VOLUME 12 • NUMBER 01 • MAY 2023

University of St. La Salle Law Journal

University of St. La Salle BACOLOD

University of St. La Salle College of Law

WALTZING WITH AN ORWELLIAN REGIME

Discussions on the Right to Privacy, Information and Language Deception, and the Legality of the Big Tech

Republic of the Philippines
Supreme Court
Manila

FROM THE CHAMBERS OF:

Alfredo Benjamin S. Caguioa
ASSOCIATE JUSTICE

FOREWORD

Digitalization has undoubtedly been accelerated by the pandemic. Private institutions, such as schools, banks, and business enterprises, were quick to install or upgrade their information technology systems to keep up with the rapidly changing demands and landscape of the market. The government, albeit at a much more measured pace, had to devise alternative means to process transactions, render public service, and fulfill their mandates. The Judiciary, for example, allowed the electronic filing of complaints and charges, the conduct of virtual hearings, and the remote notarization of documents, and launched the first ever digital bar examinations in the country, among other innovations. As the nation emerges from this health crisis, the transitional digital measures introduced in the last three years are being reviewed and amplified to be permanently interwoven in the new normal.

With digitalization comes the demand for and commodification of information. One of the earliest government responses to the pandemic was to require the citizenry to accomplish health declaration forms, either

online or manually through pen and paper. These forms asked for personal information, even sensitive personal information, and knowingly or unthinkingly, we have given such information, including our full names, birthday, phone numbers, and home and email addresses. Lamentably, these innovations that were intended to provide essential public service have been hounded by allegations that the very data collected had been shared or sold without our knowledge and consent.

The Editorial Team of this Journal points out that legal scholars worldwide are ringing the warning bell over the decline of privacy and the rise of technology intrusions. Significant events of recent years lead one to argue that we are already in such a situation. There have been reports of hacking of databases of certain agencies, allowing access to the data of millions of Filipinos. Throughout the pandemic, phishing activities have grown rampant and sophisticated. Moreover, mobile phone users are being bombarded by unsolicited offers from unknown numbers on a daily basis.

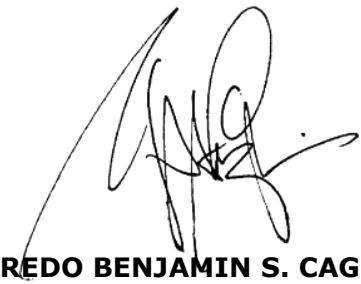
The government has our data. Private entities have our data. Entities lurking in the shadows have our data. The big question is, *what now?*

I commend the USLS Law Journal for fearlessly asking whether our institutions are equipped to combat the further unlawful processing and use of our information and whether the State is staying true to its constitutional duty to respect our right to privacy and freedom of expression. Likewise, I commend the contributors for these thought-provoking pieces that I hope would kick-start a wider conversation about the topics.

With this issue focusing on privacy, technology, and State power, the USLS Law Journal stays the course in its commitment to offer opinions on paramount issues that have been brought to the fore by current events, including

insights on legal issues submitted to and/or decided by the Supreme Court.

My congratulations to the USLS Law Journal for this issue and I hope that the publication continues to offer a venue for discourse, not only among members of the academe, but extending to an even broader audience that is the public.



ALFREDO BENJAMIN S. CAGUIOA
Associate Justice
Supreme Court of the Philippines

University of St. La Salle
College of Law
La Salle Avenue, Bacolod City, 6100

FROM THE OFFICE OF:

Rosanne Juliana R. Gonzaga LL.M.
DEAN, COLLEGE OF LAW

MESSAGE FROM THE DEAN

There are many discussions about the legality of big tech and its impact on people's privacy and information. The common concerns include the right to be free from unwanted surveillance, the use of language deception, and the protection of individuals from being exposed to harmful content. Big tech refers to dominant companies in the information technology industry that have the potential to transform the way we live and work. Its primary purpose is to improve efficiency and productivity in various fields. Such companies influence user behavior through online activities and control large amounts of user data without much regulation.

The rise of technology takes center stage in our daily lives. From how we communicate to making everyday decisions, it creates opportunities and challenges. Moreover, it allows us to develop a sense of individuality and freedom. With a few buttons, we can research any topic, find solutions to most problems, and connect with peers. Technology enables us to do more with less, but it also raises concerns about its potential misuse and exploitation.

Today, it is possible for anyone, including the government, to gain access to our personal information which we voluntarily surrender or upload to the world wide web, and to monitor our activities without our consent. Furthermore, the rise of the cloud enables us to store personal data in a seemingly secure environment. Thus, making it accessible to companies to use to identify and target us based on our interests.

One of the most important factors we must consider while using technology is the protection of our privacy. Many acknowledge the importance of the Data Protection Act of 2012, but very few understand its true impact. The law, as applied, provides for more transparency and accountability in how companies handle and use our personal information. Thus, it is of paramount importance to adopt a set of ethical rules when it comes to utilizing our digital assets.

In recent years, the ease by which people interact virtually through smart devices had led to the decline of the need for old-fashioned telephones. The way we consume information had changed as well. Gone were the days when we bought a newspaper from the newsstand and read about the happenings in our communities and the world. Today, we just needed to go online to get our fill of current events. The relative ease of virtual shopping made browsing for goods a delightful and convenient way to purchase products and services. The entertainment industry was no longer limited to just movies and television shows. We made vlogs and devoured social media using our handheld devices and downloaded applications. Big tech was now a part of every facet of our lives, from our work and to our education, to our hobbies and our relationships. It was not a surprise how quickly technology evolves. We no longer needed to carry around a pen and paper to express our thoughts and ideas.

In the academic setting, schools have adopted technology to deliver services efficiently. The modern

admission process allowed students to apply virtually without needing traditional paper forms. The virtual platform and various learning management systems made it very convenient for students to pursue their studies without leaving their homes. The use of a library catalog drastically decreased, and the instant search facility through the internet made this process almost obsolete. The routine of borrowing books declined with the availability of online resources for learning.

Two fundamental rights need to be protected in this digital age. The first is the freedom to use and control our information, and the second is the right to be informed about what affects us. Becoming careless with our digital lives exposes us to potentially harmful and life-threatening situations. We must therefore train ourselves to be cautious with our personal information and take steps to safeguard it. Borrowing the words of Benjamin Franklin, "an ounce of prevention is worth a pound of cure."

Nothing can replace our real-life interactions with our family and friends. We need to find a way to balance the benefits of technology with its drawbacks, allowing us to live more fulfilling and productive lives.

We acknowledge the hard work and discipline poured into creating this collection of masterful writing by the USLS Law Journal Team and its esteemed contributors. Congratulations! Animo!

Rosanne Juliana R. Gonzaga, Ll.M.
Dean, College of Law
University of St. La Salle

University of St. La Salle
College of Law
La Salle Avenue, Bacolod City, 6100

MESSAGE FROM THE EDITOR-IN-CHIEF

The University of St. La Salle College of Law – Law Journal is a hallmark of diverse legal thought and discussions. The information age undeniably carries new legal issues surrounding how technology and digitalization creep into our private lives.

In this inaugural issue, twelve contributions explore the intricacies besetting the Philippine society and the international arena in the information age. These articles and essays set out the policy frameworks and legal parameters from various fields. Every aspect of this issue is intended to further the legal narrative among students and law professors that make up the foundation of a Lasallian lawyer.

The first essay by *Atty. Daniel Victor L. Zayco,* under Privacy in the Information Age, analyzes the unenumerated rights methodology and the review of privacy in understanding this concept. When a right is not expressly provided in the Constitution, and when such a right is the subject of resolution in a case, how may the Court decide on this matter?

In the second contribution, *Atty. Rhodora P. Lo* explores the novel "right to be forgotten" and the emerging information and communications technology issues confronting our privacy today. My essay, the *Privacy*

Paradox and the Pitfalls of Unthinking, deals with the legal aspects of renouncing our privacies to receive a highly personalized service. We become more desensitized to such a process, subjecting ourselves to technological unthinking with our complicity.

In their respective essays*, Frances Zarah P. de la Peña and Steffani Mitchelle M. Patriarca* reflect on the issues of privacy as a derogable right. Yet a violation thereof is a sacrilege to humanity.

Part II of the issue underlines Language and Information Deception. *Atty. Maria Reylan M. Garcia's* article explores the role of language deception in estafa cases, especially concerning investment scams and financial schemes. Atty. Garcia further elucidates the creeping effect of deceit in these cases. *April Therese L. Escarda* and *Jose Adrian Miguel P. Maestral* address the challenges of blurring the case of free speech and hiding the truth from the public. Their essays highlight the underlying issues surrounding freedom of expression and the right to access information wherein deepfakes and false narratives dominate the powerplay in the technological stage.

Under Part III or the Reflections on Artificial Intelligence ("AI") and Big Tech, *Justitia Deus Ex Machina: The Legality and Feasibility of Artificial Intelligence as Judge and Justice in the Philippines* by *Judge Michael Hanz D. Villaster* offers an exposition of the legality of AI in judiciary matters. Judge Villaster examines this concept as a *deus ex machina* confronting the future of court decisions.

Jarre V. Gromea further examines the role of the big tech or the "digital leviathans" in managing the state of technology and the seemingly intertwined reality of how online dynamics work. On the other hand, *Bryan Alvin Rommel Y. Villarosa* explores the legality of content creation tailored to our preferences and the confronting legal issues these may entail in our pursuit of freedom.

The last contribution, a comment by *Gabriel Christian J. Lacson*, discusses the constitutional change in the Philippines and the legal issues confronting the current Philippine setting, especially in the age of information.

May this publication issue continue the USLS Law Journal's commitment to promoting legal discussions and instilling questions that spark constructive debates in tandem with the ever-changing policy developments in our modern society.

On behalf of the USLS Law Journal 2022-2023, I am grateful for the gift of collective effort and dedication by the team behind this publication.

Animo, La Salle!

RACHEL LOIS B. GELLA
Editor-in-Chief
USLS Law Journal 2022-2023

CONTENTS

LEGAL ARTICLES AND ESSAYS

1

PRIVACY IN THE INFORMATION AGE

1

A Review of Privacy and Unenumerated Rights Methodology

by Atty. Daniel Victor L. Zayco

REVIEW OF PRIVACY AND UNENUMERATED RIGHTS METHODOLOGY

*Atty. Daniel Victor L. Zayco**

I. INTRODUCTION

"Liberty finds no refuge in a jurisprudence of doubt."[1]

In *Dobbs v. Jackson Women's Health Organization*,[2] the Supreme Court of the United States (SCOTUS) overruled the controversial case of *Roe v. Wade* and its holding that a woman has a constitutional right to an abortion.[3] *Roe's* privacy-as-liberty reasoning for establishing an unenumerated right to abortion was built upon, modified, and made part of the reasoning in subsequent cases establishing other previously unspecified liberties.[4] The only issue in *Dobbs* was about abortion, and the majority decision said that "[n]othing in [the] opinion should be understood to cast doubt on precedents that do not concern abortion."[5] Despite this caveat, the decision does put into question the *method* of identifying unenumerated fundamental rights in the Constitution.

Justice Francis Jardeleza of the Philippine Supreme Court states the problem: "Unlike the case of rights that can be located on the text of the Bill of Rights, the rules concerning locating unenumerated 'fundamental' rights, however, are not clear."[6] When a purported right is not one of those explicitly mentioned in the Constitution, the question of whether it is a right is answered only by the Supreme Court. As Justice Anthony Kennedy of the SCOTUS said: "The identification and protection of fundamental rights is an enduring part of the judicial duty to interpret the Constitution."[7] The point of difference in jurisprudence, and the issue that this writing looks into, is how the Court identifies unenumerated rights or rights not explicitly in the text of the Constitution.[8]

---

* *'16* A.B. Pol. Sci.; *'20* J.D., University of St. La Salle - Bacolod.

1 *Planned Parenthood of Southeastern Pa. v. Casey*, 505 U.S. 833 (1992) (overruled in *Dobbs v. Jackson Women's Health Organization, infra*).

2 597 U. S. ___ (2022).

3 410 U. S. 113, 153 (1973) (overruled in *Dobbs,* id.)

4 *See infra* Part II.

5 *Dobbs*, supra note 2, slip op. at 66.

6 *Falcis III v. Civil Registrar General*, G.R. No. 217910, September 3, 2019 (J. Jardeleza, concurring opinion).

7 *Obergefell v. Hodges*, 576 U. S. 644 (2015).

8 For a more comprehensive discussion on this topic *see* Robert Farrell, *An Excess of Methods: Identifying Implied Fundamental Rights in the Supreme Court*, Saint Louis University Public Law Review: Vol. 26: No. 2, Article 5. (2007) <https://scholarship.law.slu.edu/plr/vol26/iss2/5> (visited August 30, 2022) and *Versoza v.People*, G.R. No. 184535, September 3, 2019 (J. Jardeleza, separate opinion) <https://sc.judiciary.gov.ph/9168/> (visited August 30, 2022).

Part II looks at how the right to privacy and other unenumerated rights have developed through jurisprudence. Part III examines the methods that the Court has used to identify unenumerated rights. Part IV examines how the *Dobbs* decision could impact other unenumerated rights, if at all.

II. OVERVIEW OF PRIVACY AND UNENUMERATED RIGHTS

A. *Defining Terms, Scope, and Significance*

Before proceeding, it is important first to define the terms being used. "Privacy," as used in this article, refers to "decisional privacy" or "the right of individuals to make certain kinds of fundamental choices with respect to their personal and reproductive autonomy."[9] It is to be distinguished from "locational privacy," or "privacy that is felt in physical space, such as that which may be violated by trespass and unwarranted search and seizure,"[10] and "informational privacy" or "the right of individuals to control information about themselves."[11] These two kinds of privacy will not be discussed here anymore. An "unenumerated right" is not expressly mentioned in the Constitution, as distinguished from those expressly listed in the Bill of Rights. While some American writers differ on the semantics of this point,[12] for the purposes of this writing, "unenumerated rights" is understood to be part of the doctrine of substantive due process.

The review of privacy/liberty jurisprudence developing in the United States has significant importance for the Philippines, considering that SCOTUS cases influenced local jurisprudence on the subject. The right to privacy was first recognized in the Philippines in the case of *Morfe v. Mutuc*.[13] Taking inspiration from Justice William Douglas, the Court separated privacy from liberty under the Due Process Clause, thus: "The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional

---

9 *Vivares v. St. Therese College,* G.R. No. 202666, September 29, 2014 (citing Chief Justice Reynato Puno's Speech "The Common Right to Privacy", delivered before the Forum on The Writ of Habeas Data and Human Rights, sponsored by the National Union of Peoples' Lawyers on March 12, 2008 at the Innotech Seminar Hall, Commonwealth Ave., Quezon City).

10 *Id.*

11 *Id.*

12 *Compare* Lee Goldman, *The Constitutional Right to Privacy*, 84 Denv. U. L. Rev. 601, 603 n. 13 (2006) ("The constitutional right to privacy, as used in this article, refers to the unenumerated right to privacy protected by substantive due process.") *with* Randy E. Barnett, *Scrutiny Land*, 106 Mich. L. Rev. 1479, 1486 n. 30 (2008).

13 G.R. No. L-20387, January 31, 1968.

protection."[14] Note, however, that *Morfe* was decided in 1968, prior to *Roe*, and is not a decisional privacy case, unlike the soon-to-be-discussed *Griswold* or *Roe*. In *Ople v. Torres*,[15] the Court, again following *Griswold*, held that privacy is recognized and enshrined in various provisions of the Bill of Rights of the 1987 Constitution.[16] The Court also held that the right to privacy is a fundamental one and that burdening it requires a compelling state interest that is narrowly tailored.[17] Like *Morfe*, *Ople* is not a decisional privacy case but one concerning informational privacy. Despite the difference in the type of privacy involved, Philippine case law has recognized a general right to privacy.[18]

While abortion in the Philippines remains a felony under Articles 256, 257, 258, and 259 of the Revised Penal Code, what is under consideration now is not the specific rights (such as one for abortion) but how these rights are identified.

As a limitation, this article will not attempt to critique the methods used by the Court – that have already been done by more competent writers in Constitutional Law. The exploration of the methods used is for the purpose of seeing what, when, and how they have been used or not used.

B. *Development of Privacy and Liberty Jurisprudence*

The word privacy is not found in the United States Constitution. In the 1987 Constitution of the Philippines, it appears only once in Article III, Section 3, providing for the privacy of communication and correspondence.

However, jurisprudence, both here and in the United States has recognized a general right to privacy. *Griswold v. Connecticut*,[19] the case that gave rise to the unenumerated right to privacy,[20] held that a law prohibiting the use and distribution of contraceptives, and counseling the use of it, violated the right to privacy of married couples. While not explicitly in the Constitution, privacy emanates from its various express rights. The Court explained that "specific guarantees in the Bill of Rights

---

14 *Id.*

15 *Ople v. Torres*, G.R. No. 127685, July 23, 1998.

16 *Id.*

17 *Id.*

18 *See, e.g., Imbong v. Ochoa, Jr.,* G.R. No. 204819, April 8, 2014 (*the RH Law Cases*).

19 381 U. S. 479 (1965).

20 *See* Farrell, *supra* note 8, at 211 (describing *Griswold* as "the first of the modern privacy cases").

have penumbras, formed by emanations from those guarantees that help give them life and substance."[21] From these penumbras and emanations come the right to privacy.

> Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment, in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[22]

The use of contraceptives as a privacy right was extended to unmarried couples in *Eisenstadt v. Baird*[23] on equal protection grounds, with the Court saying: "If the right of privacy means anything, it is the right of the individual, *married or single*, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."[24]

In *Roe v. Wade*,[25] the Court put *Griswold*'s privacy right into the sphere of substantive due process that it had once rejected. In ruling that a woman has a fundamental right to an abortion, the Court said:

> The Constitution does not explicitly mention any right to privacy. In a line of decisions, however, x x x, the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. x x x

---

21 *Griswold v. Connecticut*, *supra* note 19, at 484.

22 *Id.*

23 *Eisenstadt v. Baird,* 405 U. S. 438 (1972).

24 *Id.* At 453 (italics supplied).

25 *Roe v. Wade*, supra note 3.

> This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.[26]

This right, *Roe* held, is not absolute, thus: "the right of personal privacy includes the abortion decision, but that this right is not unqualified, and must be considered against important state interests in regulation."[27] That regulatory framework was first set in *Planned Parenthood v. Casey*.[28] There the Court upheld *Roe's* "central holding" – that a woman has a right to an abortion, albeit not an absolute one – but replaced *Roe's* trimester framework with viability and that state regulation must not impose an undue burden on a woman's decision to terminate her pregnancy. "Only where state regulation imposes an undue burden on a woman's ability to make this decision does the power of the State reach into the heart of the liberty protected by the Due Process Clause."[29] A regulation is an undue burden "if its purpose or effect is to place a substantial obstacle in the path of a woman seeking an abortion before the fetus attains viability."[30] Simply put, the state could regulate abortion from conception[31] as long as it did not impose an undue burden on the woman's right to have an abortion – which was higher than the state's interest before viability.

Note that while Roe has assimilated the right to privacy into substantive due process doctrine, they were initially in separate spheres of the Court's unenumerated rights jurisprudence. *Griswold* explicitly avoided linking privacy to due process.[32] The rejection was to avoid being linked to he recently discredited line of cases related to *Lochner v. New York*[33] and

---

26 *Id.* At 152-53.

27 *Id.* At 154.

28 *Planned Parenthood v. Casey*, supra note 1.

29 *Id.* At 874.

30 *Id.*. At 878.

31 *Id.* At 872 ("Though the woman has a right to choose to terminate or continue her pregnancy before viability, it does not at all follow that the State is prohibited from taking steps to ensure that this choice is thoughtful and informed. Even in the earliest stages of pregnancy, the State may enact rules and regulations designed to encourage her to know that there are philosophic and social arguments of great weight that can be brought to bear in favor of continuing the pregnancy to full term and that there are procedures and institutions to allow adoption of unwanted children as well as a certain degree of state assistance if the mother chooses to raise the child herself.").

32 *See Griswold v. Connecticut*, supra note 19, at 481-82.

33 198 U.S. 45 (1905).

its liberty to contract.[34] Hence, in the cases following *Roe*, privacy would be replaced by liberty under the Due Process Clause. However, they remain inextricably linked. For example, in *Lawrence v. Texas*[35] the SCOTUS said:

> There are broad statements of the substantive reach of liberty under the Due Process Clause in earlier cases, including *Pierce v. Society of Sisters*, 268 U.S. 510 (1925), and *Meyer v. Nebraska*, 262 U.S. 390 (1923); *but the most pertinent beginning point is our decision in Griswold v. Connecticut*, 381 U.S. 479 (1965).[36]

Also in *Lawrence*, the Court reversed the conviction of two homosexual men for violating a Texas statute that made it criminal to have "deviant sexual intercourse with another individual of the same sex." It overturned a previous case sustaining a law-making sodomy criminal.[37] The ruling in *Lawrence* would base liberty on individual dignity. The Court held:

> The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government. "It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter." Casey, supra, at 847. The Texas statute furthers no legitimate state interest which can justify its intrusion into the personal and private life of the individual.[38]

The SCOTUS also used this emphasis on individual dignity and autonomy as a basis in ruling that same-sex couples have a fundamental right to marry under the Due Process Clause.[39]

---

[34] *Griswold v. Connecticut*, supra note 19, at 481-82. *Lochner* and its progeny will not be discussed here.

[35] *Lawrence v. Texas*, 539 U. S. 558 (2003).

[36] *Id.* at 564 (Italics supplied) *Cf.* Jamal Greene, *The So-Called Right to Privacy*, 43 U.C. DAVIS L. REV. 715 (2010). (arguing that the right to privacy is no more).

[37] *Bowers v. Hardwick*, 478 U.S. 186 (1986).

[38] *Lawrence v. Texas*, supra note 35, at 578.

[39] *Obergefell v. Hodges*, supra note 7.

III. METHODS OF IDENTIFYING UNENUMERATED PRIVACY RIGHTS

Two methods have come out of the privacy and liberty cases that have been used by the SCOTUS to identify unenumerated rights in the Constitution in relevant and recent cases. The previously mentioned cases in Part II comprise the first method: determining whether the right involves choices central to personal dignity and autonomy, or are central to liberty under the Due Process Clause.[40]

In *Casey*, the Court held that "[a]t the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State."[41] In *Lawrence*, the Court said "[l]iberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[42] In *Obergefell*, Justice Kennedy declared "the right to personal choice regarding marriage is inherent in the concept of individual autonomy."[43]

The second method of identifying unenumerated rights is the use of history and tradition as provided in *Washington v. Glucksberg.*[44] As Chief Justice William Rehnquist explained:

> Our established method of substantive-due-process analysis has two primary features: First, we have regularly observed that the Due Process Clause specially protects those fundamental rights and liberties which are, objectively, deeply rooted in this Nation's history and tradition and implicit in the concept of ordered liberty, such that neither liberty nor justice would exist if they were sacrificed. Second, we have required in substantive-due process cases a careful description of the asserted fundamental liberty interest. Our Nation's history, legal traditions, and practices thus provide the crucial guideposts for responsible decision making that direct and restrain our exposition of the Due Process Clause.[45]

---

40 *See* Goldman, supra note 12, at 602, 604-11. *See, however,* Farrell, supra note 8, at Part IV listing seven methods used by the SCOTUS to identify unenumerated rights.

41 *Planned Parenthood v. Casey*, supra note 1, at 851.

42 *Lawrence v. Texas*, supra note 35, at 562.

43 *Obergefell v. Hodges*, supra note 7. *See also* Goldman, supra note 12.

44 521 U.S. 702 (1997).

45 *Id.* at 720-21 (citations and internal quotation marks omitted).

In *Glucksberg*, the Court held that there is no fundamental right to assisted suicide after surveying "more than 700 years of Anglo-American common law tradition,"[46] and determining that no such right was "deeply rooted in history and tradition." In *Dobbs,* the test was simply stated as whether the right is deeply rooted in our history and tradition and whether it is essential to our Nation's scheme of ordered liberty."[47]

This second test was formulated to put a limit on substantive due process and unenumerated rights. In the words of Chief Justice Rehnquist:

> But we have always been reluctant to expand the concept of substantive due process because guideposts for responsible decision making in this unchartered area are scarce and open-ended. By extending constitutional protection to an asserted right or liberty interest, we, to a great extent, place the matter outside the arena of public debate and legislative action. We must therefore exercise the utmost care whenever we are asked to break new ground in this field, lest the liberty protected by the Due Process Clause be subtly transformed into the policy preferences of the Members of this Court.[48]

Justice Samuel Alito emphasized in *Dobbs* that reliance on "liberty" alone was not enough in identifying unenumerated rights:

> Historical inquiries of this nature are essential whenever we are asked to recognize a new component of the "liberty" protected by the Due Process Clause because the term "liberty" alone provides little guidance. "Liberty" is a capacious term. As Lincoln once said: "We all declare for Liberty; but in using the same word we do not all mean the same thing."[49]

With these two methods, what now is the problem? The SCOTUS has not been clear when one or the other is the applicable test or if one or the other has been overruled.

---

[46] *Dobbs v. Jackson Women's Health Organization,* supra note 2, slip op. at 13 (internal quotation marks omitted).

[47] *Id.* slip op. at 12.

[48] *Washington v. Glucksberg*, supra note 44, at 720 (citations and internal quotation marks omitted).

[49] *Dobbs v. Jackson Women's Health Organization, supra* note 2, slip op. at 13.

Glucksberg was decided in 1997, but in 2003 the *Lawrence* Court ignored the history and tradition test and did so again in 2015 in *Obergefell.* Recall that *Lawrence* overturned *Bowers*.[50] *Bowers* was a 1986 case that would lay the foundations for *Glucksberg's* test. In that case, the Court upheld a Georgia anti-sodomy statute. In ruling that there was no fundamental right to engage in sexual sodomy, the Court did a historical inquiry and found that sodomy had always been a crime.

When *Lawrence* overruled *Bowers*, it said that "history and tradition are the starting point but not in all cases the ending point of the substantive due process inquiry."[51] In *Obergefell*, the Court, following *Lawrence*, said: "Yet while [*Glucksberg's*] approach may have been appropriate for the asserted right there involved (physician-assisted suicide), it is inconsistent with the approach this Court has used in discussing other fundamental rights, including marriage and intimacy."[52] While there was no express repudiation of any further use of the method, this appeared to be the end of the line for *Glucksberg's* test in unenumerated rights jurisprudence. That is, until it was revived in *Dobbs.*

IV. *DOBBS* RETURNS TO HISTORY AND TRADITION

In *Dobbs*, the SCOTUS overruled *Roe* and *Casey*, on the reasoning that abortion was expressly protected by the Constitution and that the history of common law and the United States showed that abortion was not considered a right prior to the 1973 decision in *Roe*, but was a crime. Justice Alito, writing for the majority, said:

> We hold that *Roe* and *Casey* must be overruled. The Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision, including the one on which the defenders of Roe and Casey now chiefly rely—the Due Process Clause of the Fourteenth Amendment. That provision has been held to guarantee some rights that are not mentioned in the Constitution, but any such right must be deeply rooted in this Nation's history and tradition and implicit in the concept of ordered liberty.[53]

---

50 *Bowers v. Hardwick*, supra note 37.

51 *Lawrence v. Texas*, supra note 35, at 572 citing *County of Sacramento v. Lewis*, 523 U.S. 833, 857 (1998) (J. Kennedy, concurring).

52 *Obergefell v. Hodges*, supra note 7.

53 *Dobbs v. Jackson Women's Health Organization,* supra note 2, slip op. at 5.

The majority decision did not go into whether other previous substantive due process cases fail the history and tradition test because *Dobbs* was only about abortion. While heavily criticizing substantive due process,[54] the Court did not expressly say that the method used in cases like *Griswold*, *Lawrence*, and *Obergefell* is no longer viable in constitutional inquiry.[55]

However, Justice Clarence Thomas, one of the members of the majority, wrote separately to state his rejection of the entirety of the substantive due process doctrine.[56] He asks the Court to reconsider in the future other substantive due process cases with specific mention of *Griswold*, *Lawrence*, and *Obergefell*.[57]

Given this latest development, when another case reaches the Supreme Court asking for a certain conduct to be considered a right protected by the Constitution or, as Justice Thomas asks, that past precedent be reviewed, what method will now be used? To this dilemma, Justice Jardeleza, while recognizing that there is no one method that can be used for all circumstances, suggests that "the Court should endeavor to be deliberate and open about its choice of approach in fundamental rights cases."[58] This approach of selection would "reinforce the credibility of [the Court's] decisions, by exacting upon the Court and its members the duty to clearly and consistently articulate the bases of its decisions in difficult constitutional cases."[59]

V. CONCLUSION

When a purported right not expressly in the Constitution is the subject of a constitutional case, one of the major issues to be resolved will be how the Court will decide if it is indeed a right or not. Because the SCOTUS has no single method used and developed, resolving the issue will prove difficult. The personal dignity and autonomy approach appeared to be the dominant method used for a time, with the history and tradition approach being formulated in reaction to what was perceived to be an overreach of substantive due process. This test was used to reason that

---

54 *Id.* slip op. at 14.
55 *See* id. slip op. at 32, 66.
56 *Id.* (J. Thomas, concurring).
57 *Id.*
58 *Falcis III v. Civil Registrar General*, supra note 6, (J. Jardeleza, concurring opinion).
59 *Id.*

there is no fundamental right to assisted suicide. It was then ignored in two privacy rights cases involving intimate relationships and marriage that were further built on the dignity and autonomy model. The Court then shifted back to using history and tradition in *Dobbs* to overturn *Roe*, again with reaction to substantive due process.

Despite this shifting back and forth, the SCOTUS has not made a definitive ruling on the use of each method. It has not taken steps to be deliberate, open, clear, and consistent in its usage. Perhaps that is the problem when dealing with issues of privacy, intimacy, autonomy, and dignity of persons. The issues are far too complex for one single approach to resolve.

2

Balancing the Novel "Right to be Forgotten" with the Time-Honored Freedoms of Speech and Expression, of the Press, and the Right of the Public to Know

by Atty. Rhodora P. Lo

BALANCING THE NOVEL "RIGHT TO BE FORGOTTEN" WITH THE TIME-HONORED FUNDAMENTAL FREEDOMS OF SPEECH AND EXPRESSION, OF THE PRESS AND THE RIGHT OF THE PUBLIC TO KNOW

*Atty. Rhodora P. Lo**

> *Where a person has by his own efforts rehabilitated himself, we, as right thinking members of society, should permit him to continue in the path of rectitude rather than throw him back into a life of shame or crime. Even the thief on the cross was permitted to repent during the final hours of his agony.*
>
> *Melvin v. Reid*
> *112 Cal. App. 285 (Cal. Ct. App. 1931)*

I. INTRODUCTION

The enactment of The Data Privacy Act ('DPA') of 2012 or Republic Act 10173 entitled "An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, creating for the Purpose the National Privacy Commission and for Other Purposes, brought into the Philippines the new "*Right to be Forgotten*."

The DPA enunciated that it is the policy of the State to protect the fundamental human right of privacy, of communication, while ensuring the free flow of information, to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information and communications systems in the government and the private sector are secured and protected.[1]

---

* Atty. Rhodora P. Lo is a member of the faculty of the University of St. La Salle-College of Law teaching Information Technology Law, Property Law, and Gender and the Law since 2017. She holds a Bachelor of Arts Degree in Mass Communications and is class valedictorian of the Juris Doctor Class of 2014 of the University of St. La Salle. She has been engaged in the private practice of law since 2015 and is a partner at Lo & Ariño Law Office.

1 An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act], Republic Act No. 10173, §2 (2012).

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing, including those personal information controllers ("PIC") and processors ("PIP") who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines.[2]

Personal information refers to information whether recorded in a material form or not, from which the identity 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.[3] Sensitive personal information refers to personal information (1) about an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations; (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by an executive order or an act of Congress to be kept classified.[4] The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose, and proportionality.[5]

A data subject, an individual whose personal information is processed,[6] has the following rights under the DPA:

a. Be informed whether personal information pertaining to him or her shall be, are being or have been processed;

b. Be furnished the information xxx before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity;

c. Reasonable access to, upon demand xxx;

---

2 *Id.* § 4.

3 *Id.* § 3 ¶ (g).

4 *Id.* § 3 ¶ (l).

5 *Id.* § 11.

6 *Id.* § 3 ¶ (c).

d. Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable xxx;

e. Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from 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. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

f. Be indemnified for any damages sustained due to such inaccurate, outdated, false, unlawfully obtained or unauthorized use of personal information.[7]

Paragraph (e) above provides the legal basis for the right to blocking or erasure by the data subject under the DPA, also known as the right to be forgotten.

II. THE "RIGHT TO BE FORGOTTEN"

The Court of Justice of the European Union ("CJEU"), in the case entitled *Google Spain SL. Google Inc. v. Agencia Española de Proteccion de Datos (AEPD), Mario Costeja,*[8] made use of the word "forgotten" in interpreting the right of data subjects guaranteed under Directive 95/46. Directive 95/46/EC was promulgated by the European Parliament and of the Council on 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Object of such directive is for Member States to protect the fundamental rights and freedoms of natural persons, and in particular, their right to privacy concerning the processing of personal data[9] and that Member States shall neither prohibit the free flow of personal data between Member States for the reasons connected with the protection.[10]

---

7 Data Privacy Act, § 16.

8 C-131/12 13 May 2014 available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131, (last accessed September 23, 2022) (EU).

9 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 1.

10 *Id.* art. 2.

The facts of the *Costeja* case are as follows:

On 5 March 2010, Mr. Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against LA Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr. Costeja González's name in the search engine of the Google group (Google Search), he would obtain links to two pages of La Vanguardia's newspaper of 19 January and 9 March 1998 respectively on which an announcement mentioning Mr. Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

By that complaint, Mr. Costeja González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines to protect the data. Second, he requested that Google Spain or Google, Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to *La Vanguardia*. Mr. *Costeja González* stated in this context that the attachment proceedings concerning him had been fully resolved for several years, and reference to them was now entirely irrelevant.

The Court of Justice of the European Union was asked to consider whether Article 12 (b)[11] and subparagraph a of Article 14[12] of Directive 95/46 are to be interpreted as enabling the data subject to require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating

---

[11] Article 12, Right of Access, Member States shall guarantee every data subject the right to obtain from the controller: (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inacurate nature of the data.

[12] Article 14, The Data Subject's Right to Object, Members States shall grant the data subject the right: (a) at least in the cases referred in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to this particular situation to the processing of data relating to him, save where otherwise provided by national legistlation. Where there is a justification, the processing instigated by the controller may no longer involve those data. Article 7. Member States shall provide that personal data may be processed only if: (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; (f) processing is necessary for the purpose of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1.

to him, on the ground that the information may be prejudicial to him or that he wishes it to be "forgotten" after a certain time. The Court of Justice ruled in the affirmative, as follows:

> Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

Meanwhile in the Philippines, Section 3, paragraph (e) of the Implementing Rules and Regulations of the DPA provides:

> e. Right to erasure or blocking. The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal controller's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:
    a. The personal data is incomplete, outdated, false, or unlawfully obtained;
    b. The personal data is being used for purposes not authorized by the data subject;
    c. The personal data is no longer necessary for the purposes for which they were collected;
    d. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
    e. The personal data contains private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression or of the press or otherwise authorized;
    f. The processing is unlawful;
    g. The personal information controller or personal information processor violated the rights of the data subject.
2. The personal information controller may notify third parties who have previously received such processed personal information.

The National Privacy Commission, the agency created to implement the provisions of the DPA, provided further guidance on the matter in NPC Advisory No. 2021-01 on the Subject: Data Subject Rights, issued on 29 January 2021. Section 10 of the Advisory provides:

> Section 10. Right to Erasure or Blocking. – A data subject has the right to request for the suspension, withdrawal, blocking, removal, or destruction of his or her personal data from the PICs filing system, in both live and back-up systems.
>
> A. This right may be exercised upon discovery and substantial proof of any of the following:
>
> 1. The personal data is:
>   a. incomplete, outdated, false or unlawfully obtained;
>   b. used for an unauthorized purpose;
>   c. no longer necessary for the purpose/s for which they were collected; or
>   d. concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression, of or the press, or otherwise authorized;

2. The data subject objects to the processing, and there are no other applicable lawful criteria for processing;

3. The processing is unlawful; or

4. The PIC or PIP violated the rights of the data subject.

B. The PICs should judiciously evaluate requests for the right to erasure or blocking.

1. Approval of Request. When a request for erasure or blocking is made on any of the following grounds, the PIC is directed to grant such request:

   a. Unlawful processing;
   b. Used for unauthorized purpose; and
   c. Violation of data subject rights.

2. Denial of Request. A request for erasure or blocking may be denied, wholly or partly, when personal data is still necessary in any of the following instances:

   a. Fulfillment of the purpose/s for which the data was obtained;
   b. Compliance with a legal obligation;
   c. Establishment, exercise or defense of any legal claim;
   d. Legitimate business purposes of the PIC, consistent with applicable industry standard for personal data retention;
   e. To apprise the public on matters that have an overriding public interest or concern, taking into consideration the following factors:
      i. Constitutionally guaranteed rights and freedoms of speech, of expression or of the press;
      ii. Whether or not the personal data pertains to a data subject who is a public figure; and
      iii. Other analogous considerations where personal data are processed in circumstances where data subjects can reasonably expect further processing.
   f. As may be provided by any existing law, rules and regulations.

C. PICs shall inform the recipients or third parties who have previously received such personal data of the fact of erasure. PICs shall likewise inform the data subject about such recipients of his or her personal data.

D. Where personal data that is the subject of a request for erasure is publicly available, i.e. online, reasonable and appropriate measures shall be taken by the PIC to communicate with other PICs, including third party indexes, and request them to erase copies or remove or de-list search results or links to the pertinent personal data. In determining what is reasonable and appropriate, the available technology and the cost of implementation shall be considered.

E. Data subjects must be adequately informed of the consequences of the erasure of their personal data."

III. THE RIGHT TO PRIVACY VIS À VIS THE RIGHT TO INFORMATION ON MATTERS OF PUBLIC CONCERN

The right to privacy is enshrined in our Constitution and in our laws. It is defined as the "right to be free from unwarranted exploitation of one's person or from intrusion into one's private activities in such a way as to cause humiliation to one's sensibilities." It is the right of an individual to be "free from unwarranted publicity, or to live without unwarranted interference by the public in matters in which the public is not necessarily concerned. Simply put, the right to privacy is the "right to be let alone."[13]

As a matter of fact, this right to be let alone is, to quote from Mr. Justice Brandeis, "the most comprehensive of rights and the right most valued by civilized men."[14]

Sections 2 and 3 of Article III of the Bill of Rights of the 1987 Constitution provide the constitutional basis for the right to privacy, to wit:

---

13 *Spouses Hing v. Choachuy, Sr.*, G.R. No. 179736, (2013).

14 *Olmstead v. United States*, 277 U.S. 438 (1928).

> Section 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for whatever purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.
>
> Section 3. (1) 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.
>
> (2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.

In the Supreme Court case of *Vivares v. St. Theresa's College (STC),*[15] parents of high school students invoked their children's right to privacy against St. Theresa's College. The school official's act of accessing and printing the students' scantily clad photos posted on social networking site Facebook and their use of the same photos as evidence to penalize the students for violating the school's social media policy, were argued to be violations of the right to informational privacy. Informational privacy was explained, as follows:

> The right to privacy has, through time, greatly evolved, with technological advancements having an influential part therein. This evolution was briefly recounted in former Chief Justice Reynato S. Puno's speech, The Common Right to Privacy, where he explained the three strands of the right to privacy, viz: (1) locational or situational privacy, (2) informational privacy, (3) decisional privacy. Of the three, what is relevant to the case at bar is the right to informational privacy – usually defined as the right of individuals to control information about themselves.

---

[15] *Vivares v. STC*, G.R. No. 202666 (2014).

> With the availability of various avenues for information gathering and data sharing nowadays, not to mention each system's inherent vulnerability to attacks and intrusions, there is more reason that every individual's right to control the flow of information should be protected and that each individual should have at least a reasonable expectation of privacy in cyberspace.

IV. FREEDOM OF SPEECH, OF EXPRESSION AND OF THE PRESS

Sections 4 and 7 of the 1987 Constitution provide limitations to the right to privacy, in the form of freedom of speech and expression and the right of the people to information on matters of public concern, to wit:

> Section 4. No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances.

As regards freedom of speech, of expression, and of the press, the discussion of the case of *Chavez v. Gonzales*[16] is very informative, as it explained:

> Surrounding the freedom of speech clause are various concepts that we have adopted as part and parcel of our Bill of Rights provision on this basic freedom.

What is embraced under this provision was discussed exhaustively by the Court in *Gonzales v. Commission on Elections*, in which it was held:

> … At the very least, free speech and free press may be identified with the liberty to discuss publicly and truthfully any matter of public interest without censorship and punishment. There is to be no previous restraint on the communication of views or subsequent liabilities whether in libel suits,

---

16 *Chavez v. Gonzalez*, G.R. No. 168338 , 15 February 2008.

> prosecution for sedition, for damages, for contempt proceedings unless there be a clear and present danger of substantive evil that Congress has a right to prevent.
>
> *Gonzales* further explained that the vital need of a constitutional democracy of freedom of expression is undeniable, whether as a means of assuring individual self-fulfillment; of attaining the truth; of assuring participation by the people in social, including political decision -making; and of maintaining the balance between stability and change.
>
> As early as the 1920, the trend, as reflected in Philippine and American decisions, was to recognize the broadest scope and assure the widest latitude for this constitutional guarantee. The trend represents a profound commitment to the principle that debate on public issue should be uninhibited, robust and wide-open.

The right of the people to be informed on matters of public concern is anchored on Section 7 of the 1987 Constitution, which states:

> Section 7. The right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents, and papers pertaining to official acts, transaction or decisions as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law.

In the case of *Morfe v. Mutuc,*[17] the constitutionality of the Anti-Graft and Corrupt Practices Act, insofar as it requires government employees to submit their statement of assets and liabilities annually was challenged on the ground that it violates the individual's right to privacy.

The Court recognized the right to privacy but upheld the constitutionality of the provision, to wit:

---

[17] *Morfe v. Mutuc,* G.R. No. L—20387, 130 Phil 415, 440 , 31 January 1968.

> The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection.

The language of Prof. Emerson is particularly apt:

> The concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen. This is indeed one of the basic distinctions between absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of life, is the hallmark of the absolute state. In contrast, the system of limited government, safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the state can control. Protection of this private sector –in other words, of the dignity and integrity of the individual – has become increasingly important as modern society has developed. All the forces of a technological age – industrialization, urbanization, organization – operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and totalitarian society.
>
> Even with due recognition of such a view, it cannot be said that the challenged statutory provision calls for the disclosure of information which infringes on the right of a person to privacy. It cannot be denied that the rational relationship such a requirement possesses within the objective of a valid statute goes very far in precluding assent to an objection of such character. This is not to say that a public officer, by virtue of the position he holds, is bereft of constitutional protection; it is only to emphasize that in subjecting him to such a further revelation of his assets and liabilities, including the statement of the amounts and sources of income, the amounts of personal and family expenses, and the amount of income taxes paid for the next preceding calendar year, there is no unconstitutional intrusion into what otherwise would be a private sphere.

V. WHEN THE DATA SUBJECT IS A PUBLIC FIGURE

The right to blocking and erasure, as pointed out above, is subject to limitations, one of which is when the data subject is a public figure, as provided in NPC Advisory No. 2021-01 on the Subject: Data Subject Rights, Section 10, (B) (2) (e) (ii). The case of *Sidis v. FR Pub Corporation*[18] is instructive on the matter.

William James Sidis was a famous child prodigy in 1910. His name and prowess were well known to newspaper readers of the period. At the age of eleven, he lectured to distinguished mathematicians and at sixteen, he graduated from Harvard College, amid considerable public attention. Since then, his name has appeared in the press sporadically, and he has sought to live as unobtrusively as possible.

In 1937, Sidis was made one of the subject of a biographical sketch by the *New Yorker*, a weekly magazine, of current and past personalities entitled "Where Are They Now?" under the subtitle "April Fool" (Sidis was born on April Fool's day). The author describes his subject's early accomplishments in mathematics and the widespread attention he received, then recounts his general breakdown and the revulsion that Sidis thereafter felt for his former life of fame and study. The unfortunate prodigy was traced over the years that followed, through his attempts to conceal his identity, through his chosen career as an insignificant clerk who would not need to employ unusual mathematical talents, and through the bizarre ways in which his genius flowered, as in his enthusiasm for collecting streetcar transfers, and in his proficiency with an adding machine. The article closes with an account of an interview with Sidis at his present lodgings, "a hall bedroom of Boston's shabby south end."

Sidis filed a complaint against the magazine publisher for violating his right of privacy.

The US Circuit Court of Appeals for the Second Circuit ruled against Sidis, explaining that Sidis was once a public figure, and the article complained of, which answers the question as to whether or not Sidis fulfilled his early promise, was still a matter of public concern.

---

[18] *Sidis v. FR Pub Corporation*, 113 F.2d 806 (2d Circ. 1940).

The decision cited the Warren and Brandeis article on the Right to Privacy, stating:

> All comment upon the right of privacy must stem from the famous article by Warren and Brandeis on The Right of Privacy in 4 Harv. L. Rev. 193. The learned authors of that paper were convinced that some limits ought to be imposed upon the privilege of newspapers to publish truthful items of a personal nature. xxx The intensity of life, attendant upon advancing civilization, has rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. Certain public figures, they conceded, such as holders of public office, must sacrifice their privacy and expose at least part of their lives to public scrutiny as the price of the powers they attain. It must be conceded that under the strict standards suggested by these authors plaintiff's right to privacy has been invaded. Sidis today is neither politician, public administrator nor statesman. Even if he were, some of the personal details revealed were of that sort that Warren and Brandeis believed "all men alike are entitled to keep from popular curiosity."

The decision, however, notwithstanding the discussion of the right of privacy, ruled to the contrary in the sense that *Sidis* is a public figure and his right to privacy was not violated, with the following explanation:

> But despite eminent opinion to the contrary, we are not yet disposed to afford to all of the intimate details of private life an absolute immunity from the prying of the press. Everyone will agree that at some point the public interest in obtaining information becomes dominant over the individual's desire for privacy. William James Sidis was once a public figure. As a

> child prodigy, he excited both admiration and curiosity. Of him great deeds were expected. In 1910, he was a person about whom the newspapers might display a legitimate intellectual interest, in the sense meant by Warren and Brandeis, as distinguished from a trivial and unseemly curiosity. But the precise motives of the press we regard as unimportant. And even if Sidis had loathed public attention at that time, we think his uncommon achievements and personality would have made the attention permissible. Since then Sidis has cloaked himself in obscurity, but his subsequent history, containing as it did the answer to the question of whether or not he had fulfilled his early promise, was still a matter of public concern. The article in the New Yorker sketched the life of an unusual personality, and it possessed considerable popular news interest.

The DPA itself, at the onset, provided the following exclusions to the coverage of the law, as follows:

> This Act does not apply to the following:
>
> a. Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
>
> 1. The fact that the individual is or was an officer or employee of the government institution;
> 2. The title, business address and office telephone number of the individual;
> 3. The classification, salary range and responsibilities of the position held by the individual; and
> 4. The name of the individual on a document prepared by the individual in the course of employment with the government;
>
> b. Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

c. Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

d. Personal information processed for journalistic, artistic, literary or research purposes;

e. Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

f. Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws.

VI. CONCLUSION

We are in the information/digital age. The quality of our lives depends on our level of engagement and proficiency in navigating existing information and communications technology and the internet. Data, indeed, is the new currency. We interact socially, commercially, and professionally by providing and receiving personal data using information technology on a daily basis. We share and disclose much of our personal information, with the expectation that we do so to facilitate life in a faster, more accessible, more convenient if not more luxurious, and more meaningful manner.

While not explicitly provided in our Constitution, we would do well to learn from the fundamental law of California, which provides: "All men are by nature free and independent, and have certain inalienable rights, among which are those of enjoying and defending life or liberty; acquiring, possessing and protecting property; and pursuing and obtaining safety and happiness."[19]

The right to be "forgotten", or to "move on" or to "sink into oblivion" or for erasure and blocking of personal information involving facts and events which are prejudicial to one's reputation and social standing, and for information which are no longer relevant because of time and changed circumstances, under reasonable limitations of freedom of speech, of expression, of the press and the right to information on matters of public concern, is indispensable if we are to afford each one the right to pursue and obtain our own version of safety and happiness.

[19] Calif. Constitution, art. 1, § 1.

3

Privacy Paradox and the Pitfalls of Unthinking

by Rachel Lois B. Gella

PRIVACY PARADOX AND THE PITFALLS OF UNTHINKING

*Rachel Lois Gella**

I. INTRODUCTION

The lie-truth dichotomy is a language that bespeaks the mind. In much the same way, the privacy paradox speaks of a dichotomy of desires: at one end, the desire for privacy, and on the other, the desire for disclosure. The latter results in relinquishment which proves an improvident fate.

If every click recurs an infinite number of times an information is shared with no agency of choice, we are nailed to eternity in the digital space, deceived by technological unthinking. Here, the privacy paradox has become a lore in the information age. Its constant weaponizing is a confrontation with privacy protection approaches, and its warrant is a ploy for dystopian fantasies. And yet, we are presently living with its unseen but commanding presence.

People with no agency of an alternative option to avoid risks online may be more attuned to trading their personal information for welfare benefits.[1] The birth of the privacy paradox is the inconsistency resulting from a "rational risk-benefit tradeoff"[2] in which individuals ignore privacy concerns when they feel the benefits of sharing personal information outweigh the risks. Despite having the right to choose what information to disclose, the stake demanded is too high; it costs a portion of personal information that may be used as a weapon against us. Arguably, it is a confrontation with *fait accompli*.

This essay has a three-fold purpose: (1) it will examine the privacy paradox as a legal theory confronting the legal framework of privacy and the demands for its protection and regulation; (2) analyze the pitfalls of privacy and the emerging bargaining powers in the information age; and (3) determine the legal implications of the privacy paradox in protecting privacy.

---

* Rachel Lois Gella is a fourth-year Juris Doctor student at the University of St. La Salle. She sits as the current Editor-in-Chief of the USLS Law Journal. She has published three columns in the Philippine Daily Inquirer, and contributed to the Asian Law Student's Association 2023 Legal Newsletter.

1 *Srinivasan, J., Bailur, S., Schoemaker, E., & Seshagiri, S.*, Privacy at the margins| The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India, 2018, <https://ijoc.org/index.php/ijoc/article/view/7046/2296>, (visited 27 November 2022).

2 Mourey, J., & Waldman, A. E. (2020). *Past the Privacy Paradox: The Importance of Privacy Changes as a Function of Control and Complexity. Journal of the Association for Consumer Research.* doi:10.1086/708034. <https://ideas.repec.org/a/ucp/jacres/doi10.1086-708034.html> (Visited 23 December 2022).

II. THE BIRTH OF THE PARADOX

Paradoxes exist in legal thought. Canons of legal thought may be confronted with logical inconsistencies that preclude the proper application of the law.[3] For instance, privacy protection is where legal language is used to clothe what are, essentially, never-ending debates.

The privacy paradox is rooted in the logic that comes with an intent to give up a portion of privacy at the expense of receiving benefits. For this writing, "privacy paradox" refers to the intention of individuals to disclose personal information at the cost of their privacy. When people disclose information about themselves, they do so with certain expectations about using such information, which shape their assessment of the privacy risks involved. While initially a consumerist concept, the privacy paradox extends its trajectory to privacy legislation since the harms confronting this concept include private everyday life transactions.

The inherent value of privacy is autonomy which includes the freedom of choice. This involves the full agency of one's decisions. There is then a presupposition of a right to participate in an exchange where a constant bargain of privacy occurs, even if it results in a loss of autonomy. And the loss of autonomy is a privacy fear that runs the course of the privacy paradox.

Privacy paradox, as a legal theory, entails the element of choice as it necessarily presumes an exchange of bargain. After all, the decision to "renounce" certain privacies, as the paradox requires, assumes an alternative path and an admission that a choice, in fact, exists.[4] This marked agency of choice, despite being a product of a privacy right, may also be the underlying cause of why privacy breach is justified.

Note, however, that not all choices are equal. In his essay, *The Difference Between Choice and Control*, Duffy argues that the most primitive choice is consent, while control is the most developed.[5] This essay will explore both kinds in relation to the privacy paradox.

---

3 *George P. Fletcher,* Paradoxes in Legal Thought, 85 COLUM. L. REV. 1263, 1985, <https://scholarship.law.columbia.edu/faculty_scholarship/1072>, (visited 21 November 2022).

4 *Gabriella Razzano*, Understanding the Theory of Collective Rights: Redefining the Privacy Paradox, February 2020, <https://researchictafrica.net/wp/wpcontent/uploads/2021/02/Data-Trusts-Concept-Note.pdf., (visited 3 October 2022).

5 *Simon Duffy*, The Difference Between Choice and Control, 2016,< https://citizen-network.org/library/the-difference-between-choice-control.html>, (visited 1 December 2022).

To have control and autonomy over the information we share is a hallmark of freedom. Still, so many decisions are made secretly without our awareness or participation. At the height of the information age, privacy flourished, then died a thousand times. In *Disini v. Secretary of Justice*, the Court noted that forces of the technological age operate to narrow the area of privacy and facilitate intrusions into it.[6] It is nearly impossible not to share personal information, but it comes with a price: the inherent vulnerability to attacks and unwarranted disclosure. In fact, breaches of security leading to accidental disclosure of personal data[7] have a legal term, not just a mere happenstance.

The current debates on privacy should be understood in the context of the underlying presence of the privacy paradox. The paradox thrives when people protect their privacy but also want to receive highly personalized information and service. As *Festin* wrote, "*The individual's desire for privacy is never absolute since participation in society is an equally powerful desire."*[8]

People disclose portions of personal information to pay the cost of the benefits they seek. Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 ('DPA'), provides:

> It is the policy of the State to protect the fundamental human right of privacy of communication while ensuring the free flow of information to promote innovation and growth.

But how does the law maintain the liminal space in between? There should be an inquiry into what makes people relinquish their privacy for protection and how this relinquishment may also be the reason why an evil exists that must be avoided.

---

6 *Disini vs. Secretary of Justice,* G.R. No. 203335, 11 February 2014.

7 *NPC Circular 16-03-Personal Data Breach Management,* Section 3 (f), wherein "personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

8 *Alan F. Westin, Privacy and Freedom*, 25 WASH. & LEE L. REV. 166 (1968)<https://scholarly.commons.law.wlu.edu/wlulr/vol25/iss1/20/> (visited 23 December 2022).

III. THE LEGAL FRAMEWORK OF PRIVACY

At its core, the concept of privacy remains a repository of freedom.[9] In *Morfe v. Mutuc*, the Court affirmed that the right to privacy exists independently of its identification with liberty and is fully deserving of constitutional protection.[10] The Philippine Constitution guarantees the right against unreasonable searches and seizures and the right to privacy of communication and correspondence. There is an express guarantee of the right against self-incrimination, liberty of abode, and right to due process. The State also recognizes the vital role of communication and information in nation-building.[11]

In the international context, this right is derived from the Universal Declaration of Human Rights, which mandates that "no one shall be subjected to arbitrary interference with his privacy"[12] and "everyone has the right to the protection of the law against such interference or attacks."[13]

For this part, the discussion on the legal framework of privacy in relation to the privacy paradox will be limited to the right to privacy and the challenges to privacy protection under Philippine law.

A. *The Right to Privacy under Philippine Law*

The right to privacy is the right to be let alone and it signifies the beginning of all freedoms,[14] a truism that bears no room for any unwarranted claim. *Disini v. Secretary of Justice*, citing *Sabio v. Gordon,*[15] recognizes that our laws recognize and protect zones of privacy. Within these zones, any intrusion is impermissible unless excused by law and by customary legal processes. In *Whalen v. Roe,*[16] the United States Supreme Court characterized two different kinds of interest in protecting privacy: the individual interest in avoiding disclosure of personal matters and the interest in independence in making certain important decisions. As discussed in the case of *Vivares v. St. Theresa's College (STC),*[17] to wit:

---

9 *Public Utilities Commission v. Pollak* 343 U. S. 451, 467 (1952).

10 *Morfe vs. Mutuc,* G.R. No. L-2038, 31 January 1968.

11 Constitution, Art. II, Sec. 24.

12 Universal Declaration of Human Rights (1948), Art. 12.

13 Universal Declaration of Human Rights (1948), Art. 17.

14 *Morfe v. Mutuc,* supra note 10.

15 *Sabio vs. Gordon,* 535 Phil. 687, 714-715, 17 October 2006.

16 *Whalen vs. Roe,* 429 U.S. 589, 22 February 1977.

17 *Vivares v. St. Theresa's College (STC),* G.R. No. 202666, 29 September 2014.

> The concept of privacy has, through time, greatly evolved, with technological advancements having an influential part therein. This evolution was briefly recounted in former Chief Justice Reynato S. Puno's speech, The Common Right to Privacy, where he explained the three strands of the right to privacy, viz: (1) locational or situational privacy; (2) informational privacy; and (3) decisional privacy. Of the three, what is relevant to the case at bar is the right to informational privacy–usually defined as the right of individuals to control information about themselves.

The right to informational privacy allows us to control the information we disclose, but the extent to how much information we should share continues to be an elusive discussion. Simply put, the right to informational privacy is an individual's right to control information about themselves[18] which involves personal information that "refers to any information, whether recorded in a material form or not, from which the identity 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."[19]

When people have the right to control information about themselves, they have the control to protect their privacy. The Supreme Court in *Disini*[20] reiterated the aspects of informational privacy and its relationship with data collection:

> Informational privacy has two aspects: the right not to have private information disclosed and the right to live freely without surveillance and intrusion. In determining whether a matter is entitled to the right to privacy, this Court has laid down a two-fold test. The first is a subjective test, where one claiming the right must have an actual or legitimate expectation of privacy over a certain matter. The second is an objective test, where their expectation of privacy must be one society is prepared to accept as objectively reasonable. The factual circumstances of

---

18 *Id.*

19 Republic Act No. 10173, (2012), Sec. 3 (g).

20 *Disini vs. Secretary of Justice*, supra note 6.

> the case determine the reasonableness of the expectation. However, other factors, such as customs, physical surroundings, and practices of a particular activity, may create or diminish this expectation.

In this light, there is an accorded right to control information about ourselves, a developed form of choice which carries responsibility. As further elucidated in *Vivares*:

> Online Social Network ('OSN') users should be aware of the risks they expose themselves to whenever they engage in cyberspace activities. Accordingly, they should be cautious enough to control their privacy and to exercise sound discretion regarding how much information about themselves they are willing to give up. Internet consumers ought to be aware that, by entering or uploading any data or information online, they are automatically and inevitably making it permanently available online, the perpetuation of which is outside their control. Furthermore, and more importantly, information, otherwise private, voluntarily surrendered by them can be opened, read, or copied by third parties who may or may not be allowed access to such.[21]

When people share information, they provide a license to use or disclose their data in specific ways, but they retain privacy rights in that data. Worth noting, however, is the increase of privacy risks to some extent that comes along with it. There is high access to OSN in the information age. OSNs have the nature of (1) that it is facilitating and promoting real-time interaction among millions, if not billions, of users, sans the spatial barriers, bridging the gap created by physical space; and (2) that any information uploaded in OSNs leaves an indelible trace in the provider's databases, which are outside the control of the end-users.[22] The purpose of an OSN is to allow users to interact and stay connected to other users on the social media platform through sharing information in the form of photos, videos, and the posting of statuses, among others.

---

21 *Vivares vs. St. Theresa's College*, supra note 16.

22 *Id*.

Privacy laws in the Philippines have been envisioned to promote a society where the vital role of information and communications technology are recognized. The DPA is founded on 'the policy of the State to protect the fundamental human right to privacy of communication while ensuring free flow of information to promote innovation and growth and the State's inherent obligation to ensure that personal information in information and communications systems in government and the private sector are secured and protected.' Republic Act No. 10175, or the Cybercrime Prevention Act, was passed in 2012 and is considered the twin bill of the DPA.

The DPA provides that the processing of personal data must comply with the requirements of the law and must adhere to the principles of transparency, legitimate purpose, and proportionality,[23] and the collection must be for a declared, specified, and legitimate purpose.[24] The Cybercrime Prevention Act, on the other hand, penalizes acts that constitute the offense of cybercrime. Thus, the Philippines' goal is to protect online users against crime while ensuring the privacy of individuals and data security.

With fast-paced technological advancement, however, these laws may trail behind. Everyone is continually engaged in a personal license which "balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives."[25] The right to control information, specifically the right to disclose even personal matters, is a right that must be donned with reason. But then, the individual's control over information can also relieve the burden of responsibility for certain perceived privacy breaches. For example, when people publicly post embarrassing pictures, with their full agency and without heightened privacy settings, they are victims of their recklessness. By publicizing such information, they voluntarily relinquished control. Yet such a waiver is still a legally recognizable privacy right.

The regulated and the regulator face more challenges than solutions. There are no real precedents to provide guidance, and circulars are still being issued to bridge gaps in the current laws. Consequently, many authorities need safeguards and well-defined standards to prevent unconstitutional intrusions.

---

23 IRR of the Data Privacy Act of 2012, Sec. 17.

24 IRR of the Data Privacy Act of 2012, Sec. 19.

25 *Privacy and Freedom*, supra note 8.

B. *The Challenges to Protecting Privacy in the Philippines*

Much of the dynamic tension confronting privacy laws today lies in the privacy paradox, as there is a marked lack of agency in these contexts of 'exchange.' As an illustration, people would always prefer to keep their privacy over giving out their information. Still, they usually lack a wide agency of choice for privacy protection. This means letting people decide the cost of privacy is tantamount to allowing a certain entity to dictate its value. This exhibits the power of default in matters concerning privacy.

People have the right to trade away their personal data, and they can value others having the right to choose for themselves. In this sense, privacy can be seen as having two edges, resulting in a fundamental tension between interests that may call for the necessity of privacy protection. The discrepancy between people's expressed privacy concerns and their sharing of personal information is a disconnection that must be addressed to create a privacy framework across various sectors that reflect how individuals want their information to be protected.

The creeping assertiveness of the privacy paradox makes the protection of privacy problematic. Beyond the challenges of setting the proper regulatory approach is establishing a privacy mindset. As noted by the National Privacy Commission's website, there is no Filipino word for "privacy". Crafting a privacy policy is like speaking the vernacular in a foreign place. Anyone can do it, but something is grating about it.

The risks and harms of privacy protection affect individuals. Thus, recourse to privacy legislation should be fundamentally individualized.[26] It is suggested that the ultimate risks and harms should only be measured for the individual rather than for any social group.

Privacy protection today carries the nature of a *caveat orator* or "let the communicator beware."[27] The communicator runs the risk of having personal information to be misused somewhere in the digital realm in exchange for a certain benefit. The right to privacy does not bar all incursions into individual privacy. The right is not intended to stifle scientific and technological advancements that enhance public service for the common good. It merely requires that the law be narrowly focused and that a compelling interest justify such intrusions.

---

26 *Understanding the Theory of Collective Rights: Redefining the Privacy Paradox*, supra note at 4.

27 *Eric Jorstad,* The Privacy Paradox, William Mitchell Law Review: Vol. 27: Iss. 3, Article 16, 2001, < https://open.mitchellhamline.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1811&context=wmlr>, (visited 2 October 2022).

Through sharing information publicly on the internet, users blur the line between legitimacy and invasion of privacy. The reasonable expectation threshold is one aspect of privacy that stands as the foundation of any protection. In *Ople v. Torres,*[28] wherein the constitutionality of Administrative Order No. 308 or the "Adoption of a National Computerized Identification Reference System" was assailed as it allegedly intruded in the citizens' protected zone of privacy, the Court ruled:

> The reasonableness of a person's expectation of privacy depends on (1) whether, by his conduct, the individual has exhibited an expectation of privacy; and (2) this expectation is one that society recognizes as reasonable.
>
> "Reasonableness" is the touchstone of the validity of a government search or intrusion.[29] For a valid law on privacy rights, there must be well-defined limits to guide law enforcers. Additionally, the expectation of privacy is measured from the general public's point of view. Without a reasonable expectation of privacy, the right to it would have no basis.[30]

Technological advances diminished individual private spaces through electronic surveillance and brought more efficient means of collecting, categorizing, and sorting data.[31] The misalignment of legal instruments and the demands of online privacy may have been the cause of why personalized scamming and spoofing have become rampant.

IV. PRIVACY IN THE INFORMATION AGE

Sitting at the far side is privacy in the information age that warrants the relinquishment of privacy to a certain extent, weighing the scale at a more lopsided bargaining end. To further give the context to how the privacy paradox may navigate its course, it is essential to explain what drives the far end of the bargain. For this part, the proliferation of personalized scamming and spoofing will be used as an anchor that prompts protection, eventually resulting in people giving up portions of their privacy.

---

28 *Ople v. Torres*, G.R. No. 127685, 23 July 1998.

29 *Social Justice Society vs. Dangerous Drugs Board*, G.R. No. 157870, 3 November 2008.

30 *Id.*

31 *Kizza, Joseph Migga, Ethical and Social Issues in the Information Age*, Third Edition, Springer-Verlag London Limited 2007, p. 304.

Further, targeted marketing will be explained as having the potential to be a bargaining power in the privacy dynamics that affect how people trade away their personal data online.

A. *The Proliferation of Personalized Attacks*

With so much information and data, the digital realm remains open to misuse. Sharing personal information online carries the expense of vulnerability. Email or phone call scams are not new. Examples include receiving a text message bearing the words "You Won an iPhone PROMAX" or the infamous job opening scams. This is the traditional type of scamming wherein scammers do not know whom they are targeting. They create a generic message and send it out to millions of people. When information finds its way online, it can be extracted together with other data on the subject. Once removed, the information is put in the hands of any person. The end of privacy begins.[32]

Text scams are phishing attacks that entice users to give out personal and sensitive information.[33] The National Privacy Commission ('NPC') calls these attacks "smishing," or an attack that targets victims through mobile text messaging. One smishing scenario involves a text message sent to a user containing a code and a shortened link that, when clicked, binds the user's mobile number to the dummy account. Additionally, spoofing refers to transmitting misleading or inaccurate information about the source of the phone call or text message with the intent to defraud, cause harm, or wrongfully obtain anything of value.[34]

A personalized attack is different. Scammers research first and create a customized message for each intended victim. Finding a database of people's names, passwords, phone numbers, or other personal information is the initial step for scammers. With so many websites visited or hacked, this information is easily accessible. Text scammers send false text messages to their victims claiming that their mobile phone numbers won a raffle reportedly sponsored by the Bangko Sentral ng Pilipinas or other organizations, using bogus names or posing as government officials.[35]

---

32 *Ople v. Torres*, supra note 28.

33 National Privacy Commission, NPC PHE Bulletin No. 21 Preventive Data Privacy Practices Against Smishing*, available at* <https://www.privacy.gov.ph/2021/10/npc-phe-bulletin-no-21-preventive-data-privacy-practices-against-mishing/>(visited *1* October 2022).

34 Republic Act No. 11934 (2022), Sec. 3 (g).

35 *Llewellyn L. Llanillo and Khersien Y. Baustista*, Zones of Privacy: How Private?, 26 July 2021 <https://www.iadclaw.org/defensecounseljournal/zones-of-privacy-how-private/> (visited 1 October 2022).

In a more technical sense, the Anti-Cybercrime Group of the Philippines released ACG-Cyber Security Bulletin Number 212: *Understanding the Risk of Spear-Phishing,*[36] which explains the nature of "spear phishing," which are attacks targeted at specific individuals. The cybercriminal might study the target's habits or environments for even more targeted or personalized attacks.

From the foregoing, "personalized scams" result from collecting information about individuals and using the same information to personalize the attacks. Privacy International explained that an individual's phone number could match their voting preferences or health data.[37] Leandro Angelo Aguirre, the deputy privacy commissioner of the National Privacy Commission, expressed that:

> Most likely, what is happening is that data scraping, either manual or automated, is getting information coming from these different applications, and this is what is being used to match the names in the texts being sent to our countrymen.[38]

There is arguably a thin line between marketing and scamming. If marketers are capable of personalizing information, so are scammers. Either way, personal information shared online is used as raw material translated and used to efficiently segment customers or recipients based on their data points, such as purchase intent, impulsiveness, and trustworthiness.[39] In other words, personal information and data are scraped, collected, translated, and shaped to lure online recipients into giving up portions of their privacy to receive personalized services.

As ruled in *Disini*, when seemingly random bits of traffic data[40] are gathered in bulk, pooled together, and analyzed, they reveal activities that can then be used to profile any individual and target their interests. With enough traffic data, analysts may determine a person's close associations,

---

36 *Anti-Cybercrime Group*, ACG-CYBER SECURITY BULLETIN NR 212: UNDERSTANDING THE RISK OF SPEAR-PHISHING, <https://acg.pnp.gov.ph/main/cyber-security-bulletin/373-acg-cyber-security-bulletin-nr-212-understanding-the-risk-of-spear-phishing.html>, (visited 3 December 2022).

37 *Privacy International*, SIM Card Registration <https://privacyinternational.org/learn/sim-card-registration> (Visited 23 December 2022).

38 Scam texts got your name? These apps may have been the source, Xave Gregorio. <https://www.philstar.com/business/2022/09/07/2208049/scam-texts-got-your-name-these-apps-may-have-been-source> (visited 23 December 2022).

39 Kristen Baker, *Customer Segmentation: How to Effectively Segment Users & Clients*, 25 November 2022, <https://blog.hubspot.com/service/customer-segmentation>, (visited 30 November 2022).

40 Cybercrime Prevention Act (2012), Sec. 3 (p). Traffic Data is defined as 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.

religious views, political affiliations, and sexual preferences. Such information is likely beyond what the public may expect to be disclosed and falls within matters protected by the right to privacy.[41]

B. *Targeted Marketing: An Emerging Bargaining Power in the Privacy Field*

Since the privacy paradox anchors its nature from a consumerist perspective, it will be argued for this part that targeted marketing may be an emerging bargaining power that further warrants the sharing of personal information online and, ultimately, signifies the depths of how personal information may be personalized to target users. In the last decades, digital marketing has become the forefront of the information age. Sophisticated algorithms and customer segmentation grow at a faster pace than how laws embrace technology and innovation. Arguably, targeted marketing substantially impacts how people subject themselves to online transactions.

The magic trick behind personalization is targeted marketing. Targeted marketing involves breaking consumers into segments with similar characteristics, such as income, demographics, and buying power.[42] Technologies, like customer segmentation through mobile numbers,[43] personalize marketing to boost customer loyalty. Websites and digital platforms gather information from online users' and recipients' digital footprints as they explore different channels online and on various devices. Targeted ads, for example, collect and analyze users' online activity and use this data to prepare the type of ads a user prefers. Platforms and websites collect location information and mine data for targeted ads.[44] This may also be done by using cookies stored on digital devices, which are also used to track activities and webpage visits.[45] Today, modern marketing works at its highest potential when it is personalized.

---

41 Supra note 6.

42 *Baig & Bryan*, Can Target Marketing Withstand Emerging Privacy Regulations? Litigation (and Time) will Tell, National Law Review, 6 January2021,<https://www.natlawreview.com/article/can-target-marketing-withstand-emerging-privacy-regulations-litigation-and-time-will> (visited 6 October 2022).

43 Supra note at 39.

44 *Nik Froehlich*, The Truth in User Privacy And Targeted Ads <*https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/?sh=6e4ed48355e1*> (visited 23 December 2022).

45 *Id.*

While none of the Philippine laws expressly prohibit targeted marketing, this marketing tool may be problematic when unbridled, especially regarding how consumer data is collected. It bears noting that raw data stored online can easily be used to lure users. Although laws have privacy principles in their provisions and allow some legal remedies, case law is sparse. Modern times have trended towards permitting such use of data. This also extends to the usage of communication devices.

V. PRIVACY PARADOX: ITS LEGAL IMPLICATIONS IN REGULATING PRIVACY IN THE INFORMATION AGE

To further understand the workings of the privacy paradox in laws concerning an exchange of privacy, Republic Act No. 11934, otherwise known as the SIM Registration Act, will be analyzed as a case study. Registration of prepaid mobile phone Subscriber Identity Module ('SIM') has been objected to as an unconstitutional intrusion into one's privacy, but considering the prevalent text scams and other fraudulent use of SIMs, the bargaining end of the privacy trade-off has been established.

In this section, the subject matter of the discussion will be limited to the Act's privacy policies, the role of Public Telecommunication Entities, the nature of a database in storing data, and the registration guidelines. These will reflect the exchange between end-users and entities and the extent of personal information surrendered to authorities to deter crimes involving SIMs.

Note that there is a presumed existence of exchange that requires mandatory participation since doing otherwise would severely impact the users' lives, including their right to communicate freely. Here, registering your SIM involves full agency, as the paradox requires.

A. *Understanding the SIM Registration Act*

On October 10, 2022, Republic Act No. 11934, or the "SIM Registration Act," was signed into law. The SIM Registration Act is predicated on two considerations: (1) the need to promote responsibility in the use of Subscriber Identity Module and (2) to provide law enforcement agencies the tools to resolve crimes that involve its utilization and a platform to deter the commission of wrongdoings.

i. Declaration of Policy and Interpretation

Arguments opposing the idea of storing personal information include concerns about the security of the data storage, the financial load, and the lack of efficacy of the proposal as a remedy for the issue at hand. Proponents of the law, however, would argue that the SIM Registration Act is grounded on privacy principles that are detailed in its provisions, to wit:

> Section 2. *Declaration of Policy*. — The State recognizes the vital role of information and communications technology in nation-building and encourages its growth and development.
>
> It is equally cognizant that as beneficial as modern technology is, its illegal or malicious use endangers people's lives, damages property, poses hazards to public order, and even threatens the security of nations.
>
> The State shall promote responsibility in using the Subscriber Identity Module (SIM) and provide law enforcement agencies the tools to resolve crimes that involve its utilization and a platform to deter the commission of wrongdoings.
>
> Towards this end, the State shall require the registration of SIM for electronic devices by all users.

Another privacy principle worth noting is Section 14 of the same law, which provides for the manner of interpretation when there is any doubt:

> Section 14. *Interpretation.* - Any doubt in the interpretation of any provision of this Act and its implementing rules and regulations shall be construed in a manner that accords the highest respect for privacy and liberally interpreted in a manner mindful of the rights and interests of SIM subscribers.

ii. The Role of Public Telecommunications Entity

Section 4 of the Act mandates that Public Telecommunications Entity or PTE shall require the registration of SIM as a pre-requisite to the activation thereof. PTEs "shall refer to any person, firm, partnership or corporation, government or private, engaged in the provision of telecommunications services to the public for compensation, as defined under Republic Act No. 7925 or the Public Telecommunications Policy Act of the Philippines.[46]

In the Philippines, the three main telecommunications companies that will serve as PTEs under the law are Globe Telecom Inc. (Globe), Smart Communications Inc. (Smart), and DITO Telecommunity. Each has its respective means of registering SIMs from end-users, guided by the law's registration guidelines which mandate the use of a database to contain information required in this law. As provided in Section 6:

> Section 6. *SIM Register.* All PTEs *shall maintain their database containing the information required under this Act*. The database shall strictly serve as a SIM Register to be used by PTEs to process, activate or deactivate a SIM or subscription and shall not be used for any other purpose unless otherwise provided under this Act. The successful submission and acceptance of the required registration form shall serve as the certification of registration by the end-user. (emphasis mine)

A database "refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed, or stored or have been prepared, processed or stored in a formalized manner and which are intended for use in a computer system."[47] Our personal information will be stored for ten (10) years or until the SIM deactivation.

As noted in *Ople v. Torres,* the Court is not against using computers to gather, store, process, retrieve, and transmit data to improve government operations.[48] When used correctly, data stored in computers result in efficient bureaucracy by providing accurate and comprehensive information for policy-making. Using the same case law, the Court expressed that dangers to privacy come from different sources, it may

---

46 RA 11934 (2022), Sec. 3, citing RA 7925.

47 Cybercrime Prevention Act (2012), Sec. 3 (l).

48 *Ople v. Torres*, supra at note 28.

even be from the government. This is the reason why Administrative Order No. 308 was ruled unconstitutional. AO No. 308 pressures people to sacrifice their privacy by providing personal information under the guise of improving the delivery of basic services. This is one clear example of how the privacy paradox works in the legal context.

According to Privacy International,[49] for most SIM registration cases, SIM users' data are easily shared with other databases in the lack of adequate data protection regulation and monitoring, allowing the state to create profiles of individuals and giving businesses and third parties with access to a tremendous quantity of data. As technology upscales, the information gathered as part of registration today might be stored for an unlimited period and used for various purposes in the future. In NPC Case No. 17-001, any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed. As to the extent their data are or will be processed.[50] The unauthorized processing of personal information and the processing of personal and sensitive information for unauthorized purposes are punishable.

Under the SIM Registration Act, the lack of any legal solutions, should there be issues like leakage of information in the database of PTEs, should be given weight. This is especially true since personal information will be stored in these databases for 10 years. Given the database's ability to store and retrieve data, the danger from the possibility of giving the government the capability to compile such vast data still lingers. Once data creeps into the digital space, there exists indelible information of any person ready for the taking and subjected to misuse.

iii. Registration Guidelines

The Act's most controversial aspect, however, lies in its provisions on registration guidelines and how one is willing to share personal information to protect their privacy from personalized attacks, primarily text scams. While legislative intent is geared toward security purposes, registration of SIMs requires an exchange where some of your personal information is traded away despite future intrusions it may carry into the

---

49 *Privacy International*, SIM Card Registration (article on the mandatory registration and identification of all mobile phone users purchasing a pre-paid SIM Card), <https://privacyinternational.org/learn/sim-card-registration> (visited 4 October, 2022).

50 ODC v. ODB & AE, NPC Case No. 17-001 <https://www.privacy.gov.ph/wpcontent/uploads/2020/10/NPC-17-001-ODC-v-ODB-Resolution-PSD-10Sept2020- ABJ3.pdf> (visited 2 October 2022).

private lives of end-users.[51] As previously argued, this 'exchange' entails the element of a trade-off to ensure privacy protection benefits.

Section 5 of R.A. 11934 provides, to wit:

> Section 5. *Registration Guidelines.* - The SIM process shall be guided by the following parameters:
>
> (a) Submission of duly accomplished control-numbered owner's registration form with full name, date of birth, sex, and address. The registration form shall be accomplished electronically through a platform or website to be provided by the PTEs. The same shall include a declaration by the end-user that the identification documents presented are true and correct and that said person is the one who accomplished the registration form;
>
> (b) Presentation of valid government-issued identification (ID) cards or other similar forms of documents with photo that will verify the identity of the end-user such as but not limited to the following:
>
> (1) Passport;
> (2) Philippine Identification;
> (3) Social Security System ID;
> (4) Government Service Insurance System e-Card
> (5) Driver's license;
> (6) National Bureau of Investigation clearance;
> (7) Police clearance;
> (8) Firearms' license to own and possess ID;
> (9) Professional Regulation Commission ID;
> (10) Integrated Bar of the Philippines ID;
> (11) Overseas Workers Welfare Administration ID;
> (12) Bureau of Internal Revenue ID;
> (13) Voter's ID;
> (14) Senior Citizen's card;
> (15) Unified Multi-purpose Identification card;
> (16) Persons with Disabilities card; or
> (17) Other valid government-issued ID with photo.
>
> x x x

[51] RA 11934 (2022), Sec. 3 (a), defining end-users as any existing subscriber or any individual or juridical entity that purchases a SIM from the Public Telecommunications Entities (PTEs), its agents, resellers, or any entity.

(d) The registration of a SIM by a minor shall be under the name of the minor's parent or guardian: *Provided,* That the minor's parent or guardian shall give their consent and register the SIM; and

(e) In the case of end-users who are foreign nationals, they shall register their full name, nationality, passport number, and address in the Philippines and present the following:

(1) For foreign nationals visiting as tourists under Section 9(a) of Commonwealth Act No. 613, as amended:
  (i) Passport;
  (ii) Proof of address in the Philippines; and
  (iii) Return ticket to own country of the tourist or any other ticket showing the date and time of departure from the Philippines;

(2) For foreign nationals with other type of visas:
  (i) Passport;
  (ii) Proof of address in the Philippines;
  (iii) Alien Employment Permit issued by the Department of Labor and Employment (DOLE);
  (iv) Alien Certificate of Registration Identification Card or ACRI-Card issued by the Bureau of Immigration (BI);
  (v) School registration and ID for students; or
  (vi) Other pertinent documents, whichever is applicable.

The SIMs that are registered under Subsection e (1) shall only be valid temporarily for thirty (30) days, and shall automatically be deactivated upon expiration of the validity of the SIM.

The relevant government agencies and concerned PTEs shall facilitate all SIM registrations in remote areas with limited telecommunication or internet access: *Provided,* That said registration facilities in remote areas shall be established within sixty (60) days from the effectivity of this Act.

> A buyer who fails to comply with the requirements for registration shall result in their SIM not being activated.

There is an express requirement for end-users to provide their personal information in a control-numbered registration form with a full name, date of birth, address, and various identification cards. Worth noting is the amount of vast data that will be handled by the entities under this law. The state of mobile subscription in the Philippines shows that there were 156.5 million cellular mobile connections at the start of 2022.[52]

To expound further, Section 6 of the Implementing Rules and Regulations of the SIM Registration Act provides, to wit:

> Section 6. *Registration Form and Registration Process.*
>
> x x x
>
> (d) The registration process shall be guided by the following parameters:
>
> (i) Submission of the electronically and duly accomplished registration form with the following data and information only:
>
> By individual (natural person) end-user;
> (1) Full Name;
> (2) Date of Birth;
> (3) Sex;
> (4) Present/ Official Address (Choice by end-user);
> (5) Type of ID Presented; and
> (6) ID Number Presented.
>
> By juridical entity end-user;
> (1) Business Name:
> (2) Business Address; and
> (3) Full Name of Authorized Signatory.
>
> By foreign national end-user;
> (1) Full Name;
> (2) Nationality;
> (3) Date of Birth;
> (4) Passport;
> (5) Address in the Philippines;

---

[52] *GSMA Intelligence,*<https://www.gsmaintelligence.com/?utm_source=DataReportal&utm_medium=article&utm_campaign=State_Internet_Connectivity> (visited 3 December 2022).

(6) For Persons of Concern or POCs, the Type of Travel or Admission Document Presented; and

(7) ID Number or Number of Document Presented.

(ii) Presentation of valid government-issued identification (ID) card or other similar form of document with photo.

(iii) Inputting of the assigned mobile number of the SIM with its serial number.

(e) The PTEs shall be enjoined to include processes to verify the submitted information and data, subject to the applicable provisions of the Data Privacy Act, its IRR, and other relevant issuances of the National Privacy Commission.

Online users know that they cannot communicate or exchange data with one another except through some service providers to whom they must submit specific personal information for successful registration. The conveyance of this information takes them out of the private sphere, making the expectation of privacy regarding them an expectation that society is not prepared to recognize as reasonable.

Here, there are no controls to guard against the potential information leakage in the platform provided by the PTEs. When the access code of the control programs of a platform is broken, any intruder can use the data for whatever purpose, or worse, manipulate the data stored within the system[53] and eventually use the same to target and deceive online users in every transaction.

As technology advances, the level of reasonably expected privacy decreases.[54] The measure of protection granted by reasonable expectation declines as relevant technology becomes more widely accepted. Further, the factual circumstances determine the reasonableness of the expectation. However, other factors, such as customs, physical surroundings, and practices of a particular activity, may create or diminish this expectation.

The mandatory registration leaves end-users with no agency for an alternative option. As an illustration, if one forfeits to register their SIM,

---

53 *Ople v. Torres*, supra note 28.

54 *Id.*

deactivation results in the inability to communicate using mobile devices. This leaves an individual with no alternative where the element of choice exists. Leaving little to no element of choice does not assure the individual of a reasonable expectation of privacy. In the SIM Registration Act, wide discretion is given to PTEs regardless of the technology used, and any safeguard for the leak of databases cannot be inferred from its provisions. Note also that a SIM card carries a unique telephone number and stores some personal data. Without it, phone calls cannot be made, text messages cannot be sent, and transactions using ecommerce phone apps cannot be established. No SIM card will be sold to an individual who refuses to provide personal information. Policy considerations are accorded the widest latitude of deference, but modern times call for privacy fears that may result in irreversible damage to fundamental rights.

VI. CONCLUSION

The paradox of privacy remains a dynamic legal theory that casts a shadow over our privacy laws. Regulating the gray area where the freedom of choice and control are protected comprises a metaphysic web. The contours of the paradox entail the trade-off of our privacy and risks to attain benefits such as protecting a privacy right. Looking at privacy trade-offs in the form of mandatory registration in a particular context demonstrates that no standard of the privacy paradox creates a model for policy formulation. This essay has argued that the intrusions so often avoided are warranted by our actions.

In the context of online privacy, individuals have an implicit understanding that platforms will have access to at least some of their information. Still, the extent to which this information is collected and used and the limits of their control over such processes are mostly inscrutable. When technology has commanded almost all aspects of people's lives, such would be the advent of technological unthinking, where people thoughtlessly surrender their actions to such entity.

While legislation offers innovative safeguards that address modern issues, privacy fears in the information age may demand overwhelming intrusions under the pretext of protection. With technological strategies progressing at a galloping rate, like targeted marketing, the information shared for the purpose of assisting bureaucracy

may fall into evil hands. Today, the use of data is no longer limited to efficient purposes as information shared online or with others is easily subjected to misuse in a society of unwitting individuals. With fervor, the Court notes that "data may be gathered for gainful and useful government purposes; but the existence of this vast reservoir of personal information constitutes a covert invitation to misuse, a temptation that may be too great for some of our authorities to resist."[55]

The dynamism of sacrificing personal privacy to restrict unwanted intrusions maintains the privacy paradox. Ultimately, the unresolvable nature of the privacy paradox will continually challenge privacy regulations and protections in the future. One would expect that unless the underlying gaps in the legal system are properly addressed, the privacy paradox remains until it musters enough strength to become an antinomy that would disrupt privacy laws in the information age.

[55] *Ople v. Torres*, supra note at 28.

4

Making the Fundamental, Absolute: Expanding the List of Non-derogable Rights to Include the Right to Privacy

by Frances Zarah P. de la Peña

MAKING THE FUNDAMENTAL, ABSOLUTE: EXPANDING THE LIST OF NON-DEROGABLE RIGHTS TO INCLUDE THE RIGHT TO PRIVACY

*Frances Zarah P. de la Peña**

Not all rights are created equal.

There is no surprise here. Even from a non-pedagogical perspective, the right to travel or abode can never stand *mano a mano* with the right to life, nor can the right to a peaceful assembly be compared to the right to free speech or the right to freely exercise one's religion.

There are two (2) distinct and well-entrenched manifestations of such statement: First, in the form of the different levels of constitutional muster that laws must hurdle when challenged and the recognition of derogable rights under the International Covenant on Civil and Political Rights (ICCPR).

First, Philippine jurisprudence has developed three (3) tests of judicial scrutiny.[1] The strict scrutiny test applies when a classification either interferes with exercising fundamental rights, including the basic liberties guaranteed under the Constitution, or burdens suspect classes.[2] The intermediate scrutiny test applies when a classification does not involve suspect classes or fundamental rights, but requires heightened scrutiny, such as in classifications based on gender and legitimacy.[3] Lastly, the rational basis test applies to all other subjects not covered by the first two tests.

Second, Article 4 of the ICCPR, which the Philippines is a party to,[4] empowers States with a derogation power, which allows governments to temporarily suspend the application of some rights in the exceptional

---

* Frances Zarah P. de la Peña is a third-year Juris Doctor student at the University of St. La Salle. She is currently the Vice Chairperson and member of the Editorial Board of the USLS Law Journal.

1 *Ang Ladlad LGBT Party v. COMELEC,* 632 Phil. 32, 77 (2010), citing Joaquin Bernas, S.J. The 1987 Constitution of the Philippines: A Commentary 139-140 (2009).

2 In *Central Bank Employees Association, Inc. v. ESP* (id. at 693-696, citations omitted), it was opined that, "in the landmark case of *San Antonio Independent School District v. Rodriguez* (411 U.S. l; 93 S. Ct. 1278; 36 L. Ed. 2d 16 [1973] U.S. LEXIS 91), the U.S. Supreme Court in identifying a 'suspect class' as a class saddled with such disabilities, or subjected to such a history of purposeful unequal treatment, or relegated to such a position of political powerlessness as to command extraordinary protection from the majoritarian political process, articulated that suspect classifications were not limited to classifications based on race, alienage or national origin but could also be applied to other criteria such as religion.

3 Dissenting Opinion of Retired Chief Justice *Artermio V. Panganiban in Central Bank Employees Association, Inc. v. BSP*, id. at 648.

4 According to the UN Treaty Body Database, the Philippines signed and ratified the same on Dec. 19, 1966 and Oct. 23, 1986, respectively.

circumstance of a 'state of emergency'. Before a State moves to invoke Article 4, two fundamental conditions must be met: First, the situation must amount to a public emergency that threatens the life of the nation, and second, the State party must have officially proclaimed a state of emergency. When declaring a state of emergency with consequences that could entail derogation from any provision of the Covenant, States must act within their constitutional and other provisions of law that govern such proclamation and the exercise of emergency powers.[5]

Given the permissibility of certain rights that can be derogated suggests the similar existence of rights that can never be derogated—that is, they cannot be suspended even in a state of emergency. Article 4(2) of the ICCPR provides that no derogation is permitted for: (i) right to life,[6] (ii) freedom from torture or cruel, inhuman and degrading treatment or punishment; and freedom from medical or scientific experimentation without consent,[7] (iii) freedom from slavery and servitude,[8] (iv) freedom from imprisonment for inability to fulfill a contractual obligation,[9] (v) prohibition against the retrospective operation of criminal laws,[10] (vi) right to recognition before the law,[11] and (vii) freedom of thought, conscience, and religion.[12]

The existence of these tiered tests and the recognition that certain rights stay primordially protected regardless of the situation lends only to the conclusion that different rights are treated differently.

However, quite notable is the apparent absence of the right to privacy, despite its fundamental nature as a right and the pervasiveness of its recognition among States around the world.

The right to privacy means the "right to be let alone"[13] and is the "beginning of all freedoms."[14] In Philippine law, the concept of privacy is enshrined in the Constitution. It is regarded as the right to be free from unwarranted exploitation of one's person or from intrusion into one's private activities in such a way as to cause humiliation to a person's

---

5 See UN Human Rights Committee General Comment No. 29

6 ICCPR, Article 6.

7 ICCPR, Article 7.

8 ICCPR, Article 8(1) and (2).

9 ICCPR, Article 11.

10 ICCPR, Article 15.

11 ICCPR, Article 16.

12 ICCPR, Article 18.

13 *Morfe v. Mutuc*, G.R. No. L-20387, January 31, 1968.

14 *Id.*

ordinary sensibilities.[15] The Philippine Constitution guarantees the right against unreasonable searches and seizures and the right to privacy of communication and correspondence.[16] Put differently, everyone has the right to the protection of the law against such interference or attacks.[17] It has been described as the most comprehensive of rights and the right most valued by civilized men.

Internationally, the right to privacy is also widely recognized in treaties of general application, such as the United Nations Convention on Migrant Workers,[18] the UN Convention on the Rights of the Child,[19] African Charter on the Rights and Welfare of the Child,[20] African Union Principles on Freedom of Expression,[21] American Convention on Human Rights,[22] American Declaration of the Rights and Duties of Man,[23] Arab Charter on Human Rights,[24] ASEAN Human Rights Declaration,[25] and the European Convention on Human Rights.[26] This is important to note, given that wide practice can lead to the existence of customary international law, which under international law is a source of State obligation.[27]

The most popular of the international treaties dealing with the right to privacy is the ICCPR. Article 17(1) of the ICCPR mandates that, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor unlawful attacks on his honour and reputation."

Interestingly enough, the proviso attached to the right to privacy, such that an individual's person or privacy cannot be subject to arbitrary or unlawful interference, is the same restriction given to the right to life. Article 6 of the ICCPR also prescribes that, "No one shall be arbitrarily deprived of his life." In other words, life may be taken away when the

---

15 *Hing v. Choachuy, Sr.*, G.R. No. 179736, June 26, 2013.

16 Const.art. III, §§ 2-3.

17 *In the Matter of the Petition for Issuance of Writ of Habeas Corpus of Sabio v. Sen. Gordon*, G.R. No. 174340, October 17, 2006.

18 Article 14.

19 Article 16.

20 Article 10.

21 Article 4.

22 Article 11.

23 Article 5.

24 Article 16 and 21.

25 Article 21.

26 Article 8.

27 Article 38(1)(b), ICJ Statute: "The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:

xxx

international custom, as evidence of a general practice accepted as law;"

reason is not arbitrary—for instance, in cases of armed conflict when dealing with combatants.[28]

This is a cause for conversation because while privacy is not considered a non-derogable right, like the right to life, it has a proviso on allowing derogation as long as the reason is not arbitrary. While it is recognized that the right to life may be interpreted in a more profound and fundamental perspective, the right to privacy cannot be said to be lacking in that regard. For instance, the right to unreasonable searches and seizure is grounded on the right to protect one's person—from his personal effects to what society can reasonable expect for him to treat as private. Effectively, the existence of this penumbral right[29] is a person's greatest tool against the capricious and often arbitrary acts of the State.

Indeed, the greatest dominator of all the non-derogable rights is its attachment as an intrinsic nature of humanity—such that every human, at a bare minimum, deserves to be accorded such rights. The right to privacy is no different. It is the exclusive means by which one can truly exercise other fundamental rights and realize its objectives.

It is not farfetched to say that like the right to life, when the right to privacy is taken away, one ceases to maintain the "humanity" aspect of life.

---

[28] See ICRC, How does law protect in war? - Online casebook "In a generic sense, combatants are members of the fighting forces of the belligerent parties to an international armed conflict. The main feature of their status is that they have the right to directly participate in hostilities ('combatant privilege'). Nevertheless, they must respect IHL and thus be punished, should they commit violations.

In addition to having the right to participate in hostilities, combatants are entitled to POW status, if they fall into enemy hands during an international armed conflict. Among other measures aimed at ensuring they are well treated, this protective status entails that they may not be prosecuted for their mere participation in hostilities."

[29] See Griswold v. Connecticut, 381 U.S. 479 (1965) where Justice Douglas wrote that the Bill of Right's specific guarantees have "penumbras," created by "emanations from these guarantees that help give them life and opinion." That is to say that the "spirit" of the First, Third, Fourth, Fifth, and Ninth Amendment as applied against the states by the Fourteenth Amendment, creates a general "right to privacy" that cannot be unduly infringed.

5

Going Toe to Toe with the Sacred Freedom of the Press to Protect One's Right to Privacy

By Steffani Mitchelle M. Patriarca

GOING TOE TO TOE WITH THE SACRED FREEDOM OF THE PRESS TO PROTECT ONE'S RIGHT TO PRIVACY

*Steffani Mitchelle M. Patriarca**

The Filipino people put high emphasis on, and are in fact hungry for, their right to be informed. The 1987 Philippine Constitution and a multitude of laws promote said right. From the right to be informed of all kinds of government activities, up to government officials' individual assets and liabilities, and even the criminal history of every person, you name it, the Philippines has (or should have) a record of it. After all, a typical Filipino often finds himself wanting information to be available. Concomitantly, the Philippine Constitution guarantees press freedom that presumably goes hand in hand with the right to information.

Is it impossible that one would want information concerning them deleted and ultimately forgotten? Does the Philippines cater to this need? Or is this a concern of too little importance?

Assuming that Juan de la Cruz has been accused of rape of a minor under Article 266-A of the Revised Penal Code. The case gained media traction and became one of the most talked-about topics in the country like the infamous Vizconde Massacre. Later on, the judge ruled that Juan had nothing to do with the unfortunate event and was in the wrong place at the wrong time. That determination became final and unappealable, and the victim's family even accepted the verdict. A decade later, when a person "Googles" the name Juan de la Cruz, his photograph and name still appear as having previously been accused of the dastardly crime. As a result, Juan had trouble forging meaningful relationships, finding work, and gaining credit from any banking institution, among many other troubles.

The Philippines has taken steps to promote the so-called "right to be forgotten", but are they enough? The said right may perhaps be deduced from Article III, Section 3(1) of the Constitution which states, that "[t]he 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." The Supreme Court discussed the three strands of the right to privacy, viz: (1) locational or situational privacy; (2) informational privacy; and (3) decisional privacy. The Supreme Court further discussed that the right to informational privacy is the right

of individuals to control information about themselves.[1] But does this right to control information include the specific right to order the removal of information that has become public?

The "right to be forgotten" may also be dissected from the Data Privacy Act of 2012[2] ("DPA"). Section 16 of the DPA sets forth the right of every data subject to dispute the inaccuracy or error in the personal information and have it corrected immediately, order the removal of personal information that are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected, and be indemnified for any damages due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

Relative to the foregoing, Section 13 of the DPA allows the processing of sensitive personal information such as criminal proceedings, when it is provided for by existing laws and regulations and when such information is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

In an advisory opinion[3] rendered by the National Privacy Commission ('NPC') Privacy Policy Office regarding the extent of processing and disclosure of criminal history and its publication in newspapers, media, and government websites vis-à-vis the provisions of the Data Privacy Act of 2012, it was opined that:

> The DPA recognizes that journalists process personal and sensitive personal information when reporting on criminal cases on television and newspapers. As a special case, personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations, is outside of the scope of the DPA –

---

* Steffani Mitchelle M. Patriarca is a second-year Juris Doctor student at the University of St. La Salle. She is a member of the Editorial Board of the USLS Law Journal.

1 *Vivares v. St. Theresa's College*, G.R. No. 202666, September 29, 2014.

2 Republic Act 10173 (2012).

3 Advisory Opinion No. 2019-024 <https://www.privacy.gov.ph/wp-content/files /attachments/advopn/2019/v1%5BRedacted%5D%20Advisory%20Opinion%20No.%202019-024.pdf> (visited October 6, 2022).

but only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.

In addition, these publishers, editors, or duly accredited reporters, who are considered as personal information controllers (PICs) or personal information processors (PIPs) within the meaning of the DPA, are still bound to follow the law and related issuances with regard to the processing of personal data, upholding rights of their data subjects and maintaining compliance with other provisions that are not incompatible with the protection provided by Republic Act No. 53.

As to the posting of cases on the Department of Justice (DOJ) website, such processing is allowed under Section 13(b) and (f) above as part of their mandate under the Administrative Code of 19878 and other applicable laws and regulations on the matter. Please note, however, that the said processing is limited only to the minimum extent necessary to achieve the specific purpose, function, or activity of the DOJ, and the agency is not precluded from adhering to the general data privacy principles as well as the requirements of implementing measures to secure and protect personal data.

On the matter of the Constitutionally guaranteed right to information and freedom of the press vis-à -vis right to privacy, the same advisory opinion explained that the NPC recognizes the vital role of the media in protecting the interest of the public. As such, newspapers should be given such leeway and tolerance to enable them to courageously and effectively perform their essential role in our democracy.[4]

Although the right of media and government agencies to process such sensitive personal information is protected by law, it is not absolute. Their processing is limited to a fair and lawful exercise, and not in an overly intrusive and excessive manner which may prejudice an individual's privacy rights.

---

[4] *Lopez v. Court of Appeals*, G.R. No. L-26549, July 31, 1970.

In addition to the provisions of the DPA, one possible remedy is a writ of habeas data. It is a remedy available to any person whose right to privacy in life, liberty, or security is violated or threatened by an unlawful act or omission of a public official or employee or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party. It is an independent and summary remedy designed to protect an individual's image, privacy, honor, information, and freedom of information, and to provide a forum to enforce one's right to the truth and informational privacy. It seeks to protect a person's right to control information regarding oneself, particularly when such information is being collected through unlawful means to achieve illegal ends.[5]

After a summary hearing on the petition and if the allegations are proven by substantial evidence, the court shall enjoin the act complained of, or order the deletion, destruction, or rectification of the erroneous data or information and grant other relevant reliefs as may be just and equitable. It should be emphasized, however, that the operation of the writ of habeas data is conditioned upon a clear showing of the indispensable requirement of an actual or threatened violation of the aggrieved individual's right to privacy in life, liberty, or security.

Going back to the situation of Juan, may he validly request that all information regarding his past criminal record be removed? Are the preceding provisions of law and the Supreme Court's decisions considered enough basis to go to court and pray that a particular news article or information be deleted? Given all the foregoing, the Philippines has no definitive answer.

A foreign jurisdiction has a more decisive approach to this matter. In one case decided by the European Union Court of Justice, the facts show that in 2010, a quick search of Mr. Mario Costeja González's name on Google resulted in links to La Vanguardia's digitized 1998 newspaper article about the auction of his foreclosed home. At that time, the attachment proceedings for the recovery of his social security debts have been fully settled, and Mr. González claimed that reference to the 1998 article was now entirely irrelevant.

In that landmark case, the European Union Court of Justice ruled that a data subject may require the operator of a search engine to remove from the list of results displayed following a search made based on his name links to web pages published lawfully by third parties and containing

---

5 *Vivares v. St. Theresa's College*, supra note 1.

true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be 'forgotten' after a specific time.[6]

The European Union Court of Justice admitted that removing links from the list of results could, depending on the information at issue, affect the legitimate interest of internet users potentially interested in having access to that information. It emphasized that in these situations, a fair balance should be sought in particular between that interest and the data subject's fundamental rights. It further said that balance might, however, depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information. This interest may vary, in particular, according to the role played by the data subject in public life.[7]

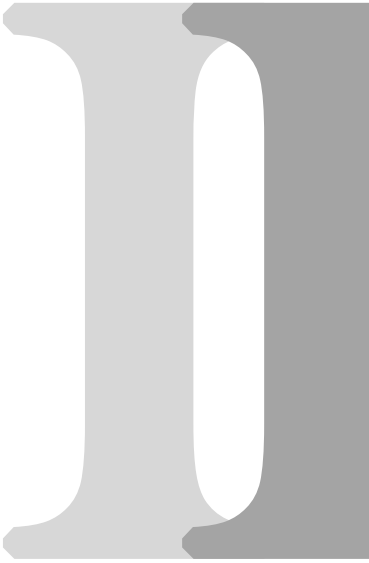
Compared to the Philippines, the European Union has taken a more decisive action while the Philippines treads lightly on this matter. The Philippines leans towards the protection of the freedom of the press.

It is high time for the Philippines to take decisive steps to protect its citizens' right to privacy, especially when the reputation of its innocent citizens is at stake. In this age of information, the Philippine government must also see to it that Filipinos may still pursue their full potential and avail of all possible opportunities and not be prejudged by information that serves no purpose than to state useless information and no longer relevant.

---

6 Google Spain SL v. Agencia Española de Protección de Datos, Judgment, Case C- 131/12, ECLI:EU:C:2014:317, (CJEU May 13, 2014).

7 *Id.* ¶ 81.



LANGUAGE AND INFORMATION DECEPTION

6

Deceptive Use of Language and Information Dissemination in Estafa

By Atty. Maria Reylan M. Garcia

DECEPTIVE USE OF LANGUAGE AND INFORMATION DISSEMINATION IN ESTAFA

*Atty. Maria Reylan M. Garcia**

Article 315 of the Revised Penal Code enumerates three (3) forms of committing the crime of Estafa: (a) with unfaithfulness or abuse of confidence; (b) by means of false pretenses or fraudulent acts; and (c) through fraudulent means. More simply, the first form is referred to as Estafa with abuse of confidence, and the second and third forms are referred to as Estafa by means of deceit.

Most of the publicized cases of Estafa and arguably much of its actual occurrence are by means of deceit. This may be attributed to the Filipinos' tendency to rely on served-on-a-plate information rather than personal research when developing commercial beliefs. In 2015, Nielsen's Global Trust in Advertising Survey showed that 91% of consumers in the Philippines "placed trust in word-of-mouth recommendations from people they know." Further, consumer opinions posted online enjoy a high 75% rating.[1] Fast forward to today when widespread, rapid, and convenient use of modern information dissemination transpires owing to a huge online presence of Filipinos estimated at 73 million users[2], deceitful schemes like networking scams spread like a virus.

As early as 2010, a financial fraud scheme by Aman Futures Group Phil, Inc. ("Aman") allegedly swayed some PhP 12B worth of money from 15,000 investors mostly from the Visayas and Mindanao islands. In particular, a certain Julius M. Labunog together with other complainants pooled their money amounting to PhP 29M from August 22 to September 17, 2010, to be invested in Aman, and upon filing a criminal complaint they claimed a total of PhP 44M (which comprised of their actual investment plus interest computed at the rate of return promised to them in damages).[3]

---

* Atty. Maria Reylan M. Garcia is a former Editor-in-Chief of the USLS Law Journal. She graduated her Juris Doctor degree in 2017 and was top 3 in her class. She is now engaged in private law practice under Sayno Law Office in Iloilo City where she actively litigates in criminal, civil, labor, and administrative cases.

1 CNN Philippines, Philippines trust word-of-mouth recommendations the most – Nielsen, <https://www.cnnphilippines.com/business/2015/09/29/Filipino-consumers-prefer-word-of-mouth-recommendations-Nielsen-Global-Trust-in-Advertising-Survey.html> (visited 29 August 2022).

2 Philippines – Country Commercial Guide, Department of Commerce, InternationalTrade Administration,<https://www.trade.gov/country-commercial-guides/philippines-ecommerce> (visited 29 August 2022).

3 Department of Justice Press Release March 11, 2013, https://www.doj.gov.ph/news_article.html?newsid=164 (visited 29 August 2022).

In 2015, another swindling scheme hit the headlines when an Egyptian national Ashraf Mohamed Abdelrahman was tricked into investing PhP 38.4 M with a promise of 30% monthly interest. The corporation involved was HPI Direct Sales and Trading Corporation ("HPI" also known as Program International Direct Sale Corporation). HPI allegedly duped many investors for over PhP 1B the HPI chairman issued. The Egyptian national initially trusted HPI executives after they issued postdated checks to him until January 2016 of which he received the promised interest from June up to September 2015. However, by October 2015 the bank informed him that the HPI account has been closed.[4]

HPI's issuance of post-dated checks as a form of guarantee was also the same scheme employed by Forex Investment Scheme allegedly founded by a certain Baarde who was a former Bureau of Internal Revenue employee. His scam involves victims, mostly from the province of Capiz, investing amounts ranging from PhP 100,000 to PhP 200,000 in exchange for high returns 20% return on their investment. Baarde then issued postdated checks which reflected the investors projected interest earnings; however, upon deposit, these checks bounced for lack of funds and the trading system they maintained ended up hacked and can no longer be restored. As per news reports,[5] the money involved in this scheme is estimated between PhP 7.2M to PhP 14.4M.

Also, a popular type of fraudulent networking scheme alongside the investment front, is the buying and selling of health products that are not properly registered with the Food and Drug Administration. This, the so-called investment packages worth PhP 8,777, and the share subscription investment opportunity for Php1M earning 1% every 6 months of the company's gross sales, is what enabled I7 Global Corporation to sway many investors to part with their hard-earned money.[6]

More recently, the infamous Chiyuto Investment scam by the Chiyuto Creative Wealth Documentation Facilitation Services also made to the national broadsheets with the Securities and Exchange Commission

---

4 Estafa complaint filed vs HPI execs over 1B investment scam, Rappler, March 8, 2016,<https://www.rappler.com/business/125052-estafa-charges-hpi-investment-scam/> (visited 29 August 2022).

5 Multimillion peso scam more investment con victims in capiz surface, The Daily Guardian, February 11, 2019 <https://dailyguardian.com.ph/multimillion-peso-scam-more-investment-con-victims-in-capiz-surface/< (visited 29 August 2022).

6 NBI Operatives nab 6 alleged investment scammers in QC, PNA, May 25, 2022 <https://www.pna.gov.ph/articles/1175229> (visited 29 August 2022).

issuing notices warning the public. Chiyuto's scheme is likened to a double-your-money roulette game which guarantees a 100% return on investment in one day, 30 days, or 45 days. This means the investor can put in any amount from PhP 1 to PhP 1M and Chiyuto uses a roulette to determine the pay-out schedule. Thereafter, the investors will be given promissory notes stating the amount of return and when the earnings will be claimed. They also offer a 5% referral commission rate and raffles for brand-new cars and motorcycles. This scheme was discovered by the SEC and because Chiyuto did not register or was not authorized by the SEC to sell securities, its Certificate of Incorporation was thereafter nullified.[7]

The abovementioned scams essentially operate following the Ponzi scheme which has been time and again noted and discussed by Philippine jurisprudence. As defined in the case of *People vs. Balasa,*[8] the Ponzi scheme, which was named after Charles Ponzi who promoted the scheme in the 1920s, involved the issuance of bonds that offered 50% interest in 45 days or a 100% profit if held for 90 days. In this scheme, the money Ponzi received from later investors will be used to pay the skyrocketing rates of return to earlier investors. Initially, this will convince more investors to give their money to Ponzi because they would very much like to realize high returns themselves. The tragedy occurs however when the number of later investors cannot keep up with the exorbitant interests to be paid to the earlier investors.

As discussed in the Balasa case:

> However, the Ponzi scheme works only as long as there is an ever-increasing number of new investors joining the scheme. To pay off the 50% bonds Ponzi had to come up with a one-and-a-half times increase with each round. To pay 100% profit he had to double the number of investors at each stage, and this is the reason why a Ponzi scheme is a scheme and not an investment strategy. The progression it depends upon is unsustainable. The pattern of increase in the number of participants in the system explains how it is able to succeed in the short run and, at the same time, why it must fail in the long run. This game is difficult to sustain over a long period of time because to continue paying the promised profits to early

---

7 SEC orders Creative Wealth to stop investment-taking operations, February 5, 2021, Philippine Daily Inquirer, <https://business.inquirer.net/317012/sec-orders-creative-wealth-to-stop-investment-taking-operations>, (visited 29 August 2022).

8 *People v. Balasa*, G.R. No. 106357, 3 September 1998.

> investors, the operator needs an ever larger pool of later investors. The idea behind this type of swindle is that the "con man" collects his money from his second or third round of investors and then absconds before anyone else shows up to collect. Necessarily, these schemes only last weeks, or months at most.[9]

To further elucidate, in the case of *People vs. Menil,*[10] the accused also made use of the Ponzi scheme as in the case of *Balasa*; however, instead of slots, coupons were given as proof of investment. They solicited investments from the public with the assurance that the investors' money will be multiplied tenfold after 15 calendar days. At the beginning since the amounts invested were small, the accused were able to pay off the interest on the investments on time; but, when the number of investors increased to the point when the daily investments reached millions of pesos, the payments of returns were then delayed until it completely stopped. And more recently, in the case of *People vs. Tibayan,*[11] the private complainants were induced to invest in Tibayan Group Investment Company because of the offer of high-interest rates and the assurance of the return on their investments. As in *Balasa* and *Menil*, the private complainants in *Tibayan* received certificates of share and postdated checks as guarantees. The checks, however, were dishonored upon encashment, and the TGICI office closed down without private complainants having been paid.

The deceit in these swindling schemes begins as early as the recruitment of initial investors wherein the accused will overwhelm the unknowing victims with tons of information – supposed relevant statistics, research results, and projection graphs. The investors will usually be asked to attend orientation programs or acquaintance events where they will eventually be led to the conclusion of how mediocre their income utilization is sans the investment and how explosive their wealth is going to be with the investment. They will be shown larger-than-life computations of potential earnings from interest and return on investment. The investor then is made to believe that he can earn millions, buy luxury merchandise, and travel to premium destinations in a matter of months.

And while the information disseminated may not necessarily be false, most often they are vague, sugarcoated, and redacted. Indeed, these schemes inform the investor that they need to recruit "x" number of new members for them to earn or that they need to purchase first some

---

9 *Id.*

10 *People v. Menil*, G.R. No. 115054-66, 12 September 2000.

11 *People v. Tibayan*, G.R. Nos. 209655-60, 14 January 2015.

products at a bargain so they can sell at a much higher price. However, they are not notified of how unsustainable a classic pyramid scheme may become. For example, if each member will be asked to recruit six (6) members, the 12th layer of the pyramid will necessarily have 2.2 billion members and they ought to recruit 13 billion more members which is more than the world's population as of this writing. They are also not notified of how long and how tedious selling virtually unknown products is to the public. Furthermore, while the scams will present government licenses and permits to establish their credibility and legitimacy, frequently they do not have the required secondary license from the Securities and Exchange Commission to solicit and receive investments from the public or issue investment contracts or securities as defined by the Securities Regulation Code. The absence of this secondary license is what they usually conceal. In addition, their online promotional materials which include digital posters, videos, social media posts, and even private messages are well-crafted to garner a profitable view or click at the very least.

For these types of schemes, it is therefore the clever use of language and cunning dissemination of information that keep the swindling ball rolling. However clever and cunning, the law is determined to criminalize these. Aside from Estafa by means of false pretenses or fraudulent acts under Article 315 2 (a) of the Revised Penal Code, other statutes penalize this deception. The usual practice of these schemes in issuing postdated checks as guarantees which will later be dishonored because the drawer's bank account is already closed or with insufficient funds may be prosecuted under Batas Pambansa Blg. 22 which penalizes the issuance of bouncing checks. Also as previously discussed, the absence of a secondary license to be engaged in the soliciting and receiving of investments from the public and to issue investment contracts or any kind of security is a violation of the Securities Regulation Code. In the same vein, the absence of any authority or a Certificate of Incorporation from the Securities and Exchange Commission will also make these scams liable under the Revised Corporation Code.

However, it is Article 315 (2) (a) of the Revised Penal Code that categorically identifies deceit to be among its elements. Article 315 (2) (a) provides that:

> Any person who shall defraud another by any of the means mentioned herein below shall be punished by:
>
> x x x

2. By means of any of the following false pretenses or fraudulent acts executed prior or simultaneously with the commission of the fraud:

    (a) by using a fictitious name, or falsely pretending to possess power, influence, qualifications, property, credit, agency, business, or imaginary transactions, or by means of other similar deceits.

x x x

Otherwise said, the elements of the crime of Estafa under Article 315 (2) (a) are:

i. There must be a false pretense, fraudulent acts;
ii. Such false pretense, fraudulent act or fraudulent means must be made or executed prior to or simultaneously with the commission of the fraud;
iii. The offended party must have relied on false pretense, fraudulent act x x x and was thus induced to part with his money or property;
iv. As a result thereof the offended party suffered damage.[12]

The fraudulent act or fraudulent means referred to in the first element may be committed under any of the following:

a. By using a fictitious name;
b. By falsely pretending to possess: (a) power, (b) influence, (c) qualifications, (d) property, (e) credit, (f) agency, (g) business or imaginary transactions; or
c. By means of other similar deceits[13]

The above-discussed financial fraud schemes encompass the enumerated elements. As to the first element of a false pretense or fraudulent act, most of these schemes pretend to possess that they have the necessary qualifications to manage investments. While most purport to have official papers such as (a) Certificate of Registration from the Bureau of Internal Revenue, (b) Business Permit from the local government unit, (c) Business Name Registration from the Department of Trade and Industry, and (d) Certificate of Incorporation from the Securities and Exchange Commission, they almost always conceal their lack of the required secondary license to be engaged in the soliciting and receiving of

---

12 Reyes, Luis, B., The Revised Penal Code Criminal Law Book Two Articles 114-367, 18th edition, (2012).

13 *Id.*

investments from the public and to issue investment contracts or any kind of security supposedly issued by the Securities and Exchange Commission. Worse, some schemes completely do not have any permit or license at all and would resort to falsifying the same. In addition, these schemes also make use of testimonies from supposed personalities to entice would-be investors and build the scheme's credibility. However, the testimonies of these personalities could have been paid, taken out of context, or completely fabricated.

These schemes also pretend to have the property or credit that will drizzle credibility over their promises of high rewards and high returns for shorter periods. That despite the exorbitant projection of income, these schemes will be able to make good because they allegedly have a consistent stream of assets and an influx of investments coming from their exponential projection of new members being recruited. Then again, as previously discussed the classic pyramid structure of multi-level marketing is unsustainable.

As to the second element that such false pretense or fraudulent act must have been made or executed prior to or simultaneously with the commission of the fraud, the presentation of these qualifications is done in orientation programs or acquaintance events whether in big or small groups. After the said program or event, the investor, already convinced and trusting, will sign up and pay the required investment, capital, subscription fee, participation fee, or any other inviting term these schemes use. Hence, the presentation of pretend qualifications was made prior to or at the same time as the parting of the investors' money. Considering that these financial fraud schemes utilize the Ponzi scheme which relies on the actual recruitment of new paying members for survival, a positive and convincing act performed by the scam artist is necessarily needed to reel the investors in.

As to the third element wherein the offended party must have relied on false pretenses and fraudulent acts and was thus induced to part with his money or property, the innocent investors would usually allege that the cause for their decision to invest is because they were convinced, and they were made to believe that the scheme is capable of managing their investment and bringing them profit.

As to the fourth element which is a result of the deceit, the offended party suffered damage; the same is usually alleged by complainants to be the amount of the actual investment plus interest computed at the rate of return promised.

Then again, despite the rampancy of these financial fraud schemes and the consistent use of familiar strategies such as the Ponzi scheme, the prosecution is still met with legal challenges. As an example, in the relatively recent case of *Favis-Velasco vs. Gonzales*[14] no deceit was attributed to the respondent because, in the Complaint Affidavit, the petitioners themselves admitted that they were the ones who sought for the respondent by asking a mutual friend to introduce them to the latter and more importantly it was through the representation of this mutual friend that made them invest their money. Hence:

> The petitioners failed to sufficiently allege all of the foregoing elements in their Complaint-Affidavit. Their allegation that respondent Jaye induced them through fraudulent representations and false pretenses to invest their money is instantly belied by their own statement in their complaint, to wit:
>
> 1.4 We are formally charging the Respondents co-conspirators with 35 counts of Estafa by unfaithfulness and abuse of confidence as defined under Article 315 paragraph 1 (b) and 35 counts of Estafa by false pretenses as defined by paragraph 2 (a) of the same Article of the Revised Penal Code, to wit:
>
> x x x x
>
> 2.2 We first heard about Respondent Jaye through a mutual friend Marianne Onate ("Ms. Onate") when we asked her who her broker was. She identified her broker as Respondent Jaye who is the wife of Respondent Bienvenido, a very close friend of her brother. We asked for an introduction to Respondent Jaye.
>
> It must be noted that the petitioners were the ones who asked Marianne Onate (Onate) to be introduced to respondent Jaye and it was Onate who introduced respondent Jaye as her broker. Clearly, it was through the representation of Onate that petitioners will earn substantial amount of money in the stock market that induced them to invest their money. Verily, no deceit or fraud could be attributed to respondent Jaye as would induce the petitioners to part with their money or property.

---

[14] *Favis-Velasco v. Gonzales*, G.R. No. 239090, 17 June 2020.

This case presents a legal loophole for the accused who are usually the higher-ups in the pyramid or Ponzi scheme. These higher-ups, to escape liability, will point out that another person induced the victim, who is usually a lower-ranking member or another investor. Criminal liability is by principle personal and despite all the elements being present if such elements were not committed or acted upon by the accused himself, the case against him will fail. Nevertheless, there is an exception to this principle, and this is when there is a conspiracy.[15] Hence, for this scenario, it is a must for the prosecution to establish a conspiracy between the person whose representation the investor relied upon and the higher-ups or the persons intended to be prosecuted.

It shall also be beneficial if a syndicated estafa complaint is filed. This is shown in the case of *People vs. Baladjay.*[16] Initially, this case discussed the nature of syndicated estafa or how Section 1 of PD 1689 qualifies the offense of Estafa if it is committed by a syndicate. Thus:

> Section 1. Any person or persons who shall commit estafa or other forms of swindling as defined in Articles 315 and 316 of the Revised Penal Code, as amended, shall be punished by life imprisonment to death if the swindling (estafa) is committed by a syndicate consisting of five or more persons formed with the intention of carrying out the unlawful or illegal act, transaction, enterprise or scheme, and the defraudation results in the misappropriation of moneys contributed by stockholders, or members of rural banks, cooperatives, "samahang nayon(s)," or farmers' associations, or funds solicited by corporations/associations from the general public.
>
> Synthesizing the two provisions of law, the elements of Syndicated Estafa, therefore, are as follows: (a) Estafa or other forms of swindling, as defined in Articles 315 and 316 of the RPC, is committed; (b) the Estafa or swindling is committed by a syndicate of five (5) or more persons; and (c) the defraudation results in the misappropriation of moneys contributed by stockholders, or members of rural banks, cooperatives, "samahang nayon(s)," or farmers' associations, or of funds solicited by corporations/associations from the general public.

---

[15] *Vizconde vs. IAC, People*, G.R. No. 74231 April 10, 1987 cites: It is fundamental that criminal responsibility is personal and that in the absence of conspiracy, one cannot be held criminally liable for the act or default of another.

[16] *People v. Baladjay*, G.R. No. 220458, 26 July 2017.

Essentially, in this case, because of a syndicated estafa complaint filed, the accused Baladjay could no longer use the defense that she has not personally transacted with the private complainants or that she has never known the supposed Multitel counselors to whom the victims of Multitel's fraudulent scheme delivered their money. These cannot prevail over the evidence and the fact that a syndicated estafa case was filed. *Baladjay cannot feign innocence by hiding behind her so-called "counselors" because not only did they positively identify her, she also signed the checks issued in favor of the investors*.

Hence, better chances at successful prosecution of these financial fraud schemes necessitate the filing of a complaint for syndicated estafa. This will not only assure the inclusion of the higher-ups who benefited the most but also puts into perspective the widespread and systematic use of deceptive language and the dissemination of deceptive information. During the trial, evidence of organized deceit will consequently require records of promotional and recruitment activities employed such as orientation programs, acquaintance events, and online dealings including its often viral social media presence. These records will show even beyond the judicial chambers that language and information are not just the modes but are essentially the core of deceit in financial fraud schemes.

7

Pleasure at the Expense of Others: How Deepfakes Conjure a Blurred Case of Free Speech

by April Therese L. Escarda

PLEASURE AT THE EXPENSE OF OTHERS: HOW DEEPFAKES CONJURE A BLURRED CASE OF FREE SPEECH

*April Therese L. Escarda**

Free Speech is never really free.

As it should.

Inasmuch as the constitutional guarantee of freedom is solidified as one of the most fundamental of rights, its permissibility is primarily judged on the effects it bears on anyone's ears. In *Calleja vs. Executive Secretary*, the Supreme Court clarified that a content-based prior restraint, i.e. the restriction is based on the subject matter of the utterance or speech,[1] is constitutionally permissible if it passes the clear and present danger rule, which rests on the premise that speech will likely lead to an evil which the government has a right to prevent.[2] Particularly, the Court followed its latest iteration in the form of the Brandenburg Test which explains that "constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[3]

Any attempt to stifle speech may succeed when the speech sought to be controlled directly incites or produces imminent lawless action. Absent the same, the challenge must fail.

An interesting and new development in the area of free speech is the rise of deepfake videos. Deepfakes are, in their most common form, videos where one person's face has been convincingly replaced by a computer-generated face, which often resembles a second person.[4] The term "deepfake" comes from the underlying technology "deep learning," which is a form of AI. Deep learning algorithms, which teach themselves

---

* April Therese L. Escarda is a third-year Juris Doctor student at the University of St. La Salle. She is also a Member Editor, Committee Head, University of St. La Salle College of Law Bar Operations; Third Year Batch Representative, University of St. La Salle College of Law Student Council; and a government employee, Talisay City, Negros Occidental.

1 *Chavez vs. Gonzales*, G.R. No. 168338, February 15, 2008.

2 *Atty. Howard M. Calleja, et al. v. Executive Secretary*, G.R No. 252578, 7 December 2021.

3 *Id*.

4 Biggs, T., & Moran, R. (2021, June 2). What is a deep fake? The Sydney Morning Herald. Retrieved January 3, 2022, from https://www.smh.com.au/technology/what-is-the-difference-between-a-fake-and-a-deepfake-20200729-p55ghi.html.

how to solve problems when given large sets of data, are used to swap faces in video and digital content to make realistic-looking fake media.[5]

While consequences of deepfakes seem harmless in regard to clearly satirical work, the same cannot be said when matters such as politics and other real life transactions are involved. Extensive spotlight has been given to the situation in Gabon, Africa, for instance when the military launched an ultimately unsuccessful coup after the release of an apparently fake video of leader Ali Bongo suggested that the President was no longer healthy enough to hold office.[6] In 2019, the CEO of a U.K-based energy firm listened over the phone as his boss — the leader of the firm's German parent company — ordered the transfer of €220,000 to a supplier in Hungary.[7] The CEO recognized the "slight German accent and the melody" of his chief's voice and followed the order to transfer the money [equivalent to about $ 243,000] within an hour. The €220,000 was moved to Mexico and channeled to other accounts.[8] An official with Euler Hermes, the insurance company, said the thieves used artificial intelligence to create a deepfake of the German executive's voice.[9]

However, what has not been the subject of heavy media coverage is the impact of deepfakes on women. The AI firm Deeptrace found 15,000 deepfake videos online in September 2019, a near doubling over nine months prior—a staggering 96% were pornographic and 99% of those mapped faces from female celebrities on to porn stars.[10] As new techniques allow unskilled people to make deepfakes with a handful of photos, fake videos are likely to spread beyond the celebrity world to fuel revenge porn.[11] As Danielle Citron, a professor of law at Boston University, puts it: "Deepfake technology is being weaponised against women."[12]

Notably, in 2020, Sensity AI, an organization that monitors the number of deepfakes online, found that of the thousands of celebrities,

---

5 Business Insider. (2021, January 22). What is a deepfake? everything you need to know about the AI-powered fake media. Business Insider. Retrieved January 3, 2022, from https://www.businessinsider.com/what-is-deepfake.

6 Written by Alexander Puutio, P. D. R. at the U. of T. (2020). Retrieved January 3, 2022, from https://www.weforum.org/agenda/2020/10/deepfake- democracy-could-modern-elections-fall-prey-to-fiction/.

7 Somers, M. (2020, July 21). Deepfakes, explained. MIT Sloan. Retrieved August 31, 2022, from https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

8 *Id*.

9 *Id*.

10 Sample, I. (2020, January 13). What are deepfakes and how can you spot them? The Guardian. Retrieved September 28, 2022, from https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

11 *Id*.

12 *Id*.

public figures and everyday people who had deepfakes made of them, only 35 of these individuals were American politicians.[13] Female celebrities in the United States and South Korea are the main targets of sexual deepfakes.[14]

While issues on privacy and copyright regarding deepfakes have been dealt with in great detail, the question on the permissibility of deepfakes still arise, especially when the same is argued to be done with the subject's consent. In other words, the question of whether a deepfake passes constitutional muster when the video is done with intent for personal use, or purely scientific or creative gain has yet to be answered.

There have been several instances when the U.S. Supreme Court applied the Brandenburg Test. In 1973, before the Supreme Court was the case of *Hess vs. Indiana*[15] wherein Gregory Hess, an Indiana University protester, said, "We'll take the fucking street later (or again)." To the Court, Hess's profanity was protected as the speech "amounted to nothing more than advocacy of illegal action at some indefinite future time." The Court held that "since there was no evidence, or rational inference from the import of the language, that his words were intended to produce, and likely to produce, imminent disorder, those words could not be punished by the State on the ground that they had a 'tendency to lead to violence.'"

In *NAACP v. Claiborne Hardware Co*.,[16] Charles Evers threatened violence against those who refused to boycott white businesses. The speech was protected: "Strong and effective extemporaneous rhetoric cannot be nicely channeled in purely dulcet phrases. An advocate must be free to stimulate his audience with spontaneous and emotional appeals for unity and action in a common cause. When such appeals do not incite lawless action, they must be regarded as protected speech."[17]

In fact, in the case of Clarence Brandenburg himself, when he was addressing a small gathering of Ku Klux Klan members, uttered derogatory words against blacks and jews such as, "Personally, I believe the nigger should be returned to Africa, the Jew returned to Israel."[18] There was even an instance of taking direct action when the accused said, "We are

---

13 Dunn, S. (2021, March 3). Women, not politicians, are targeted most often by deepfake videos Retrieved September 31, 2022, from https://www.cigionline.org/articles/women-not-politicians-are-targeted-most-often-deepfake-videos/.

14 *Id*.

15 414 U.S.105 (1973).

16 458 U.S. 886 (1982).

17 *Id*.

18 Brandenburg v. Ohio, 395 U.S. 444 (1969).

marching on Congress July the Fourth, four hundred thousand strong. From there, we are dividing into two groups, one group to march on St. Augustine, Florida, the other group to march into Mississippi. Thank you."[19] And still, the Supreme Court ruled that the Ohio punishing Brandenburg was unconstitutional.

From the foregoing, it appears that the bar is quite high for a valid restriction on speech. The fact that women or the general public may be enraged by the subject matter of the videos might not cross the threshold of directing imminent lawless action, even in a vacuum. This conclusion could also be supported by the fact that deepfakes created with sexual purposes is not tied down to a specific societal circumstance in time such as war time or societal upheaval. That is to say that the need or urge to create deepfakes are necessitated to exist in a wide plethora of situations.

The closest legal challenge in relation to free speech could be the invocation of the Miller test[20] as enunciated by the U.S. Supreme Court in *Miller vs. California*.[21] But even the use of "community standards" gives no definite answer as to the permissibility of deepfakes. Moreover, the literary, artistic, political, and scientific value of the work itself poses difficulty, especially when deepfakes are a continuing technological science—thereby incentivizing its potential use in other fields such as medicine and therapy.[22]

---

19 *Id*.

20 Three pongs of the Miller Test:
1) whether the average person applying contemporary community standards would find the work, taken as a whole, appeals to the prurient interest;
2) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and
3) whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value.

21 *Miller v. California*, 413 U.S. (1973).

22 Smith, N. B. and D. (2022, September 29). Ai could catch alzheimer's in brain scans 6 years earlier. Artificial Intelligence Can Detect Alzheimer's Disease in Brain Scans Six Years Before a Diagnosis | UC San Francisco. Retrieved September 31, 2022, from https://www.ucsf.edu/news/2019/01/412946/artificial-intelligence-can-detect-alzheimers-disease-brain-scans-six-years.

8

How Tyrants Padlock the Truth

by Jose Adrian Miguel P. Maestral

HOW TYRANTS PADLOCK THE TRUTH

*Jose Adrian Miguel P. Maestral**

Tyrants, who are they? They are prominently known to seize power, instill fear, and control the state and its people. One of the most notorious ways a tyrant can establish control is to hide the truth. This topic will tackle how state censorship happens in a domain ruled by a tyrant. Under Article III, Section 7 of the Constitution, "The right of the people to information on matters of public concern shall be recognized. Access to official records and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as the basis for policy development, shall be afforded the citizen, subject to limitations as may be provided by this law."[1] And yet, why hide away the truth?

Throughout history, tyrants, regardless of a state's government system, whether it be a monarchy, capitalist, or communist, have the possibility of tyranny existing in their respective strongholds. The use of state censorship played a vital role in hiding the truth from the world.

During the 1930s, a catastrophic famine took place in the Soviet Union and Ukraine, which was also under the influence of the Soviet Union. Peasants were forced off their lands to join state farms. Despite the shortages of food supplies, the state demanded grains and all other edible commodities, police officers and local party activists raided peasant households and seized everything edible: potatoes, beans, peas, and even live farm animals such as livestock and poultry. As a result, at least 5 million people perished from hunger across the Soviet Union. Among the 5 million were 4 million Ukrainians who died from food deprivation. Inside the Soviet Union, the topic of the catastrophic famine was never mentioned nor recognized by the Union of Soviet Specialists Republic (USSR). The discussions regarding these concerns were actively repressed, and economic statistics of the state were altered or hidden from the public.

Fear-mongering was so rampant that everyone in the country remained silent to preserve themselves from an imminent arrest and possibly death. Journalists that favored the side of the Soviet Union were given special privileges during their stay in the motherland. As the famine

---

* Miguel Maestral is a JD 1 student at the University of St. La Salle. He has had experience in writing, contributing to Panublion, the official publication of the Bacolod-based group CORE (Children Optimization for the Revitalization of the Environment), and also to EG Archive, the official publication of the USLS special interest club, Earthguards USLS, where he was once Auditor in his 1st year, President from 2nd to 3rd, and Vice President for External Affairs in his final years.

1 Constitution, (1987), Art. III, Sec. 7.

worsened, the Foreign Ministry in 1933 refused all requests to visit the poor condition in Ukraine. Journalists were only allowed to write certain words and phrases in their articles as the Soviet Union censored them. On the contrary, journalists, after traveling to Ukraine by train to interview peasants, wrote an article in *The Evening Standard* on March 31st of 1933 with the heading "Famine Rules Russia" explaining how the so-called 5-year plan had killed the bread supply, costing the lives of millions of Russians and Ukrainians. This was later denied by many as just an exaggeration as the public relied on the reports of the correspondent of Moscow to *The New York Times* Walter Duranty whose articles were more credible and widely read but were neutral to the concern of the famine. The Soviet Union and the United States gave him special recognition that Duranty received the Pulitzer Prize.[2]

In the Democratic People's Republic of North Korea the generations of the Kim family, with the first President Kim Il-Sung who described the great famine as the "Arduous March. Words such as "famine" and "hunger" were banned from their media, newspapers, television, and radio stations. Anyone who would dare speak that the cause of the hunger was due to the famine could get into serious trouble with the authorities.[3]

Following the death of the "Great Leader" Kim Il-Sung in 1994, he was succeeded by his eldest son Kim Jong-Il who became known as the "Dear Leader" of North Korea. When he was still 25 years old, Kim Jong-il volunteered to head the film industry of North Korea which was also part of his father's plan to cement his control in North Korea. Immediately, he was appointed the Cultural Arts Director. Kim Jong-il produced a film titled the *Sea of Blood* in 1969, where it was set in the 1930s while Korea was in the hands of Japanese occupying forces which the protagonist Sun-Nyo and her family suffered numerous tragedies under the Japanese until eventually pushed themselves to join the communist revolution and topple their oppressors. The film was supposed to be propaganda to promote his late father's ideology of Juche which translates to self-reliance.

Films were produced under Kim Jong-il's watchful eye.[4] However, all the films were loosely about his father who was hailed a hero and divine being of North Korea on the screen. Kim Jong-il now plans to create a

---

2 Kiger, P. J. (2019, April 16). *How Joseph Stalin starved millions in the Ukrainian famine* .History. com. Retrieved Available at: <https://www.history.com/news/ukrainian-famine-stalin> (visited 15 September 2022).

3 Blakemore, E. (2018, September 1). *North Korea's Devastating Famine*. HISTORY. https://www.history.com/news/north-koreas-devastating-famine.

4 Savage, M., 2011. *Kim Jong-il: The cinephile despot*. [online] BBC News. Available at: <https://www.bbc.com/news/entertainment-arts-16245174> (visited 15 September 2022).

narrative where it all begins in North Korea's sacred site, Mount Paektu. The narrative began when Kim Il Sung, before North Korea achieved independence, was the leader of the guerilla fighters against the Japanese forces on the slopes of Mount Paektu. As a sign to establish Kim Jong-il's role as heir apparent, he added himself to the family myth. The legend alleged that he was born in Mount Paektu, but historians believe he was born in Russia. So, in the tale, while the guerilla fighters fought in Mount Paektu, Kim Jong-il's birth was foretold by a swallow who had descended from heaven. The wintery night sky parted to show the brightest double rainbow ever seen, and a star appeared. The soldiers who witnessed this sang joyfully as they were assured that a new leader could someday succeed their great leader Kim Il Sung. The legend was made popular, written in books and songs, and even taught in their schools.

North Korea began issuing press releases to write and publish important "facts" about the rising leader. Anything that pleases his name and his dynasty's name was approved for publication in general circulation.[5]

In April 2014, Kim Jong-un the grandson of Kim Il-Sung, issued an order to "arrest people who had contacts with Christianity", this made religious persecution worse and harsher. The North Korean government also bans any religious activities in their country. Religious beliefs became an anti-state activity and were punishable as a political crime. The Database Center for North Korean Human Rights ever since 2007 has been publishing white papers on religious freedom yearly. Sources of such information come mostly from fugitives. In the year 2006, the Data Center has managed to gather 1,234 respondents for this study who confirmed the ban and the harsh persecutions that befall the believers. Among them, 46% confirmed that people involved in religious activities are sent to forced labor camps, while 38.6% say they have no knowledge of the punishments as they have no knowledge of religion, to begin with. Even religious information was censored in this state.[6]

In conclusion, there are many more of these tyrants that padlock the truth from the inhabitants of where they establish their rule of censorship. Crimes they commit while in power could be null as they may have possible immunity for being heads of their states, but someday justice may one day serve them as good always prevails over evil.

---

5 Maslin, J., 2015. *Review: 'A Kim Jong-il Production' Recounts a Bizarre Legacy*. [online] The New York Times. Available at: <https://www.nytimes.com/2015/02/17/books/review-a-kim-jong-il-production-recounts-a-bizarre-legacy.html> (Accessed 15 September 2022).

6 AsiaNews.it. (n.d.). *Religions almost completely wiped out in North Korea*. [online] NORTH KOREA. Available at: <https://www.asianews.it/news-en/Religions-almost-completely-wiped-out-in-North-Korea-51702.html> (visited 15 September 2022).

II

REFLECTIONS ON ARTIFICIAL INTELLIGENCE AND THE BIG TECH

9

Justitia Deus Ex Machina: The Legality and Feasibility of Artificial Intelligence as Judge and Justice in the Philippines

by Judge Michael Hanz D. Villaster

JUSTITIA DEUS EX MACHINA: THE LEGALITY AND FEASIBILITY OF ARTIFICIAL INTELLIGENCE AS JUDGE AND JUSTICE IN THE PHILIPPINES

*Michael Hanz D. Villaster**

Table of Contents

---

* *Cite as* Michael Hanz D. Villaster, *Justitia Deus Ex Machina: The Legality and Feasibility of Artificial Intelligence as Judge and Justice in the Philippines*, _____ (page cited) (2022).

** Municipal Trial Judge-At-Large (currently Acting Presiding Judge of the Municipal Trial Court in Cities Branches 3 and 6, Bacolod City); Bachelor of Laws (Juris Doctor), University of St. La Salle - Bacolod City (2009); National Moot Court Competition on International Humanitarian Law Champion (2007); Bachelor of Arts Major in Political Science (magna cum laude), University of St. La Salle - Bacolod City (2005).

I. INTRODUCTION

The theater and play plot device of *deus ex machina* first saw light in the works of ancient Greek tragedians such as Aeschylus and Euripides, as well as that of English playwright William Shakespeare. It uses the idea of an actor portraying a god, coming down from a riser onto the stage with the use of a machine- providing a solution to an irremediable situation and concluding the show with an upbeat ending. The story's main human protagonist yields to the god's pronouncement, as it is regarded to be infallible and omniscient. The fragility of the human's decision-making, limited by physiological and psychological constitutions hindering one to unfailingly deconstruct very convoluted propositions, ultimately subjugates the protagonist to defer to the "all-knowing being".

Other than the literary and performance realms that are heavily influenced by fatalism and religious views, the concept of *deus ex machina* has found its way in other aspects of life. Take for example the reliance of humans on the mercies and wonders of machines and technology. What used to be unperformable tasks are now efficiently and effectively decided upon and carried out by robots and smart tools. Quandaries traditionally befalling fields of manufacturing, medicine, transportation, and communication, to name a few, are now made simpler all thanks to scientific and technological advancements. Today more than before, many human functions are now being "controlled" and "charted" by unconventional software and hardware.

Having recognized the power of machines and technology, one interesting showcase of *deus ex machina* interaction is the accession of human beings to the abilities of the "all-knowing being" known as artificial intelligence ("AI").

Many day-to-day human operations — from the intricate and complex to the undemanding and mundane — are nowadays being dictated by AI. In personal affairs for instance, it is evidenced in the swiftness and clarity of one Zoom call meeting, the seamlessness of streaming a TV series from Netflix, and the viralness of dance moves and posts in TikTok and Facebook, respectively. In the more serious field of governance, where major choices are taken for the benefit of the common good, AI has displaced bureaucratic technocrats and politicians in accomplishing many chores usually completed cognitively. Lastly, in the more focused territory of judicial initiatives across the globe, many jurisdictions have conceded to the power of AI in making simple to complicated decisions.

As a member of the Philippine bench, I will attempt to discuss and zero in in this paper on the legality, utility, and reliability of AI in the various processes of the judicial arm of the government. With more specificity, this paper will endeavor to determine whether the usage of AI in the decision-making process of judges and justices involving cases confronting their courts will be lawful within the milieu of the Philippine Constitution and established rules, and whether its application is achievable and its results reliable given the challenges and opportunities surrounding our judicial system. In sum, this paper will show how the AI will be a *deus ex machina* in rendering verdicts normally necessitating the personal and unprejudiced assessment of a Filipino magistrate.

To achieve the goals of this paper, it is important to streamline the sub-topics to be discussed hereinafter.

First, I will introduce how AI works. From the basics involving the type of modeling used, the factors considered in achieving the desired output, and up to the expected infallibility and reliability of its *ex ante* outcome predictions. *Second*, I will make a review on the use of AI in many judicial settings, scrounging from practices of an existing international tribunal and various national and local courts. *Third*, I will attempt to scrutinize and view the use of AI under the lens of our Philippine Constitution, the Rules of Court, and judicial canon. *Fourth*, I will attempt to theorize the feasibility of using AI in coming up with court decisions in general and in the Philippine backdrop in particular. *Fifth*, I will conclude by making a recommendation on the use of AI in the Philippine judiciary as a means moving forward.

II. UNDERSTANDING THE "INTELLIGENCE" OF AI

A. *The Nature and the Factors (Vs of Big Data)*

At the expense of being repetitive, AI's influence in the modern-day world would become increasingly more significant. From the most minute to some of the major aspects of life, AI will continue if not permanently pervade in the foreseeable future, inescapably changing the landscape of how things are to be done and even how lives are to be run. The judicial systems are no exceptions.

Some legal experts in the field of information technology see the use of AI as beneficial and necessary in the practice of law. AI already

touched many areas of law, including contract analysis, legal research, e-discovery, etc.[1] But how does AI work?

AI can be defined as "making a machine behave in ways that would be called intelligent if a human were so behaving."[2] It also refers to the "theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."[3]

When taken in the context of the judiciary whereby the AI would either assist or supplant judges and justices in crafting the bases of their judgments, it will involve machine learning wherein computer programs "learn" from experience and improve their performance over time."[4] To data specialists, the process of machine learning will require the AI to be highly dependent on the four main Vs of Big Data (Volume, Variety, Velocity, and Veracity). These factors admittedly serve as the cornerstones of data-driven projects.[5]

The first consideration is the concept of *Volume*. Any data-driven AI programs foremost require access to data. Machine learning models, which are based on probabilistic inferences, are data-hungry. The larger the same data, the more accurate the model's predictive value.[6]

Second is *Variety*. In data-research terminology, variety of data refers to the fact that data comes from different sources and may be structured (*i.e.* a file containing names, phone numbers, addresses) or unstructured (*i.e.* photos, videos, social media feeds).[7] Viewed from the perspective of judicial decision-making processes, the variety aspect will

---

1 Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* (2d ed., Oxford University Press 2017); *Philip Hanke, Computers with Law Degrees? The Role of Artificial Intelligence in Transnational Dispute Resolution, and Its Implications of the Legal Profession*, 14(2) Transnational Dispute Management 1 (2017).

2 John McCarthy et al., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence* (31 Aug. 1955).

3 Oxford Living Dictionaries, <https://en.oxforddictionaries.com/definition/artificial_intelligence> (visited 01 December 2022).

4 Rusell & Norvig, *Artificial Intelligence: A Modern Approach* at 693 (3d ed., Pearson 2010).

5 Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 Washington University Law Review, 859, 867 (2016); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 Pepp. Law Review 773, 795 (2015).

6 Maxi Scherer, *Artificial Intelligence and Legal Decision-Making: The Wide Open? A Study Examining International Arbitration*, Journal of Arbitration 36, no. 5 (2019): 539-574.

7 Lieke Jetten & Stephen Sharon, *Selected Issues Concerning the Ethical Use of Big Data Health Analytics*, 71 Washington & Lee Law Review Online 486, 487 (2016): Uthayasankar Sivarajah, et al., *Critical Analysis of Big Data Challenges and Analytical Methods*, 70 J. Business Research 263, 269 (2017).

not rely on the varying structures or sources of data since what will be at the crux of the AI's learning phase are the contents of past judgments inputted into a database. Extrapolating on consistent sequences and legal tessellations, the AI will require cyclic patterns.

Another factor is *Velocity*. This refers to the regularity and iteration of incoming data, which the machine learning model must process and regurgitate through time. It involves the frequency and speed of data being generated and how the data is stored, managed, or moved.

Last among the factors is *Veracity*, which relates to the accuracy and trustworthiness of the data and information assets used. In AI jargon, veracity would require high veracity data to be analyzed in order to generate an outcome that is crucial to coming up with meaningful results.

To engage in vivid imagery, all these four (4) factors would serve as the "village" responsible for raising the AI. Stated differently, it can be said that AI is like an animal reared and taught through cognitivism, constructivism, and connectivism. Though without corporeal and mental faculties compared to human beings, AI is expected to have "(t)he ability to learn, understand, and make judgments or have opinions that are based on reason."[8] While AI is a non-life, it will have "(t)his ability (that) distinguishes human beings from other forms of non-intelligent or less intelligent life.[9]

B. *The Ex Ante Outcome Prediction (Infallibility and Reliability of Court Decisions)*

While the legal profession is a field very much open to modernization and improvement in the ways justice is made accessible to everyone, many are still adamant about AI-driven programs having the capacity to *ex ante* predict the outcome of court decisions. For some, the projections are counter-intuitive bordering to being capricious.

Many lawyers instinctively believe that legal decision-making requires cognitive process- such as understanding the parties' legal submissions and determining the right outcome through reasoning- which cannot be achieved by computer programs.[10]

---

8 Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/intelligence> (visited 01 December 2022).

9 Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence*, 24 et seq. (Knopf 2017).

10 Scherer, *supra* note 6.

However, many authors claim that computer models are now able to achieve "intelligent" results, which, if performed by humans, are believed to require high-level cognitive processes.[11] Several studies may lend support to the thesis that computer programs are better than humans in predicting the outcome of legal decision-making.[12] The basic explanation for this AI-success- apparently triumphant- is that human brains suffer "hardware" limitations which computer programs surpass easily.[13] In fact, in the coming years, it is expected that computers available at the consumer level will reach storage capacity of several petabytes. Fifty petabytes are sufficient to store information content of the "entire written works of mankind from the beginning of recorded history in all languages."[14] Accordingly, computers can simply stock amounts of data and draw from that data or experience much more quickly and efficiently than humans ever will.[15]

Furthermore, several other assumptions arise in the use of AI in court decision-making.

First, AI models have the advantage of algorithmic objectivity and infallibility over humans who inevitably make mistakes and are influenced by subjective, non-rational factors. Research in the area of psychology, cognitive science, and economy have shown that humans often fail to act rationally.[16] AI-based decision-making is alleged to be superior to human decision-making on the basis that computers would be immune to cognitive biases or undue influence of extraneous factors.[17] In connection to this, Nobel-prize winner Daniel Kahneman and Amos Tversky have studied heuristics and cognitive biases in human choices. Their studies provide multiple examples in which heuristics (*i.e.* cognitive short-cuts for otherwise intractable problems) and biases (*i.e.* factors which appear to be irrelevant to the merit of our choices but affect them nonetheless) appear in human day-to-day decisions.[18]

---

11 Scherer, *supra* note 6.

12 For some of the earlier studies, see Roger Guimerà and Marta Sales-Pardo, *Justice Blocks and Predicitability of U.S. Supreme Court Votes,* 6(11) PloS One (2011); Andrew D. Martin et al., Competing Approaches to Predicting Supreme Court Decision Making, 2(4) Persp. Pol. 761 (2004); Philip E. Tetlock, *Expert Political Judgment: How Good Is it? How Can We Know?* (Princeton University Press 2005).

13 Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence*, 27-28 et seq. (Knopf 2017).

14 Daniel M. Katz, *Quantitative Legal Prediction*, 62 Emory L.J. 909, 917 (2013).

15 *Ibid.*

16 Christine Jolls, Cass Sunstein & Richard Thaler, *A Behavioral Approach to Law and Economic*, 50 Stanford Law Review 1471 (1998); Avishalom Tor, *The Methodology of the Behavioral Analysis of Law*, 4 Haifa Law Review 237 (2008).

17 Philip Hanke, *Computers with Law Degrees? The Role of Artificial Intelligence in Transnational Dispute Resolution, and Its Implications of the Legal Profession*, 14(2) Transnat'l Disp. Mgmt.1 2017).

18 Daniel Kahneman & Amos Tversky, *Subjective Probability: A Judgment of Representativeness*, 3 Cognitive Psychology 430, 431 (1972); Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, 185 Science 1124 (1974).

Second, the use of AI will rule out the subjectivity aspect in the decision-making process, which is more in keeping with the legal formalism school of thought. In its purest form, legal formalism posits that law is, and should be, an entirely self-contained system, in which judges never face choices or questions of interpretation that would be resolvable through extra-legal considerations.[19] A judicial decision is thus the product of a seemingly mechanical or mathematical application of pre-established legal principles or rules to proven facts using means of logic.[20] The underlying idea can be expressed in the simple formula "R + F = C" or "rule plus facts yields conclusion."[21]

Hence, court decisions drafted and promulgated with the aid of AI are argued to be prejudice-free, able to distill confounding facts and complicated laws. These assumptions must not, however, be approached with a simplistic attitude. As will be further discussed hereunder, several other key points need to be considered in objectively concluding that the *ex ante* prediction outcomes of AI-based decisions are indeed infallible and reliable.

III. AI AND ITS UTILIZATION IN MODERN JUDICIAL SYSTEMS

A. *The European Court of Human Rights ("ECtHR")*

In international arbitration and adjudication, the use of AI has been used for a wide variety of tasks, including legal research, drafting and proof-reading of written submissions, translation of documents, case management and document organization, hearing arrangements (such as transcripts or simultaneous foreign language interpretation), and drafting of standard sections of awards (such as procedural history).[22]

In 2016, a study conducted by a group of researchers focused on decisions by the ECtHR rendered in English language about three provisions of the European Convention on Human Rights, namely Article 3 on the prohibition of torture, Article 6 on the right to a fair trial, and Article 8 on the right to respect for private and family life. These provisions were chosen because they represent the highest number of decisions under the Convention and thus sufficient data on which base to study.[23] The study

---

19 Hans Kelsen, *reine Rechtslehre* 478 (2nd edition, Deuticke 1960).

20 Marie-France Renoux-Zagame, *La figure du juge chez Domat*, 39 Droits 35 (2004).

21 Neil MacCormick, *Legal Reasoning and Legal Theory x* (Oxford Clarendon 1977).

22 Kate Apostolova & Mike Kung, *Don't Fear AI in IA*, Global Arb. Rev. (27 April 2018).

23 Nikolaos Aletras, et al, *Predicting Judicial Decisions of the European Court of Human Rights: A Natural Language Processing Perspective*, PerJ Computer Science 2:e93 (2016).

selected an equal number of decisions in which the ECtHR found a violation or none of the Convention.

The methodology used in the study focused on the textual information contained in the decisions, using natural language processing and machine learning. The study input was the text found in the decisions, following the usual structure of decisions of the ECtHR including sections on the procedure, factual background, and legal arguments. Not included in the input were the operative sections of the decisions where the ECtHR announces the outcome of the case. The output target was a binary classification task as to whether the ECtHR found a violation of the underlying provision of the Convention. The model was trained and tested on a 10% subset of the dataset.[24]

As a result, the model obtained an overall accuracy to predict the outcome of the ECtHR's decision in 79% of all cases. The decision sections with the best predictive value were those setting out the factual circumstances and procedural background (76% and 73% respectively), whereas the legal reasoning section had a lesser outcome prediction value (62%). The study also set out the most frequently used words for various topics, indicating their relative predictive weight for a violation or non-violation. For example, under Article 3, the most frequently used words with a high prediction value are "injury", "damage", "Ukraine", "course", "region", "effective", "prison", "ill treatment", "force", "beaten".[25]

The authors claim that their work may lead the way to predicting *ex ante* the outcome of future ECtHR cases based on a text-based approach.[26] The authors likewise confirm the legal realist theories that judges are primarily responsive to non-legal, rather than to legal, reasons when deciding cases. They conclude that the information regarding the factual background of the case as this is formulated by the Court in the relevant subsections of its judgment is the most important part obtaining on average the strongest predictive performance of the ECtHR's decision outcome and thus suggest that the rather robust correlation between the outcomes of cases and the text corresponding to fact patterns coheres well with other empirical work on judicial decision-making in hard cases and backs basic legal realist intuitions.[27]

---

24 *Ibid.*

25 Nikolaos Aletras, et al, *Predicting Judicial Decisions of the European Court of Human Rights: A Natural Language Processing Perspective*, PerJ Computer Science 2:e93 (2016).

26 *Ibid.*

27 *Ibid.*

However, the study pronounced two limitations. *First*, it included the ECtHR's legal reasoning thus making the overall prediction results all but surprising. The inclusion of the ECtHR's legal reasoning significantly undermined the study's claim to lead the way towards possible *ex ante* outcome prediction. *Second*, the formulation by the ECtHR of the factual background may have provided hints of the outcome as they were tailor-made to fit a specific preferred outcome. Without suggesting bias or partiality, the facts described in the decisions may be a selection of those facts that will be relevant to the decision's legal reasoning and outcome, leaving aside other non-pertinent facts pleaded by the parties.[28]

B. *The United States of America ("US")*

In 2017, a group of researchers focused on the prediction of US Supreme Court decisions. It was viewed as innovative because the goal was to obtain a model that would generally and consistently be applicable to all US Supreme Court decisions over time, not only in a given year or for a given composition of the Court with justices. Of course, it applied the principle that all information required for the model to produce an estimate should be knowable prior to the date of the decision.[29]

For its scope of the study, it sifted through US Supreme Court decisions from almost two centuries, from 1816 to 2015. This resulted in input data of more than 28,000 case outcomes and more than 240,000 individual justices' votes. Rather than merely relying on textual information contained in the decisions, as was the case for ECtHR decisions, this study labelled the data using certain features such as identity of the parties, the issues at stake or the timing of the decision to be rendered, the information from the lower court's decisions, and the composition of the Supreme Court like the identity of the justices, their previous rate of reversal votes or dissents, as well as their political preferences.[30]

Overall, the model predicted the votes of individual justices with 71.9% accuracy, and the outcome of the decisions with 70% accuracy.[31]

Like the ECtHR study, it had its own inherent limitations. All information required for the model to produce an estimate should be knowable prior to the date of the decision, some of the input data features

---

28 *Ibid.*

29 Daniel M. Katz, Michael Bommarito II & Josh Blackman*, A General Approach for Predicting the Behavior of the Supreme Court of the United States*, 12(4) PloS one (2017), pages 2-3.

30 *Ibid.*

31 *Ibid.*

are available only shortly before the decision is rendered, like late stage oral arguments set. Also, it concerned cases on appeal and not cases of original jurisdiction. Finally, it conceded to the idea that Supreme Court decisions are often highly political. Hence, decisions are influenced by the political spectrum one comes from, particularly the possibility of gun control being one example.[32]

C. *The People's Republic of China ("PRC")*

The use of AI in the PRC is not novel. It has been employed in "Smart Courts" and internet courts, gradually forming a new trial mode in which Chinese courts extensively use electronic case files, websites for disclosing case information, modern case handling and management platforms, and similar case pushing and evidence review systems.[33]

In terms of in-depth case analysis and auxiliary judgment, the "wise Judge" system of Beijing Court can automatically sort out the facts to be tried before the trial, generate the trial outline, and push it to the trial system. The biggest highlight of the Shanghai "206 system" is the evidence standard and evidence rule guidance function, which realizes the intelligent examination of evidence data and provides standardized guidance for case handling personnel. In addition, the "AI judge" launched by Ali Co. Ltd. has established a complete set of trial knowledge atlas for transaction dispute cases, which can quickly analyze the case and make recommendations to judges within a short period.[34]

IV. AI AND THE PHILIPPINE JUDICIAL SYSTEM

A. The legality of the Philippine judges and justices' use of AI in their judgments

On 03 March 2022, Chief Justice Alexander G. Gesmundo of the Supreme Court of the Philippines revealed during a virtual meeting with the Joint Foreign Chambers (JFC) of the Philippines that "(t)he Supreme Court is looking to use artificial intelligence (AI) to improve operations in the Judiciary as part of its drive to unclog court dockets and expedite decisions."[35] Earlier Supreme Court initiatives have seen the power of AI in

---

32 *Ibid.*

33 Zichun Xu, *Human Judges in the Era of Artificial Intelligence: Challenges and Opportunities*, Applied Artificial Intelligence, (2022) 36:1, 2013652, DOI:10.1080/08839514.2021.2013652.

34 Chen., M., and H. Xiao, *The Provincial Higher People's Court held a symposium on the review of standardized sentencing intelligent auxiliary systems*, (2017) Hainan Legal Times, published on 2017- 12-8.

35 Supreme Court of the Philippines, <https://sc.judiciary.gov.ph/25055/> (visited 01 December 2022).

the conduct of videoconferencing hearings, with AI-enabled voice to text transcription application allowing real-time access to transcripts of court proceedings. Building on these developments, the Supreme Court, through its Strategic Plan for Judiciary Innovations (SPJI) 2022-2026, envisions the use of AI-enabled legal research tools and "to capitalize artificial intelligence (AI) to improve court operations, such as the use of technology in preparing transcripts of stenographic notes and in digitalizing judgments rendered."[36]

Other than these intended short-term and long-term plans, the use of AI in deriving at actual court decisions is yet to merit ruminations at the discussion table. For many quarters, AI superseding judges and justices in matters requiring the use of conventional human knowledge and wisdom may pose some legal obstacles under the present Constitutional and legal frameworks in the Philippines.

The parameters by which Philippine justices and judges are to be guided in rendering decisions is enunciated under the 1987 Philippine Constitution, particularly in Article VIII, Section 14 thereof, *viz*:

> xxx. No decision shall be rendered by any court without expressing therein clearly and distinctly the facts and the law on which it is based.

While the 1987 Philippine Constitution does not require that the judge or justice promulgating the decision should personally examine the facts and apply the pertinent laws to the case, the Supreme Court through the Rules of Court offer a slightly different take. Both the 2019 Amendments to the 1997 Rules of Civil Procedure ("2019 Amended Civil Procedure") as well as the 2000 Revised Rules on Criminal Procedure ("2000 Revised Criminal Procedure"), require justices and judges to make personal assessment and preparation of the decision.

Rule 36, Section 1 of the 2019 Amended Civil Procedure provides:

> xxx *Rendition of judgments and final orders.* - A judgment or final order determining the merits of the case shall be in writing **personally and directly prepared by the judge, stating clearly and distinctly the facts and the law on which it is based**, signed by him, and filed with the clerk of the court." (boldface supplied)

---

[36] *Id.*

In a similarly couched version, Rule 120, Section 1 of the 2000 Revised Criminal Procedure states that:

> xxx *Judgment definition and form*. — Judgment is the adjudication by the court that the accused is guilty or not guilty of the offense charged and the imposition on him of the proper penalty and civil liability, if any. It must be written in the official language, **personally and directly prepared by the judge and signed by him and shall contain clearly and distinctly a statement of the facts and the law upon which it is based.** (boldface supplied)

Aside from the 1987 Philippine Constitution and the Rules of Court, the concern on the use of AI in replacing the required astuteness of judges and justices in demonstrating the reasons and concluding decisions is specifically addressed under Canon 3, Rule 3.02 of the Code of Judicial Conduct, *viz*:

> xxx- In every case, **a judge shall endeavor diligently to ascertain the facts and the applicable law** unswayed by partisan interests, public opinion or fear of criticism. (boldface supplied)

With the foregoing legal considerations in mind, noting the fundamental tenet that the Rules of Court may well be amended by the Supreme Court pursuant to its rule-making power under Article VIII, Section 5(5) of the 1987 Constitution, there is no legal barrier for the use of AI in decision-making processes in the country. The Supreme Court may premise the AI's introduction in the field of decision-making, albeit involving limited kinds of cases at its inception, as a workable solution to making the disposition of court actions noticeably speedier, inexpensive, and just, thus precluding unintentional or intentional delays in the administration of justice. With the employment of AI in court decisions, the Supreme Court may achieve its desire of decongesting the lower and ppellate courts of cases by "exploring the collective life experience and overall rationality of judges, and avoid the uncertainty risk brought by judges' individual discretion."[37] The AI's introduction in court-decision may be a good follow-up to the Supreme Court's SPJI 2022-2026.

---

[37] Jenkins, J., *What can information technology do for law?*, Harvard Journal of Law & Technology 21 (2):589–607.

B. The feasibility of the use of AI in court-decisions in general

Conceding that nothing might serve to legally hinder the exploitation of AI's potentials in augmenting courts in their decision-making tasks, it will only be a matter of time before AI finds its essential niche in the Philippine judicial system. Two curious questions, however, crop up. Will it be the case of the dog wagging its tail or the tail wagging the dog? Will the eventual "subservience" of justices and judges to the formidable algorithms and calculations of AI assuage the dilemma of judicial efficiency or will its downsides outweigh the good that it brings?

Many technology experts say that the robustness and trustworthiness of AI are recurrent topics in the discussion on AI.[38] It is both a course of action and a medium susceptible of becoming a double-edged sword.

Some risk-averse lawyers and scholars opine that AI programs will have significant issues in providing reasoned legal decisions and meeting those rationales. They argue that one advantage of human courts, for fragile reasons, is related to procedural fairness. Between a decision delivered via software and court adjudication, human courts may yield deeper acceptance and greater public satisfaction even if they deliver the same results.[39] In the future, the very fact of human decision- especially when the stakes are high- may become a mark of fairness.[40] Whilst resigning to the thought that AI is inevitable in the future,[41] many scholars express skepticism mainly on the assumption that some "human factor" would be necessary to ensure sympathy and emotional justice.[42]

Anent the Four Vs of Big Data, several challenges are presented in holding that AI is a viable answer to the growing demands of court litigation.

On the factor concerning *Volume*, a manifest limitation may be two-fold. *First*, case data may not always be accessible because in certain

---

38 See *i.e.* European Commission Press Release, Artificial Intelligence: Commission Tasks Forward Its Work on Ethics Guidelines (8 April 2019).

39 E. Allan Lind & Tom R. Tyler, *The Social Psychology of Procedural Justice* (Melvin J. Lerner ed., 1988).

40 Aziz. Huq, *A Right to a Human Decision*, 105 Vancouver Law Review (2020).

41 Apostolova, et al, *supra* note 22.

42 Francisco Uribarri Soares, *New Technologies and Arbitration: Traditional Conceptions and Innovative Trens, In International Arbitration: The Coming of a New Age?* ICCA Congress Series 17, 654-67 (Albert Jan van den Berd ed., Wolters Kluwer 2013).

areas of the law, decisions are confidential and are not available to non-parties (*i.e.* family court cases). *Second*, when case data is accessible, a large sample size is important. While there is no hard rule of a required sample size, the more data, the more accurate the extracted model is. Accordingly, areas of law with large numbers of decisions on a given topic will be more suitable for AI models.[43] Contrariwise, areas of law that are not yet brimming with jurisprudence or are fairly new (*i.e.* cyber-offense cases) would meet challenges in terms of volume.

For *Variety* challenges, AI-driven decision-making produce two critical questions. *First,* a limitation is seen on whether the extent an AI-based decision-making model would require repetitive fact patterns or, conversely, whether it would be able to deal with topics that are complex and non-repetitive. The more outliers or non-repetitive issues, the more difficulties the AI model will face. *Second*, the model output. The legal prediction studies in ECtHR and US Supreme Court use binary classification as the output task (violation or no violation). This raises a question whether those, or other similar models, could be built for more diverse, non-binary tasks. Others may be tempted to say that any legal decision could be further subdivided into a multitude of binary classification tasks, such as whether it has jurisdiction (yes/no), a contract was validly entered into (yes/no), the contact was breached (yes/no), then you factor into which side has the burden of proof and if it miserably fails to discharge it then assign as 1 or 0.[44] The difficulty arises since every case proffers hordes of binary tasks, and resolving each case would be case-specific.

Velocity would not be experiencing much predicament since the problem largely lies not on the sheer volume and wealth of data coming in but, on the unavailability, and consistency thereof. Another concern is the quick policy turnovers and jurisprudence changes over time, which might leave the already abundant information assets and stored data irrelevant let alone without legal worth. In several areas of the law, involving constitutional law for example, policy changes seem malleable and unpredictable, thus making it difficult for the AI models to keep up with the constantly-evolving legal precepts. AI, being a trained creature reliant on extant data, its likely refuge is to maintain *status quo* in accordance with past and established jurisprudential precedents.

---

43 Scherer, *supra* note 6.

44 Scherer, *supra* note 6.

On the *Veracity* aspect, AI research shows recently the risks of misbehaving or biased algorithms with computer systems used for a variety of tasks such a flight listings, credit scores, or online advertisements.[45] Some argue that hidden and unregulated algorithms produce authoritative scores for individuals that mediate access to opportunities.[46] Hence, vulnerability in the data diet has negative consequences on the extracted model. For example, the underlying data which was used to train the algorithm might have been "infected" with human biases. The model might extract patterns from the data and infer them in a way that might lead to systemic mistakes.[47] Studies in the US have shown that the use of algorithms in criminal risk assessment has led to racially biased outcomes.[48] This is based on the Correctional Offended Management Profiling for Alternative Sanctions ("COMPAS") system that is used in the US to assess the recidivism risks for defendants. Studies found that black defendants were twice as likely as white defendants to be misclassified as a higher risk of violent recidivism whereas white violent recidivists were 63% more likely to have been misclassified as a low risk of violent recidivism, compared with black violent recidivists.[49] Like in the ECtHR, words with higher predictive value include "Ukraine" or "Russian."[50]

In spite of these challenges and foreseen susceptibilities in the use of AI, computer savvy individuals with appetites for AI's limitless possibilities argue that software systems aiming to replace systems of social ordering will succeed best as human-machine hybrids, mixing scale and efficacy with human adjudication for hard cases. They will be, an older argot, "cyborg" systems of social ordering.[51] Hence, what is best would be an interdependence between humans and computers in deciding court cases.

---

45 Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, 14 ACM Transactions on Information Systems 330 (1996).

46 Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Washington Law Review, 1 (2014).

47 Scherer, *supra* note 6.

48 Julia Angwin et al, *Machine Bias: There's Software Used Across the Country to Predict Future Criminal. And It's Biased Against Balcks*, ProPublica (23 May 2016) < https://www.propublica.org /article/machine-bias-risk-assessments-in-criminal-sentencing> (visited 01 December 2022); Jeff Larson et al., *How We Analyzed the COMPAS Recidivism Algorithm*, Pro Publica (23 May 2016), < https://www.propublica,.org/article/how-we-analyzed-the-compas-recidivism-algorithm > (last accessed on 01 December 2022).

49 Jeff Larson et al., How We Analyzed the COMPAS Recidivism Algorithm, Pro Publica (23 May 2016), <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (visited 01 December 2022).

50 Aletras, et al, *supra* note 23.

51 Tim Wu, *Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-Ordering Systems*, Columbia Law Review 2002 (2019).

C. The feasibility of the Philippine judges and justices' use of AI in their judgments

The Philippine judicial system has its own unique sets of needs and restrictions, which AI-driven programs designed to help draft decisions must work its way around. For a more in-depth appreciation of how AI can assimilate itself in the Philippine judiciary, a look into the present standpoint of the Philippine courts is a must.

According to a Summary of Cases received by this author from the Court Management Office of the Office of the Court Administrator, Supreme Court of the Philippines, there were about 417,953 pending cases in the second level courts (Regional Trial Courts and Sharia District Courts) and 188,485 pending cases in the first level courts (Metropolitan Trial Courts, Municipal Trial Courts, Municipal Trial Courts in Cities, Municipal Circuit Trial Courts, and Sharia Circuit Courts) as of December 31, 2021. By the end of September 2022, the statistics improved with 405,854 active cases in the second level courts and 187,224 active cases in the first level courts. The disposition rate according to the same Summary of Cases is 28% and 48%, respectively.

With how cases are managed and disposed at the current rate, it begs the question whether AI will succeed in hastening court process, particularly in the quickness of rendering decisions. Having already established the perceived intrinsic drawbacks on the use of AI in decision-making, a succinct review of its benefits vis-à-vis its tenability in the Philippine setting, factoring in the challenges and recent breakthroughs abounding the present judicial system, is in order.

1. Small Claims Cases

With the fairly recent introduction of the Rules on Expedited Procedures in the First Level Courts (A.M. No. 08-8-7-SC) ("Expedited Procedures"), filing of Small Claims cases had been made easier, simpler, and more accessible to the general public. Even the decision-writing phase was made faster since the Expedited Procedures appended a suggested format for court decisions (Form 11-SCC). The judge merely needs to tick the boxes for the antecedents and the facts at hand, and elucidate only on the *ratio decidendi* and the dispositive portion.

This well-developed set of rules applicable to sums of money arising out of contracts of lease, loan and other credit accommodations, services, sales of personal property, and enforcement of barangay amicable settlement agreements and arbitration awards, where the money claim does not exceed One Million Pesos (PhP 1,000,000.00), may well be the springboard for the use of AI in decision-making processes in the future.

As a starter, the modelling used in the ECtHR and that of the PRC can serve as inspirations for Small Claims cases because they operate on a text-based approach. Moreover, AI-programmers would not have to overcome difficulties in training the computer machine as laws[52] and jurisprudence[53] on contracts of *mutuum* are rationally stable over the years. Laws[54] and cases[55] on the enforcement of barangay amicable settlement agreements have not also seen major fluctuations in policy, thus ripe for test cases in the application of AI.

2. Ejectment Cases

Land dispute actions that are summary in nature[56] are very suitable inclusions to the battery of cases likely to be made subject of AI. Cases such as forcible entry or unlawful detainer are replete with data to be culled from first level courts, the same having been exclusively under these courts' jurisdiction since 1991 pursuant to the 1991 Revised Rule on Summary Procedure. Hence, volume is likely not to cause any concern.

The other Vs of Big Data would not meet significant difficulties as well because the velocity and variety factors are covered by established jurisprudence[57] that have not been overthrown nor revised for several years now. Veracity is also not a grave concern because data are not vulnerable to being "infected" with human biases since the determination of the existence or non-existence of jurisdictional facts[58] for ejectment cases are most of the time based on documentary evidence.

---

52 Articles 1933 and 1953 of the New Civil Code of the Philippines

53 *Lara's Gifts & Decors, Inc. v. Midtown Industrial Sales, Inc.,* G.R. No. 225433, August 28, 2019; *Pineda v. Vda. de Vega*, G.R. No. 233774, April 10, 2019.

54 Sections 416 and 418 of Republic Act 7160 (Local Government Code of 1991); *see also* The Katarungang Pambarangay Implementing Rules and Regulations issued by the Department of Interior and Local Government (DILG).

55 *Republic v. Sandiganbayan*, (G.R. No.108292, September 10, 1993); *Sebastian v. Ng*, (G.R. No. 164594, April 22, 2015); *Vidal v. Escueta*, (G.R. No. 156228, December 10, 2003).

56 Rule 70 of the 1997 Rules of Civil Procedure.

57 *Cruz v. Spouses Christensen*, (G.R. No. 205539, October 04, 2017); *Zaragoza v. Iloilo Santos Truckers, Inc.*, (G.R. No. 224022, June 28, 2017); *Quijano v. Atty. Amante*, (G.R. No. 164277, October 08, 2014); *Javelosa v. Tapus*, (G.R. No. 204361, July 4, 2018).

58 *Hidalgo v. Velasco*, (G.R. NO. 202217, April 25, 2018).

3. Drugs Cases

Even before the advent and enactment of Republic Act 9165 (Comprehensive Dangerous Drugs Act of 2002), Regional Trial Courts have been congested with drug-related cases, thus frittering away human resources on legal research and writing of court-decisions. In more recent years, the apprehension, prosecution, and punishment of drug criminals have become a matter of national interest and public involvement. Owing to the Philippine law enforcement authorities' intensified campaign against illegal drugs based largely on the marching orders of then President Rodrigo R. Duterte, second level courts in the country have seen a sharp ascent of court cases filed and are now embattled in managing the influx and demands of drug-linked charges.

Perhaps, more controversially, this author argues that drugs cases are appropriate for AI-driven programs in order to hasten their disposals. This contention is anchored on two reasons.

First, the Supreme Court's interpretation of Republic Act 9165's Section 5 (Sale, Trading, Administration, Dispensation, Delivery, Distribution and Transportation of Dangerous Drugs and/or Controlled Precursors and Essential Chemicals), Section 11 (Possession of Dangerous Drugs), Section 12 (Possession of Equipment, Instrument, Apparatus and Other Paraphernalia for Dangerous Drugs), and Section 15 (Use of Dangerous Drugs), have been steady for many years now. Relevant jurisprudence on the matter, such as *Dela Riva v. People*,[59] *People v. Lim*,[60] *Plan, et al. v. People*,[61] and *People v. Rivera*,[62] collectively provide a rich and uniform understanding as to how the aforesaid Sections should be dealt with in criminal proceedings.

Second, taking after the modelling and legal prediction studies involving the US Supreme Court and the ECtHR, Philippine drug cases may use binary classification as the output task to determine the commission or non-commission of the relevant crimes under Republic Act 9165. The AI program may factor into recurring essential legal themes, such as the legality of arrest (yes/no), the performance of official duty (yes/no), the ill-

---

59 *Dela Riva v. People,* G.R. No. 212940, September 16, 2015.

60 *People v. Lim,* G.R. No. 231989, September 04, 2018.

61 *Plan v. People,* G.R. No. 247589, August 24, 2020.

62 *People v Rivera,* G.R. No. 252886, March 15, 2021.

motive of law enforcers (yes/no), the existence of planted evidence (yes/no), the physical inventory and photograph of seized items (yes/no), the presence of indispensable witnesses during the inventory and photograph sessions (yes/no), the unbroken chain of custody (specifically its four links) (yes/no), the precautionary steps taken by the forensic chemist (yes/no), and the integrity of *corpus delicti* (yes/no), *inter alia*. Since the *onus* of proving the crimes under Republic Act 9165 is always on the State, the binary classification shall assign the result as either 1 or 0.

4. Rape, Murder, and Allied Cases

The most challenging cases for AI-propelled computer programs would be those that require the personal assessment of judges on the demeanor and credibility of witnesses in court.

Cases in point are rape and murder charges where the credibility of private offended parties and their witnesses are measured by their categorical, straightforward, spontaneous, consistent, and frank manner[63] of narrating the material events. This is correlated to the deeply entrenched principle that "when the decision hinges on the credibility of witnesses and their respective testimonies, the trial court's observations and conclusions deserve great respect and are accorded finality, unless the records show facts or circumstances of material weight and substance that the lower court overlooked, misunderstood or misappreciated and which, if properly considered, would alter the result of the case."[64]

In this context, what the AI would not be able to usurp is the trial judge's advantage of observing the witness' deportment and manner of testifying, and ultimately determining if the witness is telling the truth, being in the ideal position to weigh conflicting testimonies.[65]

Until this legal teaching is effectively substituted by foolproof metrics and algorithms to be devised by technology doyens, this territory shall remain outside the reach of AI and will continue to be subject of the judges' personal reflections and deductions.

---

[63] *People v. Quinto*, G.R. No. 246460, June 08, 2020, *citing People v. Ponsara*, G.R. Nos. 139616-17, February 6, 2002.

[64] *People v. Rupal*, G.R. No. 222497, June 27, 2018, *citing People v. Gaa*, G.R. No. 212934, 7 June 2017.

[65] *People v. Bauit*, G.R. No. 223102, 14 February 2018.

D. CONCLUSION AND RECOMMENDATION

AI becoming the judiciary's *deus ex machina* is not just, figuratively speaking, a divine being descending from a machine, but also a state of eureka where one comes to a realization that overwhelming difficult situations are not to be fled from, but rather embraced with an open mind and an adaptable spirit. Truth be told, the demarcating line defining the capabilities of humans and computers is slowly coming to a haze, with technology catching up and in a very rapid pace. The emergence of AI, like a hero startlingly emerging from the trapdoor on the floor, is a call to ride the ebbs and tides of time. Though cognizant of some ethical and philosophical issues that would call into question the propriety of using AI in court decision-making processes, the promises the AI bring are far-reaching for those who dream of a better judicial system treading along science and negotiating forward with remarked adeptness and true fidelity to the cause of justice. With an end of achieving the judicious use of human assets, the confluence of science and labor in maximizing proficient court operations would be a necessity rather than a taboo.

Looking ahead, the author suggests a general course of action to realize, to the fullest extent possible, the benefits of AI in the Philippine judicial system. Without maintaining a blind deferential attitude towards AI, those at the helm of the judiciary must explore and carefully study its use in the decision-making of judges and justices. Of course, sufficient safeguards for its reliability and trustworthiness must be endeavored to be incorporated.

With the complexities of judicial activities, it is safe to say that the AI managing to fully replace a judge or justice sooner than later is a very remote idea. Nonetheless, the marriage of the boundless capabilities of AI and the humanization of laws by humans would be the most pragmatic solution in coming up with fast yet reasoned and well-informed court judgments.

10

Waking the Digital Leviathans

by Jarre V. Gromea

WAKING THE DIGITAL LEVIATHANS

Jarre V. Gromea[*]

I. INTRODUCTION

The Leviathan, in mythology, is a gargantuan sea serpent. Its gaping maw represents the pits of hell. The impenetrable scales signify its indomitable nature that humankind cannot overcome. It is a monster that embodies chaos.[1]

But for political philosopher Thomas Hobbes, the term '*Leviathan*' connotes to an artificial being created by humans for their protection. This being is the State.[2] Its artificial soul is the sovereignty vested unto it by a social contract. The individual gives up the authority to govern oneself in exchange for peace and protection. It is therefore the consent of the governed which wakes the leviathan. Now we have not one but several leviathans—several sovereign states.

However, recent advances in technology and information processing gave birth to the digital world. A new species has awoken. Digital leviathans rule this new world, each sovereign in their own platforms.

This paper aims to examine, explore, and resolve the legal issues involved in rousing these digital leviathans. It will include discussions on online platforms, user consent, data privacy, algorithms, and accountability.

II. THE RISE OF ONLINE PLATFORMS AND ITS IMPACT TO FILIPINO USERS

The term "online platform" is used to describe a range of services available on the Internet. But what exactly is an online platform? The Organization for Economic Co-operation and Development ("OECD") defines an online platform as a digital service that facilitates interactions between two or more distinct but interdependent sets of users who interact through the service via the Internet. [3]

---

* JD4 Student, University of St. La Salle – College of Law (2022).

1 Timothy Beal, *Religion and Its Monsters*, Routledge New York, 2002, p. 50.

2 Hobbes, Thomas, and Gaskin J C A., *Leviathan* (2008).

3 OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, 13 May 2022.

Online platforms have gained popularity over the past few decades following the creation of the World Wide Web in the late 1980s. Improvements in speed and accessibility increased the number of users on a staggering scale. Data from the International Telecommunication Union (ITU), UN's specialized agency for information and communication technologies, shows that about 4.9 billion people are using the internet as of 2021.[4] This means 63 percent of the world's population is now online.

Worldwide, the Philippines ranked as the top country whose citizens spend the most time online[5] from 2015 to 2021. Filipinos spend an average of 10 hours and 56 minutes on the internet daily. From this, we can infer that Filipino users are most likely to be exposed to and influenced by online platform content.

The term "pinoy-baiting" surfaced in 2021 which describes the act of satisfying the Filipino's unquenching thirst for online validation. One article describes it as a "misplaced search for relevance."[6] Another describes it as a digital form of cultural exploitation.[7] Foreign content creators take pieces of Filipino culture then sell these back to the Filipino people in exchange for clicks and views. The best example is Nas Academy's attempt to monetize Whang-Od's art of tattooing by offering paid courses online.[8]

This is but the tip of the iceberg. Beyond content creators, something sinister is lurking. Corporations behind online platforms also have their own agenda to earn profit from the data of its users.[9]

This interaction between online platforms and its users is parallel to the relationship between a State and its subjects. In the following chapter, the author will discuss the impetus of such relations.

---

4 ITU, *Measuring digital development Facts and figures 2021*, Geneva, Switzerland, 2021.

5 Cristina Eloisa Baclig, *Filipinos remain most active internet, social media users globally — study* PHIL. DAILY INQ., February 1, 2021.

6 Gideon Lasco, *Rethinking 'Pinoy Pride'* PHIL. DAILY INQ., July 9, 2021.

7 Anna Cristina Tuazon, *Baited, gaslighted, and exploited,* PHIL. DAILY INQ., August 11, 2021.

8 Vincent Cabreza, *NCIP finds Nas Daily deal with Whang-od 'onerous,* PHIL. DAILY INQ., August 31, 2021.

9 Marc Jones, *Big Tech data harvesting comes under fire by world central bank group,* Reuters, December 1, 2021.

III. DATA PRIVACY POLICIES AND CONSENT OF THE USER –'THE CONSENT TRAP'

When a user logs into an online platform for the first time, they are asked to create an account. The user is then asked to provide personal information. At the end of the registration process, the user is also required to tick a box and click the button signifying their consent to the data privacy policy of the online platform. This is a digital contract of adhesion.

In a contract of adhesion, one party imposes a ready-made contract to the other party whose sole participation is either to accept or reject the agreement.[10] The parties do not bargain on equal footing in the execution of this kind of contract given that the other party is limited "to take it or leave it" option[11] and there is no room for negotiation.[12] However, such contract is not entirely prohibited. The one adhering is free to give his consent inasmuch as he is also free to reject it completely.[13]

As applied to digital platforms, a contract of adhesion is a veritable trap for the weaker party whom the courts are bound to protect from abuse and imposition.[14] Hence, in case of doubt which will cause a great imbalance of rights, the contract shall be construed strictly against the party who prepared it.[15] This is pursuant to the mandate that in all contractual, property, or other relations, when one of the parties is at a disadvantage on account of his moral dependence, ignorance, indigence, mental weakness, tender age or other handicap, the courts must be vigilant for his protection.[16]

Consent is essential for the existence of a contract, and where it is wanting, the contract is void.[17] Consent in contracts presupposes the following requisites: (1) it should be intelligent or with an exact notion of the matter to which it refers; (2) it should be free; and (3) it should be spontaneous.[18] Intelligence in consent is vitiated by error; freedom is vitiated by violence, intimidation or undue influence; and spontaneity is

---

10 *Prudential Bank v. Alviar*, 502 Phil. 595, 610 (2005).

11 *Phil. National Bank v. The Hon. Court of Appeals*, G.R. No. 88880, April 30, 1991.

12 *RCPI v. Verchez,* 516 Phil. 725, 742 (2006).

13 *Norton Resources and Dev't. Corp. v. All Asia Bank Corp.,* 620 Phil. 381, 392 (2009).

14 *Quiambao v. China Banking Corporation,* G.R. No. 238462, 12 May 2021.

15 *Asiatrust Development Bank v. Tuble,* 691 Phil. 732, 745 (2012).

16 New Civil Code, Art. 24.

17 *Salonga v. Farrales*, et al., G.R. No. L-47088, 10 July 1981, 105 SCRA 359.

18 *Lim Jr. v. San*, 481 Phil. 421 (2004).

vitiated by fraud.[19] It is submitted that for a lot of users of online platforms, intelligence is vitiated because what the users erroneously agree to is not the collection and use of their data. Rather, they click agree to use the Service.

Beyond Philippine jurisprudence, consent is a sacred concept with a distinguished pedigree. It has been regarded as the foundation of political legitimacy. The idea of the state as a 'social contract' has been popular since the Enlightenment. More than a century ago, Samuel Warren and Louis Brandeis argued that every individual possesses a 'right to be let alone'[20] and over time, this evolved into a general assumption that individuals should be left to determine for themselves, 'when, how, and to what extent information about them is communicated to others.'[21]

Only one in a thousand people click to see an end-license agreement before purchasing software online.[22] On average, those who do look spend just fourteen seconds on documents that would need at least forty-five minutes for adequate comprehension.[23] As an example, Facebook's privacy policy is more difficult to read than Stephen Hawking's A Brief History of Time.[24]

Another reason why no one reads these data privacy policies is because the terms are so imprecise—*'we share your information with third parties'*—that they offer no meaningful indication of what the potential users are agreeing to.[25]

In the Philippines, the consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her.[26] The General Data Protection Regulation (GDPR) of the European Union (EU) lays down a more stringent standard in

---

19 New Civil Code, Art. 1305.

20 Samuel D. Warren and Louis D. Brandeis, *'The Right to Privacy',* Harvard Law Review, Vol. 4, No. 5 (1980), 193–220.

21 Christophe Lazaro and Daniel Le Métayer, *'Control over Personal Data: true Remedy or Fairy Tale?'* Scripted, Vol. 12, No. 1 (June 2015), 3–34.

22 Gillian K. Hadfield, *Rules for a Flat World: Why Humans Invented Law and How to Reinvent it for a Complex Global Economy,* Oxford University Press, Oxford, 2017, p. 170.

23 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, London, 2019, p. 237.

24 Kevin Litman-Navarro, '*We Read 150 Privacy Policies. They Were an Incomprehensible Disaster'*,The New York Times, 12 June 2019 <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html> (visited 16 December 2022).

25 Neil Richards and Woodrow Hartzog, *'The Pathologies of Digital Consent*', Washington University Law Review, Vol. 96 (2019).

26 R.A. 10173, *Data Privacy Act of 2012*, Sec. 3(a).

determining the existence of consent: "consent is any freely given, specific, informed and *unambiguous indication* of a data subject's wishes by which he or she, *by a statement or by clear affirmative action*, signifies agreement to the processing of personal data relating to him or her."[27]

Hence, for true consent to be valid in the context of using online platforms: (1) Users must have a clear choice without the influence of any coercion; (2) User consent must relate to specific actions involving their personal data and not for any other purpose; (3) Users must fully understand why the data is being collected and what it will be used for; (4) Lastly, the giving of consent must be a separate act and not a precondition to use a service or complete a transaction.

Where possible, individuals should be able to decide for themselves important matters about their lives. This respects their dignity and autonomy. But in the context of information technology, consent is often a trap masquerading as a safeguard. It does nothing to rebalance the relationship between consumers and powerful tech corporations. Instead, it entrenches the domination.

To demonstrate, the author attempted to open an account for TikTok. After downloading the app and running it, there was no link to any data privacy policy. It only displayed a screen which states, "By continuing, you agree to TikTok's Terms of Service and confirm that you have read TikTok's privacy policy." No other options were available except the big button with the word 'Next.' If this is the same experience for all Filipino users of TikTok, user consent is not only vitiated, genuine consent is impossible. What we have is a consent trap.[28]

IV. THE HIDDEN ALGORITHMS THAT SHAPE PUBLIC PERCEPTION – DIGITAL NUDGES AND SHOVES

Part of being free is being able to form our own preferences and act for our own reasons.[29] With the current state of our technology, smart-targeted ads unconsciously encourage to purchase or consume products, surrender time or attention, and offer up personal information. Digital

---

27 *The General Data Protection Regulation* (GDPR). 2018, Art. 4 par. 11, hereinafter [GDPR].

28 Sacha Molitorisz, *The Consent Trap*, Center for Media Transition, University of Technology Sydney, December 14, 2020.

29 Emily Bell, *'The Unintentional Press: How Technology Companies Fail as Publishers'*, in Lee C. Bollinger and Geoffrey R. Stone, The Free Speech Century, Oxford University Press, New York, 2019, p. 237.

leviathans change our behavior through 'conditioning' rather than reason or persuasion.[30]

Not all acts of conditioning are a threat to our fundamental freedoms. Netflix's algorithms do not pose a threat to our way of life. Nor does Spotify's music or podcast recommendations. But taken together, the nudges and demands on our attention may eventually result in a significant impairment of liberty.[31] Technology subtly degrades our ability to decide what we want and our will to pursue it.[32] It can operate beneath human consciousness in a manner closer to manipulation than influence.

The systems we build to gather, store, analyze, and communicate information are as fundamental to our shared existence as any economic, legal or political institutions.[33]

For example, the popular platform TikTok has over a billion users, many young adults and children. TikTok was not designed for a political purpose yet its sheer size and reach have made TikTok a potent social force. When users open the app, the first thing they see is the For You page, which promotes content likely to draw in users. This content is curated, partly by algorithms and partly by humans. In 2020, it emerged that TikTok's human curators had been instructed to block images of 'chubby' people and those with an 'abnormal body shape' from appearing on the For You page. Likewise, people with dwarfism and acromegaly were filtered from view, along with 'seniors' and those with 'ugly facial looks.' Curators were also told not to promote videos shot in 'shabby and dilapidated' surroundings.[34]

With these policies in force, TikTok subtly marginalized the unattractive and poor. In the digital era, a person, group, or idea must not be blocked or censored to be made irrelevant. They need only be buried in a tide of other information or presented in a way that minimizes the desire

---

30 Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, Oxford, 2019, p. 83.

31 Richard H. Thaler and Cass Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness,* Penguin, London, 2009.

32 Eliza Mik, *'Persuasive Technologies: From Loss of Privacy to Loss of Autonomy,'* in Kit Barker, Karen Fairweather and Ross Grantham (eds), Private Law in the 21st Century, Hart Publishing, Oxford, 2017, p. 375.

33 Richard Susskind*, The Future of Law: Facing the Challenges of Legal Technology,* Oxford University Press, Oxford, 1996.

34 Sam Biddle, Paulo Victor Ribeiro and Tatiana Dias*, 'Invisible Censorship: TikTok Told Moderators to Suppress Posts by "Ugly" People and the Poor to Attract New Users'* The Intercept, 16 March 2020 <https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/> (accessed 20 August 2021).

to give them attention. Digital leviathans have the power to frame our perception of the world.

Some of the concerns with this kind of power are well known. For instance, being ranked too far down on Google's results pages can mean calamity for businesses, which is why they spend tens of billions of dollars every year to try to stay high in the rankings.[35] Other worries relate to abuse and manipulation. The European Commission has found that Google's search results sometimes prioritize its own products over those of rivals. Concerns have also been raised that search engines might affect the results of elections.

When Google tweaked its algorithm in a well-intentioned effort to shunt extremist publishers down its news feed, it inadvertently choked off traffic to public service websites that reported on extremist content. One saw its traffic drop 63 percent.[36]

In 2018, then CEO of Twitter, Jack Dorsey, came before Congress and somberly informed the American people that the platform's algorithms had been 'unfairly filtering' 600,000 accounts, including some members of Congress, from the platform's search auto-complete and latest results.' This admission confirmed longstanding anxieties that the platform might be manipulating the political process without anyone intending it or noticing.[37] Though his confession drew praise, it demonstrated how submissive people have become in the face of technology's power.

The current CEO of Twitter, Elon Musk, hides no shame in responding to a declaration that social media companies, including Twitter, take money from the government to censor people.[38]

It is clear that private corporations that sort and order the world's information now decide, in significant part, what goes on society's agenda. It is an important political responsibility, and with it comes risk.

---

35 Robert Epstein and Robert E. Robertson*, 'The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections,'* Proceedings of the National Academy of Sciences of the United States of America, Vol. 112, No. 33 (2015), E4512–E4521.

36 Emily Bell, *'The Unintentional Press: How Technology Companies Fail as Publishers',* in Lee C. Bollinger and Geoffrey R. Stone, The Free Speech Century, Oxford University Press, New York, 2019, p. 237.

37 Jamie Susskind, *'What we need from social media is transparency, not apologies',* The New Statesman, 6 September 2018 <https://www.newstatesman.com/science tech/2018/09/what-we-need-social-media-transparency-not-apologies> (visited 16 December 2022).

38 Elon Musk (@elonmusk). *"Other social media companies too, not just Twitter."* December 20, 2021, 11:10 p.m. Tweet.

Then there's the matter of election manipulation. In 2012, Facebook published in Nature the results of a randomized controlled study on 61 million users in the United States during the 2010 congressional elections.[39] During election day, one group of Facebook users was shown a banner encouraging them to vote with an 'I voted' button. Another was offered the same banner and photographs of friends who had already clicked 'I voted.' A third group was shown nothing. The second group – those shown photos of friends who had voted – were 0.4 percent more likely to vote. The study's authors claimed that by showing photos of friends who had voted, the turnout was increased to 340,000 votes—enough to swing many elections.[40] This brings into question how Facebook obtained the consent of the 61 million users.

Perhaps the most glaring example of perception manipulation is the Cambridge Analytica scandal. Cambridge Analytica is a British firm accused of siphoning 50 million Facebook user's data to aid Donald Trump's US presidential campaign. Whistleblowers testified in open court that Trump's key adviser, Steve Bannon—used personal information taken without authorization in early 2014 to build a system that could profile individual US voters, in order to target them with personalized political advertisements.[41] Lawsuits against Cambridge Analytica and Facebook are ongoing up to this day. Recently, Facebook (now Meta) has finally agreed to pay $725m to settle the Cambridge Analytica scandal case.[42]

Cambridge Analytica's parent company, Strategic Communications Laboratories ('SCL') had operations in the Philippines. SCL posted on its now defunct website, that their research showed that many groups within the electorate were more likely to be swayed by qualities such as toughness and decisiveness. SCL used the cross-cutting issue of crime to rebrand the client as a strong, no-nonsense man of action, who would appeal to the true values of the voters—this is a clear description of what happened in the 2016 Philippine elections.[43]

---

39 M. Bond, C. J. Fariss, J. J. Jones, A. D. Kramer, C. Marlow, J. E. Settle and J. H. Fowler *'A 61-Million-Person Experiment in Social Influence and Political Mobilization'*, Nature 489, 2012.

40 Carissa Véliz, *Privacy is Power: Why and How you Should Take Back Control of Your Data*, Transworld Publishers, London, 2020, pp. 103–104.

41 The Observer, The Guardian News and Media, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* March 17, 2018. < https:// www.theguardian.com/news /2018/mar/17/cambridge-analytica-facebook -influence-us-election> (visited 16 December 2022).

42 Nate Raymond, Reuters, *Facebook parent Meta to settle Cambridge Analytica scandal case for $725 million.*<https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/> (visited 16 December 2022).

43 Raissa Robles, South China Morning Post, *How Cambridge Analytica's parent company helped 'man of action' Rodrigo Duterte win the 2016 Philippine election*. April 4, 2018. <https://www.scmp.com/ News /asia / southeast-asia/article/2140303/ how-cambridge-analyticas-parent-company-helped-man-action> (visited 16 December 2022).

In a few decades, a relatively small number of private corporations, the *de facto* leviathans, have assumed the power to frame not only how the rest of us see the world but also nudge us to shape the world to its own liking. This is unsatisfactory. The structure and health of the information environment should not be treated as a corporate concern. It is res publica.[44]

V. UNACCOUNTABLE POWER – BIG TECH BECOMES BIG BROTHER

The central challenge for freedom and democracy can be captured in two words: unaccountable power. In the early days of the commercial internet, scholars discovered that, in cyberspace, computer code operated as a kind of 'law.'[45]

For the digital leviathans, its source of law is the programmer's code. Legislators and judges do not decide the rules – but a different kind of law, embedded in the tech itself. Whenever we use an app, platform, smartphone, or computer, we have no choice but to follow the strict rules that are coded into these technologies.

Some rules are commonplace, like the rule that you cannot access this system without the correct password. Enter the cryptocurrency owners who lost millions in fortune just because they couldn't remember the password to their virtual currency wallets.[46] Other rules are controversial, such as getting banned or temporarily suspended from social media websites for voicing out one's opinion.

Every time humans use a search engine, digital assistant, news app, social media platform, or the like, they let others subtly shape their outlook. Digital systems propel issues to the top of the public agenda or make them disappear. Code carries the power to affect how we perceive the world.

Another form of power lies in the capacity of digital technologies to gather data. More of our thoughts, feelings, movements, purchases and

---

[44] Melissa Lane, Greek and Roman Political Ideas, Penguin Books, London, 2014, p. 12; see also the editor's note at Marcus Tullius Cicero, The Republic and The Laws, Oxford University Press, Oxford, 1998, p. 181.

[45] Lawrence Lessig, Code Version 2.0, Basic Books, New York, 2006.

[46] Nathaniel Popper, 'Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes', The New York Times, 12 January 2021 <https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html> (visited 16 December 2022).

utterances are captured and analyzed by systems working silently around us. With constant usage, they better identify our tastes, fears and habits. This leaves us increasingly exposed to influence.

In short: technologies exert power; that power is growing, and it is entrusted to those who write code. As more of our activities are mediated through online platforms, those who write code increasingly write the rules by which the rest of us live. Software engineers are inadvertently becoming social engineers.[47]

Big Tech is not designed to be political. Digital power doesn't reside in a palace or parliament. It operates outside the traditional channels of high politics. This presents a danger. If we continue down our current path, liberty could be stifled and democracy undermined by diffuse technical forces that cannot be attributed to any single entity. There is no system of accountability. No check and balance of power. Jamie Susskind suggests one big answer to this problem. The idea is ancient in origin but modern in application. It is called digital republicanism.[48]

In the Roman Republic, the greatest threat to liberty was believed to lie in *imperium*: unaccountable power in the hands of the state. But republicanism also warns against *dominium*: unaccountable power in the hands of private individuals and corporations.[49]

James Madison understood this, urging of the need 'not only to guard the society against the oppression of its rulers; but to guard one part of the society against the injustice of the other part.'[50]

In essence, to be a republican is to oppose social structures that enable one group to exercise unaccountable power, also known as domination, over others.[51] To be a republican is to object to the idea of someone with Mark Zuckerberg's power, not Mr. Zuckerberg himself. To be a republican is to oppose the absolute power of the digital leviathans.

---

47 Jamie Susskind, *Future Politics: Living Together in a World Transformed by Tech*, Oxford University Press, 2018.

48 Jamie Susskind, *The Digital Republic: On Freedom and Democracy in the 21st Century*, Pegasus Books, 2022.

49 Richard Dagger, *'Republicanism and the Foundations of Criminal Law'*, in R. A. Duff and Stuart P. Green (eds), Philosophical Foundations of Criminal Law, Oxford University Press, Oxford, 2013, p. 47.

50 Alexander Hamilton, James Madison and John Jay, *The Federalist Papers*, Penguin Classics, New York, 2012, p. 96.

51 K. Sabeel Rahman, *Democracy Against Domination*, Oxford University Press, New York, 2017.

VI. CONCLUSION

We have woken the digital leviathans and we have experienced its effects.

Left unchecked, our digital leviathans will inevitably turn into the chaotic mythical monster that mankind can never overcome. Technology's power will grow faster than our social systems' ability to adapt. Legal reforms should be introduced to match legal responsibility.

We must reject the notion that we can only enjoy the wonders of digital technology if we submit to the unaccountable power of those who design and control it.

11

Magnetized by Big Brother: When Thought Control Comes in Enticing Robes

by Bryan Alvin Rommel Y. Villarosa

MAGNETIZED BY BIG BROTHER:
WHEN THOUGHT CONTROL COMES IN ENTICING ROBES

*Bryan Alvin Rommel Y. Villarosa**

As computers become smaller and faster, they become more powerful in influencing our lives. We welcome them to assist us and entertain us. The intimacy of this companionship enables us to access anything we want, watch anything we want, and be entertained forever. In this era called by many as "Industry 4.0", the quantity of enticing online content is staggering and the cravings for new material seem unquenchable. In a world addicted to entertainment, are we missing something?

In this article, we explore the correlation between online entertainment and thought control. First, we examine the evil of thought control as substantiated by the law; Second, we survey the timely warnings of two renowned authors; and third, we determine whether or not the "Big Brother in enticing robes" is already among us. This article gives us reflection points the next time we are magnetized by these glowing screens.

The image above is created by artificial intelligence using the keywords of this essay

I. THE MONSTER THAT IS THOUGHT CONTROL

Is mind control evil?

In Orwell's Novel, Big Brother maintains his autocratic control over Oceania by controlling the minds of the population. If you were there:

(a) You cannot turn off a telescreen in your home. Every corner of the city says, "Big Brother is watching you";

(b) Once you get caught committing a "thought crime", the Thought Police from the Ministry of Love will arrest you, and may "vaporize" or "unperson." It could mean extrajudicially shooting you at the back of your head; and

(c) You must "doublethink". It means you are conditioned to accept contradictory beliefs as correct. The examples are "War is Peace", "Freedom is Slavery", "Ignorance is Strength", and "2 + 2 = 5."

Big Brother also preserves his power by using brute force. But the question is: is this "strongman approach" always unloved by the world? Not really.

Time Magazine published "The 'Strongman Era' is Here. Here's What It Means x x x."[1] The author argues that the discouraging events in the US and EU boost the demand for more muscular, assertive leadership which is increasingly becoming popular in Russia, Asia, and other parts of the world. The basic idea is "Why emulate Western political systems, with all their checks and balances when these systems prevent our leaders from quickly solving chronic problems?" "Why pursue the freedoms of thought, speech, and expression if the West that *endorsed* them is suffering from their weaknesses? Why not simply acquiesce and let the "strongman" take charge?

---

* Bryan Villarosa is pursuing his Juris Doctor degree at USLS Bacolod while working as a legal researcher and marketer for various firms and brokers. Bryan is passionate about the intersection of law and technology because he believes in its power to drive positive change in the world. He is also enthusiastic about certain sports like marathons and obstacle racing to improve well-being and build relationships.

1 Ian Bremmer, *The Strongmen Era Is Here. Here's What It Means for You*, https://time.com/5264170 /the-strongmen-era-is-here-heres-what-it-means-for-you/ (visited September 6, 2022).

Despite this rising political inclination, I submit four main reasons why freedom of thought and its consequent rights[2] are vital. These are (1) Natural Law; (2) Positive law; (3) Economic Law; and (4) International Law.

A. *Natural Law calls us to think freely.*

Above all, freedom of thought is a natural right. It arises from natural law. It precedes the existence of the state. Even without the state, man has the right to be free from thought control.

Natural Law is the True and highest form of law. It shapes morals and public policy. Its author is God Himself. It is a sin to try to alter this law. This is the only eternal and unchangeable law that is valid for all nations and at all times.[3]

For Christians, one main source of Natural Law is the Divine Law or the Scriptures. It is filled with principles that encourage thought and reasoning.

Christ Himself never forced people to faith. He *taught* and *reasoned* with the people and then *appealed* to them to follow Him as the Messiah. He *invited* people, "Come to me, all who labor and are heavily laden and I will give you rest."[4] Using Bloom's taxonomy, He qualifies as a "master of critical thinking," a "paragon of edagogy," and a "Master Teacher par excellence."[5]

The Apostle Paul went to the synagogues and "*reasoned* with [the people]."[6]

The Old Testament prophet Isaiah told his backsliding countrymen, "Come now, let us *reason* together. Though your sins are as scarlet, they shall be white as snow." The Prophet Daniel respectfully expressed dissent to the King. He said, "Therefore, O king, *let my counsel be acceptable* to you: practice righteousness x x x break off your sins by showing mercy to the oppressed, that there may perhaps be a lengthening of your prosperity."[7]

---

2 *Estelle T. Griswold and C. Lee Buxton vs. Connecticut*, 381 U.S. 479.

3 *Republic vs. Sandiganbayan*, G.R. No. 104768 (Separate opinion of Justice Puno).

4 The Holy Bible, Matthew 11:28.

5 Jesus' Questions in the Gospel of Matthew: Promoting Critical Thinking Skills - Zummy Anselmus Dami, Ferdinant Alexander, Yanjumseby Yeverson Manafe,2021<https://journals.sagepub.com/doi/full/10.1177/0739891320971295> (visited September 8, 2022).

6 The Holy Bible, Acts 17:2.

7 The Holy Bible, Daniel 4:27.

Even God Himself gives humans the freedom of thought. When Adam and Eve disobeyed, God did not hastily punish them. He first asked, "Who told you that you were naked? *Have you eaten of the tree* of which I commanded you not to eat?"[8] There was a hearing. God gave them the opportunity to be heard.

From the perspective of science, our most significant distinction from animals is our capacity to reason. This capacity is what religion calls the "soul" which was breathed into Adam's nostrils after he was formed from the dust.[9] On top of our reasoning power - we have a moral compass, a conscience, and an inherent sense of right and wrong.[10]

Next, I argue from the perspective of positive law because if natural law is included in legal arguments, dissents are raised on the ground that the government should neither rely on religious beliefs nor conform to a particular sect.[11] But freedom of thought remains firm on the ground of positive law.

B. *The Fundamental Law protects thought freedom.*

Freedom of thought is concretely embedded in the 1987 Constitution, although not in the exact term. It can be derived from Article III Section 4 through a process called "reasoning by interpolation."[12] The law expressly provides: "No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for a redress of grievances."

Here, we can derive by implication that there is no freedom to speak if there is no freedom to think. Free speech is a penumbral effect of free thoughts. To grant only the former without the latter is nothing but gibberish.

Ultimately, there is no democracy if there is no freedom to think. Democracy is only possible if we have a rational citizenry. Hence, thought control is antithetical to democracy. After all, all government authority

---

8 The Holy Bible, Genesis 3:11.

9 The Holy Bible, Genesis 2:7.

10 *People vs. Madarang*, G.R. No. 132319.

11 *Id.*

12 Glenn H. Reynolds, Penumbral Reasoning on the Right, 140 U. Pa. L. Rev. 1333, 1334–36 (1992); see also J. Christopher Rideout, Penumbral Thinking Revisited: Metaphor in Legal Argumentation, 7 J. ALWD 155, 155–56 (2010).

emanates from [the people][13]. If we lose the ability to think, we lose our Sovereignty. And if we lose our Sovereignty, we descend into tyranny.

C. *Thought freedom and the marketplace of ideas*

In economics, a free market is the absence of restrictive external controls. Here, sellers and buyers are free to decide what goods to sell and buy subject only to certain limitations. Sellers are driven to create the best goods at the lowest price and buyers are drawn to the best sellers. Together, they create the law of supply and demand. Inferior items are destroyed and innovations are rewarded. Some call it "creative destruction." Adam Smith uses the term "the invisible hand." Hence, the driving principle of the free market is: Let the market decide. Only with the free market can cutting-edge breakthroughs thrive.

In the same way, this is true with the "Free Market of Ideas" - a marketplace that Article III Section 4 protects. There must be sellers and buyers of publicly-related ideas. They must be free to choose what ideas to own and trade. Contrary ideas are intelligently welcomed and assessed. Discourses are encouraged because this is where progress happens and democracy is preserved. To suppress them is to return to the Dark Ages - a time when free ideas were suppressed.

D. *International Law*

International law supports freedom of thought. These are given equal standing with, but are not superior to, national legislative enactments.[14]

The Universal Declaration of Human Rights, an international law, expressly provides, "Everyone has the right to freedom of thought x x x Everyone has the right to freedom of opinion and expression; x x x [to] hold opinions without interference and to seek, receive and impart information and ideas through any media x x x."[15]

From these references, natural and positive laws substantiate freedom of thought. Hence, mind control is evil.

---

13 Constitution, Art. II, Sec. 1.

14 *Secretary of Justice v. Lantion*, G.R. No. 139465.

15 Universal Declaration of Human Rights, Art. 18 and 19.

These fundamentals are also crucial because they cannot only be invoked against the government, but also against the behemoth tech corporations. Our relationships with these platforms are contractual by nature and, if unchecked, they have the vast freedom to stipulate any conditions. The only limitation that we can enforce against them is when their stipulation is "contrary to law, morals x x x or public policy."[16]

Now, an emerging threat subtly diminishes our Freedom of Thought - the pleasures of entertainment.

II. ENTICING ROLES: THE ENCHANTING BIG BROTHER

Orwell warns us of an oppressive Big Brother, but another tyrant may come in a way we may not expect - an enchanting Big Brother in enticing robes. This is what Aldous Huxley warned us about in his 1932 novel entitled, *A Brave New World*. He introduced entertainment as the villain in disguise.

In Huxley's novel, people are addicted to *soma*, a powerful drug that catapults users into heights of pleasure. It enables them to daydream and escape reality. Ultimately, the opposition was suppressed, and the authoritarian power maintained control. Huxley warns of a society that could potentially become our reality - one where an elite entity controls thoughts through exciting pleasures. He warns of a future where the powerful will enslave minds, yet people will not feel enslaved at all.

The Warnings of Orwell and Huxley

Orwell's *1984* and Huxley's *A Brave New World* both unite in illustrating a harrowing future where:

> Advanced technologies will be used to control minds;
>
> Freedoms will be curtailed, and people will be conditioned to accept it as normal;
>
> Thought control that will cause spiritual, political, and social devastation;
>
> Unaccounted powers that will systematically suppress dissent.

---

[16] New Civil Code, Art. 1306.

But Orwell and Huxley have opposite views on certain aspects:

> Orwell warned us of a terrifying dictator, while Huxley warned us of an alluring manipulator;
>
> Orwell portrayed him as a roaring lion seeking whom he shall devour, while Huxley portrayed him as a ravening wolf in sheep's clothing;
>
> Orwell's Big Brother points a gun at people's faces, while Huxley's dictator comes with smiles and embraces;
>
> Orwell feared that what we hate would destroy us, while Huxley feared that what we enjoy would enslave us;
>
> In Orwell's world, words are given double meaning until no one knows which is true; in Huxley's world, stimuli are overwhelming until no one can identify issues.
>
> Orwell's society is threatened with punishment, while Huxley's society is drowned in entertainment;

III. IS THE BIG BROTHER IN ENTICING ROBES ALREADY IN OUR MIDST?

We will not concern ourselves with analyzing whether Orwell or Huxley was right. Rather, we will assess if the "Big Brother in enticing robes" is already among us. He comes disguised in ways that capture hearts, instead of inciting uproars; hence, he comes in "enticing robes." Here are eight observations:

> First, he has been described by the Supreme Court in *Diocese of Bacolod vs. COMELEC*.[17] His existence has long been observed like a dragon ready to be hatched from its mother's eggs. Quoting Herber Marcuse's work, the High Court recognized that even in the freest and most democratic societies, the marketplace of ideas is still delimited by *dominant political actors*. The Court acknowledges that through authority, power, *resources*, identity, or status, dissenting opinions and philosophies cannot compete and *are being drowned out* by the powerful. Marcuse calls this "Repressive Tolerance." (emphasis added)

---

[17] *Diocese of Bacolod vs. COMELEC*, G.R. No. 205728.

Repressive tolerance squares with the "Big Brother with enticing robes" because such a system is subtle. It appears like a cheerful friend but stealthily drowns out dissenters and slits the latter's throats like an assassin.

Second, the reality of Big Brother is even more feasible today with our online technologies. Smartphones and social media are "necessary" tools to make such repressive tolerance possible. Here are parallels between Big Brother and current online realities:

(1) In Orwell's world, there is visual surveillance in the home; today, visual and geolocational surveillance are possible through smartphones and IP addresses;
(2) In Huxley's world, citizens are bombarded with immense mental distractions; today, our pockets carry these enormous mental distractions;
(3) In Orwell, Big Brother can see your actions; today, Big Brother can even know what's inside your mind through your online footprints. He can even know your future interests through a process called predictive analytics;
(4) In Huxley, thoughts are suppressed by narcotization; today, thoughts can be suppressed by false information.

In the year 2021, respondent Filipinos spent an average of 4 hours and 8 minutes per day on social media.[18] How much more if we include the time outside socials but online? How dependent have we become?

Third, is the addiction to dopamine. Huxley's world is addicted to *soma*. Today's world may be addicted to dopamine. Dopamine is a "feel-good" chemical released in the brain that can be triggered by smartphones and other online pleasures. If *soma* caused Huxley's world to daydream and forget time; today, dopamine can do the same.

From a neurological perspective, dopamine is the primary driver of addiction. It is a chemical responsible for pleasure. It is a neuromodulatory molecule that always wants more and is never content. As a result, we cultivate a culture where people will only pay attention if their dopamine is released.

---

[18] APAC: daily time spent using social media by country 2021 | Statista <https://www.statista.com/statistics/1128147/apac-daily-time-spent-using-socialmedia-by-country-or-region/#statisticContainer> (visited 16 December 2022).

Fourth, is the decay of self-awareness. The people in Huxley's world did not understand when John, the protagonist, confronted them about their *soma* overdose; Today, it's the same. If confronted about online addiction, many will see such confrontation as out-of-this-world or will even get pissed.

Fifth, using entertainment to suppress dissent. In Huxley's world, opposing opinions were suppressed by chemically-induced excitement; today, oppositions can be suppressed by algorithms and cancel culture.

This content can be political videos mingled with entertaining flares. These are politically motivated but repurposed into short-form content and combined with music and effects. To suppress dissent, artificial strategies are used to increase or decrease visibility.

Sixth is a filtered culture. In Huxley's world, people have come to love their own delirium. As a result, they filter and accept only those that give self-gratification. They are similar to Queen Grimhilde, the Queen in Snow White who keeps asking, "mirror mirror on the wall, who's the fairest of them wall?" The Queen listens to the mirror as it pleases her. If not, she annihilates the competition.

In the same way, online society today puts primacy on self-gratification. Like the magic mirror, online platforms are compelled to please "the queen" by showing only pleasing content. They also give the capacity to "unfollow" and "block" any disagreeable content creators. The algorithms they develop confine us in a filtered world that "annihilates" opposition. This culture erodes our capacity to gain new perspectives. It causes us to lose our sense of comparison. A marketplace of ideas deprived of competition actually weakens the culture, not strengthens it.

Seventh is the preference of the electorate for entertainers. It is worth noting that a significant number of entertainers, celebrities, and sports figures have won our elections in recent years. This does not mean that celebrities and sports stars have no right to hold a seat in the government. But when entertainment is prime, election campaigns may center around mindless entertainment jingles, rather than animated by agendas and platforms; voters will vote on the basis of fame rather than platforms and competence, and significant government positions will be filled with famous personalities instead of competent ones.

Eight is the shortening of expression through short-form videos. In Huxley's world, there is no need to ban books because the citizens are no longer interested. Today, big media are adopting what is called the short-

form format. This is becoming prominent in TikTok, Youtube, Instagram, and Facebook Reels. Its main goal is to capture attention within the first few seconds to support a short attention span. It puts primacy on showmanship, aesthetics, and oversimplification of ideas. The users are then bombarded with videos of the same character to keep their attention and keep them addicted to coming back. As a result, society frowns upon comprehensive expositions and meaningful discourses are diminished.

IV. THE PURSUIT OF REAL HAPPINESS

The Big Brother in enticing robes may be in our midst, but is it a call to uninstall our social media accounts or let go of technology? Absolutely no but his presence must not violate our natural and constitutional rights to freedom of thought.

I submit that smartphones and online entertainment are not evil per se because, needless to say, they give enormous benefits. They are a double-edged sword. They optimize learning, enhance productivity, and aid human flourishing. Also, smartphones are not one-way media like TV which we watch as passive consumers. Here, we can be in control, as long as we retain the inner drive to use them for the better.

As seekers of entertainment, we may anchor our arguments on our "unalienable Rights x x x [to] the pursuit of Happiness"[19] and that no one should be deprived of life and liberty.[20] The phrase "pursuit of happiness" was coined by a major English philosopher, John Locke, whose political writings paved the way for the American Revolution. Locke submits that when people are happy, they are mobilized to take action and responsibility. But this happiness does not simply equate to "pleasure," material things, or self-gratification which he distinguishes as false or imaginary happiness. What he persuades us to do is pursue true and real happiness. Imaginary happiness is temporary but true happiness leads to the overall quality of life. False happiness is irrational and is running only after immediate gratification and is typically followed by more pain.

Locke argues that the stronger our attachment to this freedom, the more our desires will flow naturally, and the more we will be free.[21] Hence, the constitutional guarantee of happiness is not a license to be enslaved by our urges. Unlike animals, our pursuit of happiness empowers us to be free, instead of succumbing to the dictates of nature. It empowers

---

19 United States Declaration of Independence.

20 Constitution, Art. III, Sec 1.

21 Locke, John. *An Essay Concerning Human Understanding*. Oxford University Press, 1689.

us to have victory against Big Brother in enticing robes. The key is to work on our hearts.

It goes without saying that the love for happiness is not contrary to freedom of thought, for true love leads to mental care. A truly happy world is a rational world.

The lifeblood of our laws is our values.

Since each person has the inherent right to pursue happiness, no government or corporation should try to interfere. Once clearly established, this right will strengthen our legal system now and in the future. We cannot invoke freedom of speech against the behemoths of online platforms because our relationship with them is contractual in nature, only against the State. However, the freedom to stipulate is not absolute when we have the guarantee that a certain stipulation is contrary to morals or public policy.

> Every good law draws its breath of life from morals, from those principles which are written with words of fire in the conscience of man. x x x While codes of law and statutes have changed from age to age, the conscience of man has remained fixed to its ancient moorings.[22]

The essential thing now is that as we are bombarded with enticing content, let us raise the level of our discernment and be steadfast in guarding against abuse of our intimate thoughts; to deepen our awareness of the dangling of our freedoms and the consequent effects of our lives, and to be conscientious in our engagements with emergent technologies.

Otherwise, we will end up like the citizens in Huxley's world where they drown in laughter but no longer know why they are laughing; or like the rioters in the City of Ephesus who shouted on the streets but did not actually know why they were there.[23]

After all, the enemy does not always come in terror but may come cloaked in enticing robes.

---

[22] *Secretary of Justice vs. Hon. Lantion and Mark Jimenez*, G.R. 139465.

[23] The Holy Bible, Acts 19:23-32.

IV

COMMENT

12

A Guide to Constitutional Change in the Philippines

by Gabriel Christian Lacson

A GUIDE TO CONSTITUTIONAL CHANGE IN THE PHILIPPINES

*Gabriel Christian J. Lacson**

"Time and the world do not stand still. Change is the law of life. And those who look only to the past or to the present are certain to miss the future," so spoke the former United States President John F. Kennedy. In this brief but defining statement, Kennedy made clear his views on society, morals, and systems, which informed his administration and served as food for thought for practitioners and students of the law and its evolutionary procedures. He believed that one of the delicate tasks of any government is to update laws and practices from time to time to reflect evolving social values and norms, as another Singapore Prime Minister Lee Hsien Loong would so aptly say later on.

In this regard, the major issue of constitutional reform in the Philippines remains and is viewed as a contentious political and legal issue. Since achieving sovereignty in 1946, the country has retained, in one form or another, a unitary presidential form of government, according to the 2021 CIA World Factbook[1]. With the country's Fifth Republic retaining this political system and having stood since the eventful years of 1986 and 1987, scholars, economists, legal practitioners, and politicians, to name a few professions, have debated this issue without end in light of societal problems faced by the Philippines and its people since the ratification of the current Constitution.

A DEMOCRACY CHALLENGED

Among the most prominent problems pointed out by many advocates for reforms prevailing within the current milieu include political domination by a strong president resulting in the proliferation of corrupt practices with weak party discipline,[2] hyper-centralization resulting in an over-populated metropolitan capital area,[3] and the tendency of Filipinos to

---

* Gabriel Christian J. Lacson is a fourth-year student from the University of St. La Salle College of Law, who has also contributed some opinion columns in a local digital paper. Slated to graduate in mid-2023, his interests mainly include constitutional reform, comparative political systems analyses, graphic design, and playing the ukulele.

1 Central Intelligence Agency. The World Factbook 2021. Washington, DC (2021).

2 Kawanaka, Tetsuo. "Interaction of Powers in the Philippine Presidential System." (2010), Research Gate.net,https://www.researchgate.net/publication/46473433_Interaction_of_Powers_in_the_Philippine_Presidential_System.

3 Collymore, Yvonne. "Rapid Population Growth, Crowded Cities Present Challenges in the Philippines" PRB.org, (2003), https://www.prb.org/resources/rapid-population-growth-crowded cities-resent challenges-in-the-philippines/.

find better work opportunities in other countries.[4] Its political arena has likewise been repeatedly dominated by a handful of elite and influential political families and economic tycoons. At the same time, a hefty majority of its people remain mostly poor and struggling.[5] The Philippines, although a country of plenty, has more critically been ranked as the most economically restrictive in East Asia by the Organisation for Economic Co-operation and Development.[6]

Conversely, a look back into the recent history of the Philippines during the 20th century shows how institutional infirmities have led to a persistent skepticism of reform owing to political experiences and maneuverings under President Ferdinand Marcos' period of "Constitutional Authoritarianism" and Martial Law. It became clear in President Marcos' tenure and his lawmaking powers, as evidenced by Amendment No. 6,[7] that the 1973 Constitution was re-purposed several times for his own ends, thereby creating no visible departure from the presidentialist regimes imposed by the previous 1935 charter.

Arguably, the Marcos regime's record on governance, economic management, and upholding the rule of law left a negative impression on the national interest, leading to a polarization of feelings and doubts about his government. This skepticism guides the views of a significant section of Filipinos, some of whom remain adamantly opposed to even the notion of change to avoid any risk of a resurgence of repugnant authoritarianism.

Moreover, there likewise exists many mistaken notions on how to create meaningful change through constitutional reform in a departure from these recent and historical national woes. The framers of the Constitutional Commission of 1986, however, were not blind to the eventual necessity of any potential, future reform to the document. In this vein, a closer look at the Constitution of the Republic of the Philippines, particularly the text of Article XVII,[8] affords people a more simplified, sober understanding of the necessary steps to be taken before any alteration is to be made.

---

4 Fernandez, Muyot, Pangilinan, & Quijano. "A Hero's Welcome: Repatriated Overseas Filipino Workers and COVID-19." LSE Southeast Asia Blog, October 8, 2020, https://blogs.lse.ac.uk/seac/2020/10/08/a-heros-welcome-repatriated-overseas-filipino-workers-and-covid-19/.

5 McCoy, Alfred W. (1994). An Anarchy of Families: State and Family in the Philippines.

6 OECD. "FDI Restrictiveness (indicator)." (2022), OECD, doi:10.1787/c176b7fa-en (Accessed on 16 September 2022).

7 Hernandez, C. G. "Constitutional Authoritarianism And The Prospects Of Democracy In The Philippines." Journal Of International Affairs, 243-258 (1985).

8 Constitution, Art. XVII, §§ 1-4.

HOW IS THE CONSTITUTION TO BE AMENDED?

In opening the path to constitutional reform, the first step of amending or revising the Philippine Constitution shall be through a Constitutional Convention through a vote of two-thirds of all its members contained in both the House of Representatives and the Senate. While the Constitution remains silent on whether their votes shall be counted separately or jointly, it should be inferred that separate voting is intended as a feature of the current bicameral legislative system.[9]

A Constitutional Convention will have its delegates elected by the Filipino people, similar to congressional elections. These elected delegates shall work to produce a new framework of the state within a prescribed amount of time.[10] These elections may be held either separately or jointly with national elections.

Another method of amendment and revision mentioned explicitly is through the Congress acting as a constituent assembly, through a vote of three-fourths of all its members, creating the changes it desires. As elected representatives of the Filipino people, this constituent assembly will purposefully propose changes to the basic law. Again, the consequences of bicameralism should follow in voting for this mode. Both methods of constitutional change shall only take effect and be valid when ratified by a majority of the votes cast in a plebiscite which shall be held not earlier than sixty days nor later than ninety days after the approval of such amendment or revision.[11]

The major difference between a Constitutional Convention and Constituent Assembly lies mainly in its political thresholds for either to be convened validly and lawfully. It likewise lies in the ways and means its delegates are selected and the timeframe given for the amendment or revision process. Congress acting as Constituent Assembly will, certainly, have only until the expiry of its term to propose any amendments or revisions. But certainly, either method and achieving the same will prove a drawn-out political process that entails the expenditure of time, effort, and political capital.

---

9 Bernas, Joaquin G. The 1987 Constitution of the Philippines: A Commentary. Quezon City: REX Book Store, 2009.

10 An Act Providing for the Election of Delegates to, and the Holding of, the Constitutional Convention Authorized by Resolution of Both Houses of the Congress of the Philippines (1967).

11 Bernas, J. *supra*.

Another but otherwise complicated method of providing changes to the Constitution is the method of "people's initiative," where the people may directly propose amendments to the Constitution through initiative upon a petition of at least twelve percent of the total number of registered voters, of which every legislative district must be represented by at least three percent of the registered voters in that district, but the methodologies for attaining such goals are complicated and lack major legal specificity. Crucially, Father Joaquin Bernas in his book on constitutional law further notes that no law has yet been enacted for the purpose of implementing the constitutional provision on the amendment by initiative and referendum.

AMENDMENTS VERSUS REVISIONS

In defogging the uncertainties of constitutional reform, the difference between amendments and revisions ought to be clarified, as there is a substantial distinction regarding these two forms of creating new policies in any fundamental law.

Speaking with precision, the Supreme Court of the Philippines, in the 2006 case of *Lambino et. al. vs. The Commission Elections* explained, "An amendment envisages an alteration of one or a few specific and separable provisions. The guiding original intention of an amendment is to improve specific parts or to add new provisions deemed necessary to meet new conditions or to suppress specific portions that may have become obsolete or that are judged to be dangerous."[12] Clearly, amendments are described as small and incremental steps forward in creating changes to the country's basic institutional framework.

The Court goes on in the same case to state that "In revision, however, the guiding original intention and plan contemplates a re-examination of the entire document, or of provisions of the document which have overall implications for the entire document, to determine how and to what extent they should be altered."[13] A rule of fundamental or total change applies in dealing with the text itself through revisions; the coverage is, therefore, more comprehensive.

---

12 *Lambino et. al. v. Commission on Elections*, G.R. No. 174153 (25 October 2006).

13 *Id.*

CONCLUSION

All things equal, the touchy topic of constitutional change demands scrutiny and proper nuancing by its advocates, critics, and on the part of ordinary Filipinos, as this consists of a whole-of-nation effort. It should not be viewed as a panacea, a one-shot cure for the deep ailments of the state. It is not easily understood overnight, with debates about the proposed government's mode of regional territorial administration, political accountability machinery, and economic regime up for discussion in any new basic law. Some scholars have advocated reexamining the unitary presidential system altogether. Undoubtedly, it will require a significant amount of convincing people, informing them, and educating them. These remain worthy of another discussion by themselves.

The goal of any potential constitutional reform should be to authoritatively address the democratic deficits that encumber the Filipino people with the problems of urban overcrowding, state capture by the elite, corruption, and the lack of opportunity they encounter today. Addressing the root causes of these problematic realities requires both a national and regional approach, where it is the common aspiration of the citizens for a better standard of living that is the keystone for a renewed national structure. Most importantly, citizens should be able to acknowledge and understand the vital nuances of this process of change, as the effects are certain to redound to their lives.

Ultimately, the modality of constitutional change lies in the hands of the Congress of the Philippines, but it need not be totally controlled by them. Should Filipinos across the country or at least a broad cross-section of its citizens venture and seek to benefit from the process and results of any change, they ought to be reminded that above all, we are a democratic and republican state - [14] people are sovereign; all citizens hold the keys to their future.

---

[14] Constitution, Art. II, § 1.

University of St. La Salle
College of Law
La Salle Avenue, Bacolod City 6100
Email: uslsbcdlawjournal@gmail.com

Volume 12 | Issue 1

Law Journal Staff

University of St. La Salle - College of Law
La Salle Avenue, Bacolod City 6100

Published in Bacolod City, Negros Occidental, Philippines 6100

SUBSCRIPTION INFORMATION

For further information on how to subscribe, contact:

Kim Arvin Billones
Circulation Manager, USLS Law Journal
University of St. La Salle
La Salle Avenue, Bacolod City 6100
Phone #: +63 936 964 0332
Email: uslsbcdlawjournal@gmail.com

For further information on the University of St. La Salle - College of Law, contact:

Rosanne Juliana R. Gonzaga, Ll.M.
Dean, College of Law
University of St. La Salle
La Salle Avenue, Bacolod City 6100
Phone #: +63 917 3003 050
Email: law@usls.edu.ph
www.usls.edu.ph

For editorial inquiries, contact:

Rachel Lois Gella
Editor-in-Chief, USLS Law Journal
University of St. La Salle
La Salle Avenue, Bacolod City 6100
Phone #: +63 999 5510 737
Email: uslsbcdlawjournal@gmail.com

University of St. La Salle
College of Law
La Salle Avenue, Bacolod City 6100
uslsbcdlawjournal@gmail.com