxuria Homes, Inc. vs. Court of Appeals, 302 SCRA 315, 1999

Magbanua v. Junsay, G.R. No. 132659, 12 February 2007

Maranan v. Perez, GR L-22272, Jun. 26, 1967;

McConnel, et al. v. Court of Appeals, L-10510, Mar. 17, 1961

Morfe v. Mutuc , G.R. L-20387, January 31, 1968

Navarra vs. Planters Development Bank, 527 SCRA 562, 2007

Ople v. Torres, G.R. 127685, July 23, 1998

Pe v. Pe, G.R. No. L-17396, 30 May 1962

People v. Pomar, G.R. No. L-22008, November 3, 1924

Perez v. CA, G.R. No. 162580, January 27, 2006

Republic v. Court of Appeals, G.R. No. 126316, June 25, 2004.

Rizal Commercial Banking Corporation v. Court of Appeals, G.R. No. 133107, March 25, 1999

Rivera, et al. v. Colago, et al., L-12323, Feb. 24, 1961

Philippine Export and Foreign Loan Guarantee Corporation v. V. P. Eusebio Construction, Inc., G.R. No. 140047, July 13, 2004

Philippine National Bank vs. Court of Appeals, 262 SCRA 464, 1996

Philippine National Bank vs. Court of Appeals, 238 SCRA 20, 1994

Privatization and Management Office v. Legaspi Towers 300, Inc., 611 Phil. 16, 28, 2009

Que v. IAC, G.R. No. 66865, 13 January 1989

Quisaba v. Sta. Ines, G.R. No. L-38088, 30 August 1974

San Diego v. Municipality of Naujan, G.R. No. L-9920, February 29, 1960

Saudi Arabian Airlines v. CA, G.R. 122191, October 8, 1998

Sea Commercial Company v. CA, G.R. No. 122823, 25 November, 1999

Spouses Guanio v. Makati Shangrila, G.R. 190601, 7 February 2011

Spouses Isagani Castro and Diosdada Castro v Angelina de Leon Tan, et al, G.R. 168940, November 24, 2009

Spouses Litonjua v. L.R. Corporation, G.R. No. 130722, March 27, 2000;

Spouses Panlilio v. Citibank, N.A., G.R. No. 156335, November 28, 2007

St. Louis v. CA, G.R. L-46061, 14 November 1984

Sweet Lines, Inc. v. Teves, G.R. No. L-37750, May 19, 1978

Tamio v. Ticson, 485 Phil. 434, 443 (2004)

Tanjanco v. CA, G.R. No. L-18630, 17 December 1966

Tenchavez v. Escano, 122 Phil. 752, 765 (1965)

University of the East v. Jader, G.R. No. 132344, 17 February 2000

Velayo v. Shell, G.R. No. L-7817, 31 October 1956

Wassmer v. Velez, G.R. No. L-20089, 26 December 1964

Yuchengco vs. Dacuycuy, 104 SCRA 668, 1981

National Privacy Commission of the Philippines, In re: Violations of the Data Privacy Act by several companies operating online lending applications

National Privacy Commission of the Philippines, CIDBN No. 18-J-162, Facebook Forced Logout 2018

National Privacy Commission of the Philippines, CIDBN No. 18-058, Wendy's Restaurant, Inc (PRO) Data Breach 2018

National Privacy Commission of the Philippines, CIDBN No. 17-043, Jollibee Foods Corporation 2018

Secondary Sources

Publications

Agpalo, R., Conflict of Laws (Private International Law), 2004 Ed

2 Arturo M. Tolentino, Commentaries and jurisprudence on the Civil Code of the Philippines (2004)

4 Arturo M. Tolentino, Commentaries and jurisprudence on the Civil Code of the Philippines (2002)

Angwin, J. (2014). *Dragnet Nation: A quest for privacy, security, and freedom in a world of relentless surveillance*, New York: Times Books.

American Civil Liberties Union. (2014). *Privacy rights in the digital age: A proposal for a new General Comment on the right to privacy under Article 17 of the International Covenant on Civil and Political Rights*, available at <https://www.aclu.org/other/human-right-privacy-digital-age> [accessed 13 January 2020] [ACLU Report]

Asian Business Law Institute. (2018). *Regulation of cross-border transfers of personal data in Asia: Jurisdictional report of the Republic of the Philippines*.

Casis, R. 2012. *Analysis of Philippine Law and Jurisprudence on Torts and Quasi-delicts*, UP College of Law.

Council of Europe, Committee of Ministers, Supervision of the Execution of Judgments and Decisions of the European Court of Human Rights, March 2014, 7th Annual, available at: <https://www.refworld.org/docid/5347cd3e4.html> [accessed 21 December 2019]

Council of Europe: European Court of Human Rights, The right to property: A guide to the implementation of Article 1 Protocol No. 1 of the European Convention on Human Rights, August 2003, Human rights handbooks, No. 4, available at: <https://www.refworld.org/docid/49f1810d2.html> [accessed 21 December 2019]

Council of Europe: European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, 31 December 2016, available at: <https://www.refworld.org/docid/5a016ebe4.html> [accessed 21 December 2019]

Council of Europe: European Court of Human Rights, Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights, January 2007, Human rights handbooks, No. 7, available at: <https://www.refworld.org/docid/49f183a32.html> [accessed 21 December 2019]

Coquia, J.R. and Aguilin-Pangalangan, E. (2000). *Conflict of laws: Cases, materials and comments*. Central Book Supply Inc.; Quezon City

De Leon, H.S. and de Leon, H.M., *The Law on Obligations and Contracts*, 2014 Revised Edition, Rex Bookstore: Quezon City, Philippines.

European Union Agency for Fundamental Human Rights, *Handbook on European Data Protection Law 2018 Edition*, available at <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law>, at p. 79 (last visited 8 January 2020)

McLuhan, M. (1964). *The Medium is the Message: Understanding Media: The Extensions of Man*, <https://web.mit.edu/allanmc/www/mcluhan.mediummessage.pdf> [accessed 19 February 2020]

Paras, E.L., *Philippine Conflict of Laws* (6th Ed., 1984)

Salonga, J. *Private International Law* (1995 Ed.)

UN High Commissioner for Refugees (UNHCR), *Guidance on the Protection of Personal Data of Persons of Concern to UNHCR*, 23 August 2018, available at: <https://www.refworld.org/docid/5b360f4d4.html> [accessed 21 December 2019]

Journal Articles

Allen, A.L., *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 750-57 (1999);

Barrigar, J. et al., *Let's not get psyched out of privacy: Reflections on withdrawing consent to the collection, use and disclosure of personal information*, 44 Can. Bus. L.J. 54, 56 2006-2007;

Belk, R. (2016). *Extended self and the digital world*. *Current Opinion in Psychology*, volume 10, 55-54

Bloustein, E.J. (1964). *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*. 39 N.Y.U. L. Rev. at 971.

Ciuriak, D. *The Knowledge-Based and Data-Driven Economy: Quantifying the Impacts of Trade Agreements*. CIGI Paper No. 156. Waterloo, ON: CIGI. www.cigionline.org/publications/knowledge-based-and-data-driven-economy-quantifying-impacts-trade-agreements.

Cohen, J.E., *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 142328 (2000);

Craven, J.B. Jr., (1976). *Personhood: The Right to be Let Alone*. Duke L.J. 699;

Donnelly, C. (18 January 2018). "How to transfer data to a 'third country' under the GDPR". *IT Governance Blog En*. Retrieved 4 April 2020; EU Network of Independent Experts on Fundamental Right (2006), *Commentary of the Charter of Fundamental Rights of the European Union*, available at <https://sites.uclouvain.be/cridho/documents/Download.Rep/NetworkCommentaryFinal.pdf> [accessed 14 January 2020]

Eggers, W.D., Hamill, R., and Ali, A. (2013). Data as the new currency: Government's role in facilitating the exchange. *Deloitte Review* (2013) 13, 18-31.

Florencio, Patrik S. and Ramanathan, Erik D. (2001). *Secret Code: The Need for Enhanced Privacy Protections in the United States and Canada to Prevent Employment Discrimination Based on Genetic and Health Information*. *Osgoode Hall Law Journal* 39.1: 77-116.

Garfinkel, S., and Cox, D., (2009). *Finding and archiving internet footprint*. Presented at the first Digital Lives Research Conference. London, England; John, Spacey. 2016. 6 types of digital footprint. *Simplicable*, November 24. <https://simplicable.com/new/digital-footprint>.

Holt, C.A., & Laury, S.K. (2002). Risk aversion and incentive effects. *American Economic Review*, 92, 1644-1655; Personal data: The emergence of a new asset class. Report of the World Economic Forum, Feb 2011;

Huberman, B.A., Adar, E., & Fine, L.R. (2005). Valuating privacy. *IEEE Security Privacy*, 3(5), 22-25;

Hann, I.-H., Hui, K.-L., Lee, S.-Y.T., & Png, I.P.L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, 24(2), 13-42;

Gkatzelis, V., Aperjis, C., & Huberman, B.A. (2012). Pricing private data. SSRN eLibrary;

Karanasiou, A.P and Douilhet, E., (2016). *Never mind the data: The legal quest over control of information and the networked self*. 100-105. 10.1109/IC2EW.2016.39.

Lai, E.R. (2011). *Motivation: A Literature Review*. Research report, available at http://images.pearsonassessments.com/images/tmrs/Motivation_Review_final.pdf [accessed 2 February 2020]

Laudon, K.C., *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept. 1996, at 92;

Lemley, M.L., *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1551 (2000);

Lessig, L., *Code and Other Laws of Cyberspace*, 142-63 (1999);

Li, C, Li, D.Y., Miklau, G., and Suciu, D. (2013). *A theory of pricing private data*. ICDT 13: Proceedings of the 16th International Conference on Database Theory; C.

Aperjis and B. A. Huberman. A market for unbiased private data: Paying individuals according to their privacy attitudes. *First Monday*, 17(5), 2012;

Acquisti, A., John. L., and Loewenstein, G.. What is privacy worth? In *Workshop on Information Systems and Economics*, 2009

Lynskey, O. (2014) "DECONSTRUCTING DATA PROTECTION: THE 'ADDED-VALUE' OF A RIGHT TO DATA PROTECTION IN THE EU LEGAL ORDER," *International and Comparative Law Quarterly*. Cambridge University Press, 63(3), pp. 569-597. doi: 10.1017/S0020589314000244.

Mell, P., *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, II BERKELEY TECH. L.J. 1, 26-41 (1996);

McFarland, M. (2012). *Privacy and balancing institutional power with individual freedom*. Markkula Center for Applied Ethics, Santa Clara University, available at <https://www.scu.edu/ethics/>

focus-areas/internet-ethics/resources/privacy-and-balancing-institutional-power/ (last visited 8 January 2020)

Murphy, R.S., *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 *GEO. L.J.* 2381, 2385 (1996);

Rachels, J. (1986). *Kantian Theory: The Idea of Human Dignity*. *The Elements of Moral Philosophy*, 114-117, 122-123.

J.H. Reiman, (1977). *Privacy, Intimacy, and Personhood*. 6 *Phil. & Pub. Aff.* 26;

Rotenberg, M. *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 *STAN. TECH. L. REV.* s, 92-97

Salahuddin A (2018) *Robert Nozick's Entitlement Theory of Justice, Libertarian Rights and the Minimal State: A Critical Evaluation*. *J Civil Legal Sci* 7: 234. doi: 10.4172/2169-0170.1000234

Schau, Terry. *Internet Use: Here, There, and Everywhere*. *Occupational Outlook Quarterly*, v44 n4 p40-47 Win 2000-2001

Tomuschat, C. (2008). *International Covenant on Civil and Political Rights*. United Nations Audiovisual Library of International Law, available at https://legal.un.org/avl/pdf/ha/iccpr/iccpr_e.pdf (last visited 10 January 2020)

Vishwajith, A.S. and Varanasi, S. (2012) *I am mine or am I? Analyzing the need for a property right in personal information*. *Indian Journal of Intellectual Property Law*. 5, 106, available at <http://www.commonlii.org/in/journals/INJIPLaw/2012+/9.pdf> [accessed 1 January 2020]

Warren, S.D. and Brandeis, L.D.. (1890). *The Right to Privacy*. *Harvard Law Review*, Vol. 4, No. 5; 193-220.

Weaver, S.D. and Gahegan, M. (2007). *Constructing, Visualizing, and Analyzing a Digital Footprint*. *Geographical Review*. Vol 97, No 3, *Geosurveillance* (July 2007), pp. 324-350.

Zuboff, S. (2015). *Big other: Surveillance capitalism and the prospects of an information civilization*. *Journal of Information Technology* (2015) 30, 75-39

Zuiderveen Borgesius, F.J. (April 2016). "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation". *Computer Law & Security Review*. doi:10.1016/j.clsr.2015.12.013. ISSN 0267-3649

European Union Court Decisions Case

Client Earth et. al v. EFSA, C-615/13 (2015)

Digital Rights Ireland Ltd. v. Ireland, C-293/12; C-594/12 (2014)

Dudgeon v. United Kingdom, Application no 7525/76 (1981)

Facebook/Whatsapp, Case No. COMP/M.7217 (2014)

Google/DoubleClick, Case No. COMP/M.4731 (2008)

Hoffmann-La Roche v. Commission, C-85/76 (1979)

Microsoft/LinkedIn, Case No. COMP/M.8124 (2016)

Microsoft/Skype, Case No. COMP/M.6281 (2011)

Niemitz v. Germany, Application no 72/1991/324/396 (1992)

Pretty v. United Kingdom, Application no 2346/02 (2002)

Worten Equipamentos para o Lar Sa v. ACT, C-342/12 (2013)

X v. Germany, Application 6699/74 (1977)

United States Court Decisions

Facebook v. Power, 91 U.S.P.Q.2d 1430 (2009)

Griswold v. Connecticut, 381 U.S. 479 (1965)

Pavesich v. New England Life Insurance Co. et. al, 122 Ga. 90 (1905)

Roe v. Wade, 410 U.S. 113 (1973)

United States Of America v. Bazaarvoice, Inc., No. 3:2013cv00133 - Document 286 (N.D. Cal. 2014)

Lectures

Artemio V. Panganiban, Safeguard Liberty, Conquer Poverty, Share Prosperity (Part Three – for the the Business Community), 4th Integrity Summit with the Makati Business Club and the European Chamber of Commerce and Industry, at Dusit Thani Hotel, Makati City, available at <https://cjpanganiban.com/2014/09/19/safeguard-liberty-conquer-poverty-share-prosperity-part-three-for-thebusiness-community/>

Artemio V. Panganiban, Safeguard Liberty, Conquer Poverty, Share Prosperity (Part Two – For the Legal Profession), Luncheon Fellowship of the Philippine Bar Association held, at the Tower Club, Makati City, March 26, 2014, available at <https://cjpanganiban.com/2014/03/26/safeguard-libertyconquer-poverty-share-prosperity-2/>

Artemio V. Panganiban, Unleashing Entrepreneurial Ingenuity, 12th General Assembly of the ASEAN Law Association, at the Makati Shangri-la Hotel, Makati City, Feb. 26 to Mar. 3, 2015, available at <https://cjpanganiban.com/2015/02/26/unleashingentrepreneurial-ingenuity/> accessed 10 March 2020

Artemio V. Panganiban, Visionary Leadership by Example, 9th National Ayala Young Leaders Congress, the San Miguel Corporation Management Training Center, Alfonso, Cavite, February 7, 2007, available at <https://cjpanganiban.com/2007/02/07/visionaryleadership-by-example-2/>

Miscellaneous

Businesswire. (2018). Hagens Berman: Facebook hit with class action lawsuit following massive user data scandal, available at <https://www.businesswire.com/news/home/20180409006426/en/Hagens-Berman-Facebook-Hit-Class-Action-Lawsuit-Massive> [accesses 1 April 2020]

Conrad, A. (2018). *The right to privacy under Philippine and international law*, available at <https://www.privacyph.net/2018/06/12/the-right-to-privacy-under-philippine-and-international-law/> (last visited 10 January 2020)

European Union: European Agency for Fundamental Rights, *Fundamental Rights Report 2018*, June 2018, available at: <https://www.refworld.org/docid/5b18f1b44.html> [accessed 21 December 2019]

Facebook Company Information, available at <https://about.fb.com/company-info/> [accessed 3 March 2020]

Facebook Terms and Conditions, available at <https://www.facebook.com/legal/terms/update> [accessed 3 March 2020]

Goodson, S. (2012). If you're not paying for it, you become the product. *Forbes*, available at <https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/#2d66dceb5d6e> (last visited December 22, 2019)

Google Terms and Conditions, available at <https://policies.google.com/terms?hl=en-US> [accessed 11 March 2020];
Google Products for All, available at <https://about.google/products/> [accessed 3 March 2020]
Google Products for Businesses, available at <https://about.google/products/> [accessed 3 March 2020]

Google Products for Developers, available at <https://developers.google.com/products?hl=en> [accessed 3 March 2020]

Hagens Berman. (2018). Facebook hit with class action lawsuit following massive user data scandal, available at <https://www.hbsslaw.com/cases/facebook-users-privacy/pressrelease/facebook-users-privacy-facebook-hit-with-class-action-lawsuit-following-massive-user-data-scandal> [accessed 3 April 2020]

Hootsuite, *Social media trends 2019*, available at <https://www.digitalmarketingcommunity.com/researches/social-media-trends-2019-hootsuite/> (last visited 8 January 2020)

Hulog, L. (2019). BIR studies ways on taxing digital economy in the Philippines, available at <https://ahccounting.com/bir-looks-methods-tax-digital-economy/> [accessed 1 April 2020]

Internet World Statistics, *Philippines internet usage, population statistics and Facebook subscribers*, available at <https://www.internetworldstats.com/asia.htm#ph> (last visited 4 January 2020)

Internet World Statistics, *Top 20 countries with the highest number of internet users*, available at <https://www.internetworldstats.com/top20.htm> (last visited 3 January 2020)

Personal data: The emergence of a new asset class. Report of the World Economic Forum, Feb 2011;

Sanchez, M.J. (2019). *Digital advertising expenditure share of total media ad spending in the Philippines from 2015-2020*, available at <https://www.statista.com/statistics/771570/digital-ad-spending-share-of-total-media-ad-spending-philippines/> (last visited 4 January 2020)

Taxamo. (2020). Digital tax developments in South-east Asia, available at <https://blog.taxamo.com/insights/digital-tax-news-south-east-asia> [accessed 3 April 2020]

Taxamo. (2020). Digital trends: International plans to tax the digital economy, available at <https://blog.taxamo.com/insights/international-digital-tax-trends> [accessed 3 April 2020]

We Are Social, *Digital in 2019 global report*, available at <https://wearesocial.com/uk/>

digital-2019, at 48 (last visited 2 January 2020)

We are Social, *Digital in 2019 Philippines report*, available at

<https://www.slideshare.net/>

DataReportal/digital-2019-philippines-january-2019-v01, at 34 (last visited 8 January 2020)