THE FAR EASTERN LAW REVIEW

The Annual Publication of the Institute of Law

VOLUME LI • 2021

THE FAR EASTERN

LAW REVIEW

The Annual Publication of the Institute of Law

VOLUME LI • 2021

THE FAR EASTERN LAW REVIEW

The Annual Publication of the Institute of Law

VOLUME LI • 2021

THE FAR EASTERN LAW REVIEW

The Far Eastern Law Review (Law Review) is the official law journal of the Far Eastern University – Institute of Law. It is published annually by the FEU Law Review Editorial Board, which is composed of law students from the Institute.

The Far Eastern Law Review invites the submission of original and unpublished articles from bona fide law students of the Institute and law practitioners. The Law Review accepts submissions on interdisciplinary studies and welcomes diverse points of view on contemporary legal issues. The views, opinions, and conclusions expressed in the articles of this issue are those of the authors and do not necessarily reflect that of The Far Eastern Law Review, the Far Eastern University - Institute of Law, and the Far Eastern University. The author of each article published herein grants The Law Review the right to authorize the publication, reproduction, and distribution of the article in electronic, computerized retrieval system, and similar forms; and to transfer said rights.

Creatives and layout by Iren dela Cruz-Briones and the FEU Publications

Article Reference Format (Style Guide) adapted from The Bluebook: A Uniform System of Citation by the Harvard Law Review.

Interested contributors may submit their works through the addresses provided below. Please address correspondence to the following:

THE FAR EASTERN LAW REVIEW
Room 413
Institute of Law
Far Eastern University
Sen. Gil Puyat Ave. cor. Zuellig Loop
Makati City, Philippines
Email: feu.lawrev@gmail.com
Facebook: @FEULawReviewOfficial

FAR EASTERN UNIVERSITY
BOARD OF TRUSTEES

Dr. Lourdes R. Montinola
CHAIR EMERITUS

Mr. Aurelio R. Montinola III
CHAIRMAN

Dr. Michael M. Alba
PRESIDENT

Dr. Paulino Y. Tan
TRUSTEE

Mr. Antonio R. Montinola
TRUSTEE

Ms. Consuelo D. Garcia
TRUSTEE

Mr. Jose T. Sio
INDEPENDENT TRUSTEE

Dr. Edilberto C. De Jesus
INDEPENDENT TRUSTEE

Ms. Sherisa P. Nuesa
INDEPENDENT TRUSTEE

CORPORATE AND UNIVERSITY OFFICIALS

Dr. Michael M. Alba
PRESIDENT

Dr. Maria Teresa Trinidad P. Tinio
SENIOR VICE PRESIDENT, ACADEMIC AFFAIRS

Mr. Juan Miguel R. Montinola
CHIEF FINANCIAL OFFICER

Atty. Gianna R. Montinola
SENIOR VICE PRESIDENT FOR CORPORATE AFFAIRS

Atty. Anthony Raymond A. Goquingco
CORPORATE SECRETARY

Ms. Rosanna Esguerra-Salcedo
TREASURER

Mr. Enrique M. Amigo
CHIEF INFORMATION OFFICER

Mr. Ray Jan P. Roque
CHIEF AUDIT EXECUTIVE

Dr. Myrna P. Quinto
VICE PRESIDENT, ACADEMIC DEVELOPMENT

Engr. Edward R. Kilakiga
VICE PRESIDENT, FACILITIES AND TECHNICAL SERVICES

Mr. Glenn Z. Nagal
COMPTROLLER

FAR EASTERN UNIVERSITY
INSTITUTE OF LAW

Atty. Melencio S. Sta. Maria
DEAN

Atty. Jose Marlon Pabiton
ASSOCIATE DEAN

Maria Victoria P. Sido
SECTION HEAD

Melannie C. Santos
Karla May Z. Bayan
STAFF

FACULTY
A.Y. 2021-2022

ABES, JORGE AMBROSIO P.
ABITRIA, ROMMEL A.
ABRENICA, VERGENEE MARREE A.
AGUILA, EIRENE JHONE E.
ALENTAJAN, CARLO BONIFACIO C.
ALLAM, MARION P.
AMOROSO, DRANYL JARED P.
ATANACIO, JOHN DAVID C.
BAGUISI, ALAIN B.
BORJA, CATHERINE B.
BRONCE, ROENTGEN F.
CAMACHO, PAOLO FRANCISCO B.
CASTELO, YVES MIKKA B.
CASTILLO, PAUL CORNELIUS T.
CENIZA, SERGIO M.
CERVANTES-POCO, MARIA PATRICIA R.
CESISTA, VINCENT JOSEPH E.
CHAVEZ, MYRAFLOR L.
CRUZ, TERESITA L.
DE LEON, DINO ROBERT LIBUNAO
DE VEGA, NORIEVA D.
DEVERATURDA, JOAN PAULA A.
DY, ALEXANDER
FAJARDO, MARIAN IVY R
FRANCISCO, BELLATRIX L.
FRIAS, HELEN MAY M.
FULGUERAS, MARJORIE IVORY S.
GANCHOON, FRETTI G.
GENILO, JOSE EDUARDO T
GEOCANIGA, ROMMEL T.
GO, DAVID MICHAEL C
GOQUINGCO, ANTHONY RAYMOND A.
GREGORIO, JOEL EMERSON J
IBARRA, JOSE VENER C.
JAVIER, FILEMON RAY L.
JUMRANI, ALIAKHBAR A
KAW, EUGENE T
LADORES, IVAN MARK S
LIM, MARY ROCELYN PETALVER
LOANZON, VICTORIA V.
LOPEZ, RENATO B.
LUANSING, GLENN R .
MANO, RAZNA I.
RODRIGUEZ II, MANUEL
MARQUEZ, MARIA GWENDOLYN B.
MONSOD, KATRINA DIANE NOELLE C.
MURIA, RAMEL C. .
PABITON, JOSE MARLON P.
PAÑO, DIANA ABIGAIL A.
PARAS, EUGENE C.
PE BENITO, GALAHAD RICHARD A.
PEDRON, DIVINA GRACIA E.
PEÑA, GIDEON V.
QUAN, RYAN JEREMIAH D.
RAMOS, CHRISTINE ANTONIETTE O.
RANCES, DOMNINA T.
REAL JR., JOHN ROY ROBERT G .
REBOSA, ANTONIO ALEJANDRO D.
REYES, PIERRE MARTIN D.
RIGUERA, MANUEL R.
SALCEDO, VERA SHAYNE G.
SALUD, JOSEVICTORNIÑO L.
SAN JUAN-TORRES, MARIA JOSEFINA G.
SANA, MARCO CARLO S.
SANCHEZ, JENNIFER D.
SOKOKEN, DESIREE N.
SORIANO, ROWENA L.
STA. MARIA, MELENCIO S.
SUALOG, CYRUS VICTOR T.
TAMARGO JR., FRANKLIN P.
TAN, ROWENA NIEVES A.
TEMPROSA, FRANCIS TOM F.
TICMAN, MODESTO A.
TIU, MICHAEL JR. T.
TURINGAN, MARIETTA P.
VALENCIA, EMMANUELLE NICOLE L.
VALENCIA, MARY CLYDEEN L.
VALERA, STEPHEN RUSSELL KEITH G.
VERA, RODERICK P.
VILCHEZ, MARIA GLADYS C.
VILLALUZ, GERARDO A.
VILLANUEVA, GABRIEL S.
VILLENA, JEAN MARIE B.

THE FAR EASTERN
LAW REVIEW

MESSAGE

In this issue of the Law Journal with the theme "Technology and its Impact in the Legal Sphere," we are brought to ponder if it is the law that shapes technology or is it technology that influences law.

Should it be that law is the shaper of technology, we can expect less than what technology intends to improve itself as it is limited by the legal methodologies that draws its existence from ideas that go back in time. If technology shapes the law, we can expect to be unsettled as we see technological developments affect human lives in a way not previously foreseen by the law.

This issue of the Law Journal explores the topics of ownership and creation of digital things, digital technological advancements affecting life in the social media, the classroom, government regulation, and rights enforcement from the lens of who is the shaper of things: Technology or Law.

JOSE MARLON PABITON

Associate Dean

MESSAGE

Editor-in-Chief

Since prehistoric times, tools and technology have always been an essential part in the life of the ordinary man. Civilization and society would not have been possible without technology as it enables the ordinary man to break through and create progress.

Technology has allowed mankind to live through tough times, just like the recent COVID-19 pandemic. It allowed the world to continue moving, despite having to limit physical contact. However, just as how it has its positive effects, it also has its negative effects. Both effects require the legal field to expand, especially to ensure that no lives or human rights are endangered or lost. In this 51st volume, the Far Eastern Law Review provides several theses and articles that expound on this topic at hand: "Technology and its Impact in the Legal Sphere."

In Greek Mythology, we learn of the story of Daedalus and Icarus. Daedalus and his son, Icarus, were imprisoned by King Minos in a labyrinth. To escape, Daedalus created two pairs of gigantic wings that he and his son can use. However, the use of the wings came with a warning: to not fly close to the sun. Unfortunately, Icarus, becoming too enthusiastic of the new tool created, did so. Thus, his wings melted, which ultimately led to his death.

The constant progress of technology in society has always been a factor to the quality of lives that the ordinary man can lead. Like how Daedalus created the wings, it has led man to break through so many barriers and achieve things that are beyond what we have though was the limit. Like the wings that were created, new tools and technology will always be made to tend to the increasing needs and wants of mankind. However, just like how Daedalus had warned his son to not get close to the sun, the use of technology must also be regulated. Else, it would lead to a huge loss, just like Icarus' death. Hence, I hope that through this volume, we can tackle more on how the constant progress in the creation of these "wings" need regulation to protect lives.

I would like to take this opportunity to thank my co-Editor-in-Chief, Josie, our advisor, Atty. Nicole Valencia, our Dean, Atty. Melencio Sta. Maria, Associate Dean Jose Marlon Pabiton, and my co-EB members, Emille, Mara, Angel, Bianca, and Nicole. Vol. 51 would not have been possible without any of you. Thank you for all the support and patience.

JEZREEL Y. CHAN
Co-Editor-in-Chief

MESSAGE

Editor-in-Chief

Another year has passed, with the Philippines still living under the conditions brought by the Covid-19 pandemic. But one thing is for sure, a lot has changed for the Philippines since the government imposed the first lockdown last March 2020.

Businesses, big or small, have since then adapted to the change in times by relying on digital platforms to help them survive. The government, with its old and traditional ways, was forced to find ways to become more efficient with how they transact with the people. Even the Courts saw a major change, conducting online hearings of cases here and there. Indeed, the pandemic was no excuse for the Filipinos to put their life on hold. Everyone clamored for normalcy to come back in one form or another.

With so many changes happening around us and with our ever-growing reliance on digital platforms, it does not come as a surprise that many legal questions and issues have surfaced. For the 51st Volume of the Far Eastern Law Review, this edition showcases different articles which focus on the theme of "Technology and Its Impact in the Legal Sphere. "

For the final time, I would like to thank my fellow Editorial Board Members for the 50th and 51st Volumes. It has been both a great honor and privilege to work alongside wonderful women. More importantly, I would like to thank my co-Editor-in-Chief, Jezreel Chan, for being the heart and soul of the Far Eastern Law Review for the 50th and 51st Volumes. Your dedication and hard work do not go unnoticed, and we all thank you for your service.

JOSELLE MARIANO
Co-Editor-in-Chief

TABLE OF CONTENTS

THE FAR EASTERN LAW REVIEW

The Annual Publication of the Institute of Law

THESES

BY AI: AUTHORSHIP AND OWNERSHIP OF COPYRIGHT IN AI-GENERATED WORKS

Atty. Stephanie Gail R. King

Abstract: Given the growing comfort of Artificial Intelligence (AI) use in everyday life, coupled with the application of deep reinforcement machine learning in AI programs, an updating of current intellectual property laws should be considered.

INTRODUCTION

Intellectual Property (IP) laws such as copyright laws were crafted based on a previous reality that creative works could only be made by a human author. Nowadays, artworks, novels, and music, among others, can be made, not just by humans, but also by machines. This becomes problematic in the field of copyright law as works made by non-human authors are outside the scope of protection of a work which is, otherwise, covered by copyright protection. Losing this protection would disincentivize, not only the infusion of creativity in the development of the Fourth Industrial Revolution, but also the development of art expression itself as artists continue to be restricted by the bounds of a past age. The blurring of the hardline between technology as tools used by human creators of art, and technology as the actual creator of the art, is forcing society to re-define its current perception of who or what "authors" or "artists" are – especially in the field of copyright law.

In September 2019, the World Intellectual Property Organization (WIPO) held a meeting discussing policy questions related to the increasing and inevitable overlapping between AI and IP laws. The WIPO Secretariat was tasked to draft a list of issues related to the matter, where issues will be then open for comment from interested parties. One matter tackled in the paper was the issue of authorship of works over AI-generated works.[1] It was clearly stated in the paper that "AI applications are capable of producing literary and artistic works autonomously."[2] The paper was even of the position that current copyright laws tend to favor "human creativity over machine creativity[;]" thus, effectively stating that machines could autonomously make a work considered to be creative.

There continues to be an insistent demand for current copyright laws to be updated in the face of ever-evolving technology. Philippine IP laws should adapt in order to uphold the purpose of copyright law and prevent a situation that leaves AI-generated works to be unprotected and discriminated against other works covered by copyright protection.

ARTIFICIAL INTELLIGENCE

[1] WIPO Secretariat, WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI) Second Session, https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_ge_20/wipo_ip_ai_2_ge_20_1.pdf).
[2] *Id.*

A. DEFINING ARTIFICIAL INTELLIGENCE

AI is defined as "the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing programs endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience."[3] AI can also be defined as "the study and design of intelligent agents where an intelligent agent is a program that perceives its environment and takes actions which maximize its chances of success."[4] The scope of AI research focuses on different components of intelligence, such as perceiving, learning, problem-solving, and speaking.[5] These are developed via machine learning. An example of this learning can be seen in the works of Tom White, a computational design and creative AI lecturer in New Zealand. He created a drawing program that allows neural networks to express their versions of categories or objects that they have been trained to recognize.[6]

B. HOW ARTIFICIAL INTELLIGENCE WORKS

a. EXPERT SYSTEMS

Learning in expert systems cannot be done by the program itself as it is bound by the rules and the flow of the expert program. Thus, "learning" for expert systems can only occur if the set rules in the program are changed by a human user. The case is different when it comes to AI capable of machine learning – a program that uses neural networks. For this type of program, learning occurs within the program itself due to the nature of its reasoning process. Neural networks' reasoning uses associations among patterns, which can make it hard to predict the results it will produce. Meanwhile, expert systems only use symbolic processing that is quite straightforward as it follows the path that human users already pre-set. Hence, instead of expert systems, neural networks are used in robotics and image/speech/temporal processing as these fields require machine learning.[7]

b. MACHINE LEARNING

"Machine learning research is part of [the] research on artificial intelligence, seeking to provide knowledge to computers through data, observations, and interacting with the world.

[3] B.J. Copeland, Artificial intelligence, available at https://www.britannica.com/technology/artificial-intelligence (last accessed August 04, 2020).
[4]Artificial Intelligence: Introduction citing Stuart Russell and Peter Norvig, ARTIFICIAL INTELLIGENCE, A MODERN APPROACH. Third Edition. Pearson Education, available at http://aima.cs.berkeley.edu/, available at https://courses.edx.org/asset- v1:ColumbiaX+CSMM.101x+3T2019+type@asset+block@AI_Lecture1_sm.pdf (last accessed August 04, 2020).
[5] Copeland, *supra* note 3.
[6] Tom White, available at https://aiartists.org/tom-white (last accessed August 04, 2020).
[7] Marian S. Kurzyn, Expert Systems and Neural Networks: A Comparison, available at https://www.computer.org/csdl/proceedings-article/annes/1993/00323038/12OmNz5apLv (last accessed August 05, 2020).

That acquired knowledge allows computers to correctly generalize to new settings."[8] Machine learning is basically "pattern recognition masquerading as understanding."[9] This recognition is made possible through the use of statistical techniques that translate the data fed into the AI program. Through this kind of learning, step-by-step programming need not be done by humans for the AI to evolve into a higher level of mastery for a given task.[10]

c. NEURAL NETWORKS

In the quest to create a more advanced form of AI, society developed neural networks. Neural networks in machines are fashioned to operate the same way that brain neurons operate: smart neural pathways are created through a process of trial and error wherein the machine learns more data as it undergoes more training.[11] Like the human brain, a program equipped with a neural network strives to recognize patterns in the data inputted in them by finding and creating connections in these data.[12]

CURRENT STATUS OF AI DEVELOPMENT

Due to the abundance of unlabeled data that is being collected in society nowadays, deep learning has had an easier time developing.[13] However, the type of AI that will only realistically develop in the near future would be Narrow AI. Most, if not, all AI researchers, are of the position that society is nowhere near close to having General AI programs a reality.[14] Narrow AI development, however, gets more and more normalized in everyday life. From Siri, Spotify playlists, face recognition, Netflix recommendations, etc., Narrow AI's development will continue to become more specialized and incorporated into daily use.

C. GENERATIVE ART

With the advent of AI in everyday technology, it is inevitable for the realms of AI and art to collide. Nowadays, society has introduced Generative Art. This type of art "refers to any work that is created by a program with some level of autonomy, or work that can function with

[8] Daniel Faggella, What is Machine Learning? available at https://emerj.com/ai-glossary-terms/what-is-machine-learning/ (last accessed August 05, 2020).
[9] Vox. "How smart is today's artificial intelligence?" YouTube, uploaded by Vox, 19 December 2017, https://www.youtube.com/watch?v=IJKjMIU55pE.
[10] Brodie O'Carroll, What are the 3 types of AI? A guide to narrow, general, and super artificial intelligence, available at https://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible (last accessed August 05, 2020).
[11] Leah Davidson, Narrow vs. General AI: What's Next for Artificial Intelligence? available at https://www.springboard.com/blog/narrow-vs-general-ai/ (last accessed August 05, 2020).
[12] Shlomit Yanisky-Ravid, Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3a Era—The Human-Like Authors are Already Here—A New Model, available at https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1199&context=lr (last accessed August 04, 2020).
[13] A Beginner's Guide to Deep Reinforcement Learning, available at https://pathmind.com/wiki/deep-reinforcement-learning (last accessed August 12, 2020).
[14] Federico Berruti, Pieter Nel, and Rob Whiteman, An executive primer on artificial general intelligence, available at https://www.mckinsey.com/business-functions/operations/our-insights/an-executive-primer-on-artificial-general-intelligence (last accessed August 05, 2020).

little intervention from the artist."[15] The artist "designs the program using language rules, machines, algorithms, or genetic sequences to generate a final product that serves as the work of art."[16] Before this art was associated with the use of AI General Adversarial Networks (GANs),[17] it is important to do a quick run-through of the different intersections of technology and art in different fields of art.

In the earlier days of AI development, AI in art was primarily used as a tool for people to create art. Like a chisel to a sculptor, AI helped people in their creation of art. As it continued to develop, AIs have shifted from being mere tools to create to being the creators themselves.

a. AI AS A TOOL TO CREATE

A good example of AI used as a tool for the creation of artwork would be the use of programs, such as Adobe Photoshop and Microsoft Paint. People would say that it gets harder to distinguish whether technology is merely a digital tool used by people to create or if such technology is the one creating the art itself. The author posits that the more accurate statement would be that people are afraid to face the reality that technology can and is already making art based on its own "understanding."

b. AI OUTPUT FROM MACHINE LEARNING

General Adversarial Networks

The commonly used model for AI-generated works under the category of "Generative Art" is the General Adversarial Networks (GANs). GANs are models which combine unsupervised machine learning combined with deep learning methods.[18] As a way of explaining how GANs work, an analogy provided by Machine's Creativity is illustrative:

> Let's assume you have two children in a room, and you want them to learn how to draw cats, but without direct involvement from you. So[,] you give the first child, let's call him a "discriminator," an album full of drawings of cats, with different breeds and sizes. And you give the second child, let's call him a "generator," random dots and shapes. So[,] the generator hands the discriminator a drawing of his random album. Now you ask the discriminator to learn how to classify cats from non-cats and give his feedback to the generator by comparing his work against the cats' album. The generator, wanting to excel in his drawing skills hears the feedback and slightly modifies the random drawing to look more similar to whatever

[15] Generative Art: Origins, Artists, and Exemplary Works, available at https://www.invaluable.com/blog/generative-art/ (last accessed August 12, 2020).
[16] *Id.*
[17] This will be discussed more in the next section.
[18] Jason Brownlee, A Gentle Introduction to Generative Adversarial Networks (GANs), available at https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/ (last accessed August 12, 2020).

> the discriminator is describing. He then asks the discriminator to reevaluate his work again.[19]

Software Art and Generative Art present society with another perspective of who or what an artist is. There is a shift from the traditional notions of art – the focus of an artist being the output or display of art itself—to a view that the artist is involved in the programic process of programming. One of the reactions evoked from viewers of Casey Reas's work, Linear Perspective, shared his sentiments on Casey's Software Art:

> I felt I was getting a glimpse of machines' notions of who we are, or were — as if the signal streams were returning their algorithmic image of us for reflection. Paradoxically, these instants of time, sliced from recent media streams, felt far removed from the present, as if only a trace memory remains of the lives we are living.[20]

With this statement, the author puts forth the question: can it be said that programmers in Software Art or Generative Art are the sole authors of the works generated by the AI program? What about the interpretation of the program itself, can this be considered to be "creativity" in the relation to copyright law and protection?

Karthik Kalyanaraman, a member of the curation team for the Nature Morte exhibition for AI-generated art, is of the opinion that computers may actually deserve creative credit for art. He states that machine learning, especially the one used by White, "is similar to the process by which humans learn art, but that our 'mysticism' surrounding the notion of creativity stops us from seeing the parallels."[21] He further states: "If a machine can make humanly surprising, stylistically new kinds of art, I think it is foolish to say well it's not really creative because it doesn't have consciousness."[22]

COPYRIGHT LAW IN THE PHILIPPINES

The source of copyright as a legal right in the Philippine jurisdiction is found in Part IV of the Intellectual Property Code of the Philippines (IP Code). Copyright is not among the terms defined under Sec. 171 of the law. Instead, what is included in the list is the word "author." It refers to the "natural person who created the work."[23] The term "author" is next

[19] Machine's Creativity, Artificial Art: How GANs are making machine creative, available at https://heartbeat.fritz.ai/artificial-art-how-gans-are-making-machines-creative-b99105627198 (last accessed August 12, 2020).
[20] Johanna Drucker, Nostalgia for the Lost Subject in the Work of Casey Reas, *available at* https://lawreviewofbooks.org/article/nostalgia-for-the-lost-subject-of-technology-in-the-work-of-casey-reas/#! (last accessed August 12, 2020).
[21] James Vincent, What algorithmic art can teach us about artificial intelligence, available at https://www.theverge.com/2018/8/21/17761424/ai-algorithm-art-machine-vision-perception-tom-white-treachery-imagenet (last accessed August 12, 2020).
[22] *Id.*
[23] An Act Prescribing The Intellectual Property Code And Establishing The Intellectual Property Office, Providing For Its Powers And Functions, And For Other Purposes (INTELLECTUAL PROPERTY CODE), Republic Act No. 8293, §171.1. (1997).

found in Sec. 171.7 under the definition of "published works" – "works, which, with the consent of the authors, are made available to the public xxx"[24]

The need for the author's consent in this section can be linked to the alternative term used for copyright under the IP Code, which is highlighted in Sec. 177's heading "Copyright or Economic Rights." It provides that copyright or economic rights shall consist of the exclusive right to carry out, authorize or prevent" certain acts related to a work. However, the term "work" is also not among the terms defined under Sec. 171. Instead, it detracts from its general societal definition and gains a legal definition – at least under the IP Code – as "literary and artistic works."[25] It can be found under Sec. 172.1: "Literary and artistic works, hereinafter referred to as 'works', are original intellectual creations in the literary and artistic domain protected from the moment of their creation."[26] Based on this definition, the automatic legal protection attaches to the "work" and not necessarily automatically to the creator of the work. This is enunciated in Sec. 172.2 of the IP Code which shows that "works are protected by the sole fact of their creation, irrespective of their mode or form of expression, as well as of their content, quality and purpose."[27] Moreover, Sec. 178.1 of the IP Code provides that "subject to the provisions of this section, in the case of original literary and artistic works, copyright shall belong to the author of the work." [28] Ownership over the copyright, generally then, belongs to the author of the work.

A. OWNERSHIP VS. AUTHORSHIP

The concept of ownership under Philippine law is found in Art. 427 of the Civil Code, which provides that "ownership may be exercised over things or rights." [29] Ownership in relation to copyright law, is exhibited in two ways: (1) ownership over the copyright; and (2) ownership of the work itself. Ownership over the copyright is provided for under Sec. 178.1, Sec. 178.2, and 178.3. Ownership over the work itself is seen in Sec. 178.4.

Ownership over the copyright still primarily vests in the author, except that: (1) this can be co-owned with another author in cases of works of "joint authorship;"[30] (2) it can be vested with an employer if an employee is the author of a work and it is created "during and in the course of his employment."[31] Even in such situations, however, the author can opt to claim

[24] *Id.* §171.7.
[25] *Id.* §172.
[26] *Id.* §172.1.
[27] *Id*. §172.2.
[28] *Id.* §178.1.
[29] An Act to Ordain and Institute the Civil Code of the Philippines [CIVIL CODE OF THE PHILIPPINES], Republic Act No. 386, art. 427 (1950).
[30] INTELLECTUAL PROPERTY CODE, §178.2.
[31] *Id.* §178.3.

ownership over the copyright as Sec. 178.3(b) provides a clincher – "unless there is an agreement, express or implied, to the contrary."[32]

> The distinction between ownership of the copyright and ownership over the work itself can be seen in Sec. 178.4. This section refers to "commissioned works," which refer to "a work commissioned by a person other than an employer of the author and who pays for it, and the work is made in pursuance of the commission."[33] A commissioned work will belong to the person who pays the author, but this is only for the tangible work itself as the copyright will still remain with the author. Similar to the clincher found in Sec. 178.3(b) though, the author has an option to either keep or give away the copyright. Unlike in the earlier section which allows an implied agreement, the agreement in the case of commissioned works must be written down.[34]

These sections exhibit that generally, copyright belongs solely to the author of the work. However, this does not mean that works are made solely by an author or by two or more authors in cases of "joint authorship." Sec 178.6 reflects the reality that a finished work can be sourced from different authors. This section provides rules on copyright ownership over "audiovisual work." In these kinds of works, the law recognizes that the copyright belongs to the "creators." Such term was used for "the producer, the author of the scenario, the composer of the music, the film director, and the author of the work so adapted."[35]

a. THE CONCEPT OF AUTHORSHIP IN COPYRIGHT LAW

The concept of the author as the protected subject of copyright law dates back to 1709 when the Statute of Anne was created.[36] The press release for the establishment of copyright law then was for the celebration and protection of the creative genius of authors, but the true beneficiaries behind the creation of such laws were the publishers of the copies of the author's work.[37] Despite the apparent promotion of copyright law for artistic creativity, the stronger concept of gaining economic rights over the tangible expression of such creativity or "works" was the central focus of copyright law. The law allowed purchasers to "acquire a general dominion over the imaginative territory of a particular literary or artistic production" – which meant that even the author could be excluded from such territory.[38]

---

[32] *Id,* §178.3(b).
[33] *Id.* §178.4.
[34] *Id.*
[35] *Id.* §178.5.
[36] Oren Bracha, The Ideology of Authorship Revisited: Authors, Markets, and Liberal Values in Early American Copyright, p. 256, *available at* https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5141&context=ylj (last accessed August 13, 2020).
[37] Peter Jaszi, Toward a Theory of Copyright: The Metamorphoses of "Authorship", p. 468, *available at* https://case.edu/affil/sce/authorship/Toward_a_Theory_of_Copyright.pdf (last accessed August 13, 2020).
[38] *Id*. at 478.

This shows at the very onset of copyright protection, the motive of the law itself showed that authorship and ownership over the works could differ. Historians describe the development of copyright law as one that "linked artistic ideas like creativity and originality as a conversion of … 'things of the mind into transferable articles of property…[that] has matured simultaneously with the capitalist system."[38]

Consequently, the Statute of Anne initially vested copyright to authors instead of publishers, even if legislators knew that publishers would eventually assume control.[39] To better understand the intention behind copyright law, a discussion on some of its common theories is in order.

b. COMMON THEORIES ASSOCIATED WITH INTELLECTUAL PROPERTY LAW

When the Statute of Anne was enacted, the prevalent social thinking was "possessive individualism,"[40] which refers to a conception of the individual as essentially, the proprietor of his own person or capacities, owing nothing to society for.[41] This thinking can be linked to one of the four main theories of IP law – the Natural Rights Theory of John Locke. Under Locke's theory, "the first person who employs his or her labor to the resources available [in nature] has the sole right to appropriate it without anyone else's consent."[42] This theory adheres to a premise that everything in nature is owned in common until someone takes it and makes something out of it. However, it would eventually lead to nothing being owned by the people.

The second theory of IP law seeks to remedy this by providing a balance between personal rights and the public welfare. Under the utilitarian theory or the economic incentive theory, IP laws were created in order to spur people to create by fueling them with the incentive of exclusive rights. [43]

If people do not get incentivized by the possibility of exclusive rights, they might get incentivized by the third theory of IP law – the Personality Theory of Property. This theory provides that "intellectual property is an extension of individual personality."[44] It recognizes the tendency people have to self-identify themselves through tangible objects.

---

[38] *Id.* at 467.
[39] *Id.* at 468.
[40] Jaszi, *supra* note 17, at 470
[41] Possessive individualism, *available at* https://understandingsociety.blogspot.com/2011/08/possessive-individualism.html (last accessed August 17, 2020).
[42] Aravind Prasanna, John Locke's Labour Theory: A Justification of IPRs, *available at* http://www.legalservicesindia.com/article/2536/John-Locke%C3%A2%E2%82%AC%E2%84%A2s-Labour-Theory:-A- Justification-of-IPRs.html (last accessed August 19, 2020).
[43] Jeanne C. Fromer, Expressive Incentives in Intellectual Property, *available at* https://law.stanford.edu/wp-content/uploads/sites/default/files/event/265497/media/slspublic/Expressive_Incentives_in_Intellectual_Property_1.pdf (last accessed August 19, 2020).
[44] Intellectual Property, *available at* https://plato.stanford.edu/entries/intellectual-property/ (last accessed August 19, 2020).

The fourth theory is the Personal Identity Theory, also created by Locke. In this theory, Locke enunciates that "personal identity is a matter of psychological continuity." Consciousness or memories of the self is what makes up the self and allows for an identity beyond the body.[39] This type of identity allows the self to exist in different time and settings – even after the expiration of the physical body.

All these theories point to the general purpose of copyright law in incentivizing the continuous creation of literary and artistic works. This singular purpose, however, branches off among the different theories of IP law.

GENERATIVE ART AND COPYRIGHT PROTECTION

AI is defined as a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence, with limited or no human intervention. For the purposes of this paper, AI generally equates to "narrow AI" which is techniques and applications programmed to perform individual tasks.[40] The WIPO also established that "AI-generated" works and works "generated autonomously by AI" are terms that can be interchangeably used in describing works that are made without human intervention. These were contrasted with "AI-assisted" works that involve "material human intervention and/or direction."[41] WIPO established their recognition over the existence of AI-generated works and the existence of creativity in such works, although it has yet to make a final guideline on the copyright treatment over such works. The WIPO has a total of 193 member states, including the Philippines. Some of the WIPO's member-states already have legislation on the copyright treatment of AI-generated works.

Since the Philippine copyright law is based on US copyright law, an examination of the treatment of computer-generated works in the US must be made. Although there is no definite pronouncement in the United States Code over computer-generated works, the Compendium of U.S. Copyright Office Practices (the Compendium), an administrative manual for the US Copyright Office, states that the U.S. Copyright Office "will register an original work of authorship, provided that the work was created by a human being."[42]

[39] Namita Nimbalkar, Ph.D., John Locke on Personal Identity, *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3115296/#:~:text=John%20Locke%20holds%20that%20personal,the%20so ul%20or%20the%20body (last accessed August 19, 2020).

[40] WIPO Secretariat, WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI) Second Session, *available at* https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_ge_20/wipo_ip_ai_2_ge_20_1.pdf (last accessed August 20, 2020).

[41] *Id.*

[42] Overview Technology, Media and Telecommunications Bulletin, Part 2: Can Artificial Intelligence be an Author According to Copyright?, *available at* https://www.fasken.com/en/knowledge/2018/07/can-ai-be-an-author-according-to-copyright/#:~:text=The%20Copyright%20Act%20confers%20ownership%20of%20copyright%20on%20the%20author.&text=As%20a%20result%2C%20the%20ownership,individuals%20or%20persons%2C%20unlike%20inventors. (last accessed August 21, 2020).

However, in February 2020, the US Copyright Office also submitted a comment to the WIPO in response to its September 2019 invitation for interested parties to comment on issues related to intellectual property policies. In its comment, the Office addressed the need for guidelines regarding authorship and ownership of AI-generated works as more of such works are being entered for registration with their Office.[43] Although some countries have current legislation that does not protect AI-generated works, it does not mean that they are closed to discussing amendments to their laws. Similarly, the Philippines should start having dialogue on copyright protection related to AI-generated works.

RECOMMENDATION FOR PHILIPPINE COPYRIGHT OVER AI-GENERATED WORKS

A. WHY THE APPREHENSION IN GRANTING COPYRIGHT PROTECTION OVER SUCH WORKS?

The legal personality of AI becomes an issue in AI-generated works since society is confused as to whom (or to what) authorship needs to be attributed to. In defining AI-generated work, the WIPO declared that such works "refer to the generation of an output by AI without human intervention."[44] Because of this reality, current copyright laws do not cover AI-generated works. The theories of copyright law make an undeniable connection among humans, creative flourishing, and economic incentive. Since these theories are the foundation of copyright law, the reality that creative works are now being generated by AIs means that the whole premise upon which copyright laws are based on needs to be revisited.

With the proposition that AIs can have legal personality like corporations, the author posits that the programmers or other human contributors in the development of the AI program can just be likened to the board of directors of a company – a group of humans behind the creation of the AI ("AI stakeholders").

Assuming that authorship is attributed to AIs, what then is its significance or what is the next step in considering copyright protection over AI-generated works? Authorship under most copyright laws attribute ownership to the authors of the protected work. This, again, is another hurdle in granting authorship over such works to the AI since AIs do not have actual, natural personality. Given that the legal personality of AIs can be likened to juridical personalities granted to corporations, ownership over AI-generated works will then vest to the AI's stakeholders. Why attribute authorship to AIs even if ownership would eventually be given to the AI's stakeholders? The author is of the position that this is necessary as an ode to theories under copyright law that protected works are made by an author who generates an output through creativity. If authorship is attributed to the AI

[43] WIPO Secretariat, *supra* note 16.
[44] *Id.*

stakeholders, it will be equivalent to an admittance that creativity over the generated work was from the stakeholders themselves. The author believes this is erroneous, because the stakeholders' creativity lies in the making of the program used by the AI. Saying that the stakeholders are the ones who gives an input of creativity would be similar to saying that Canon is the one infusing creativity into photos taken by photographers. Of course, this analogy can be said to only be applicable to works made *with the assistance* of an AI, but the author argues that the main idea is the same. What AI stakeholders, particularly the programmers create are not the actual works themselves but the "possibility of creation" associated with the AI program.[45]

B. RECOMMENDATIONS FOR THE PROTECTION OF AI-GENERATED WORK

The author then proposes that ownership over AI-generated works be considered *sui generis* with ownership guidelines separate from those provided under current Philippine legislation. The author proposes the following recommendations for determining ownership over AI-generated works: (1) a proposal inspired from UK copyright laws; and (2) a proposal which likens an AI to an "employee" under Philippine copyright law.

Under the first proposal, the author submits that instead of authorship, ownership of the copyright over such works should be attributed to the one who has control over whether or not the AI can create further works. This discretion for creation will be the determining factor for such ownership. Further guidelines can be implemented in the law in order to prevent the monopoly of AI stakeholders over ownership of the copyright associated with AI-generated works. This will be similar to a scenario wherein a program is sold to a user who uses the program to create works. The copyright therein will belong to the user and not to the person or entity selling the program. This can also be considered fair since the AI stakeholders have already been rewarded through copyright protection over the AI program itself. Thus, the selling of the program already gave them a monetary reward, among other economic rights granted under copyright law.

As to the second proposal, it concerns an application of some Philippine copyright provisions to *sui generis* provisions concerning AI-generated works. Under this proposal, the author recommends the usage of the "work for hire" doctrine under the IP Code in attributing ownership over AI-generated works. The "work for hire" doctrine provides "in the case of work created by an author during and in the course of his employment, the copyright shall belong to: "xxx (b) The employer, if the work is the result of the performance of his regularly-assigned duties, unless there is an agreement, express or implied, to the contrary."[46]

[45] Tuomos Sorjamaa, I, Author – Authorship and Copyright in the Age of Artificial Intelligence, available at https://helda.helsinki.fi/bitstream/handle/10138/166456/sorjamaa.pdf?sequence=3&isAllowed=y (last accessed August 13, 2020).
[46] INTELLECTUAL PROPERTY CODE, §178.3.

In mirroring the objective of the "work for hire" doctrine in generally vesting automatic ownership over employee's works to the employers, the author proposes that AIs be treated as "employees" of the AI stakeholders insofar as the automatic vesting of ownership over such works is concerned. The exception clause, however, will not be retained. For AI-generated works then, the AI stakeholders that created the AI will be considered as the "employers" obtaining ownership of the copyright over the work.

In applying the independent contractor relationship in AI-generated works, the law can view AI stakeholders as independent contractors under the lens of Philippine labor laws. Generally, independent contractors under the IP Code refer to individuals who get commissioned by others, other than their employers, to create a work. In the Philippines, independent contractors are considered the direct employers of employees who perform the task, while the principal is the one who commissions the service. The contract is between the company as an independent contractor and the principal who seeks their service. Applying this to commissioned AI-generated works, the commission contract will be between AI stakeholders and the person who commissions the work. This type of arrangement will allow the person who commissioned the work to obtain ownership over the actual work itself, but the copyright will remain with the AI stakeholders. Consequently, once the AI program is sold to a user and a person commissions such user for an AI-generated art, the user will retain copyright over the work while ownership over the actual work will vest in the person who commissioned the work.

In connecting the two proposals, the author thus recommends that should the AI program be sold to the public, the first proposal would be applied. Should the program not be sold, the second proposal is to be applied. In case of commissioned works, an application of the first or the second proposal is to be made in relation to a provision on the independent contracting of an AI. This kind of proposed legislation has a similar objective with UK's copyright law which vests copyright with "the person by whom the arrangements necessary for the creation of the work are undertaken."[47]

CONCLUSION

The programmers of AI-generated works will not be considered as the authors of such works. Rather, it will vest in AI as the work is a new work made from the AI's own interpretation. Although the creative process of natural persons might not be exactly the same with the creative process used by AIs, it is not so far off to be considered as a process devoid of "creativity." If the WIPO itself recognizes machine creativity, why then must there be a complicated debate on whether or not AIs can be authors and whether or not AI-generated works can be protected under copyright law when indeed AI-generated works can be infused with creativity?

[47] COPYRIGHT, DESIGNS AND PATENTS ACT §9(3), (1998).

> *"Everybody has their own definition of a work of art…I've tended to think human authorship was quite important—that link with someone on the other side. But you could also say art is in the eye of the beholder. If people find it emotionally charged and inspiring, then it is. If it waddles and it quacks, it's a duck.*
>
> *-Richard Lloyd, 2018.*

ABOUT THE THESIS

This was awarded as Best Thesis in 2021 by the Far Eastern University – Institute of Law.

ABOUT THE AUTHOR

Stephanie Gail R. King graduated from Ateneo de Manila University with a degree in BS Legal Management. She graduated from the Far Eastern University – Institute of Law in 2021 and passed the February 2022 bar exam.

THERE'S DEATH, THEN THERE'S ONLINE DEATH: EXPLORING DIGITAL ASSETS AS LEGAL ASSET FOR THE TRANSMISSIBILITY OF A DECEDENT'S DIGITAL ASSETS TO HIS OR HER HEIRS

Atty. Justin Ian M. Manjares

INTRODUCTION

One of the most wasteful by-products of entrepreneurial genius is the withholding or dissolution of digital assets upon a person's death due to "privacy rights." The heirs, while theoretically inheriting properties that have inherent monetary value or those that may significantly be monetized, cannot do so because such properties are being withheld from them. Nowhere is this more apparent than the case of Canadian billionaire Gerald Cotten, fund boss of cryptocurrency company QuadrigaX. Since his death in December of 2018, investors of the said company have been unable to access their funds due to encryption. $190 Million worth of assets may very well have died with him.

Cryptocurrency and modern financial instruments are not the only emerging technologies pushing for innovation in the legal sphere. Intellectual property rights are of great importance as well. In an era of data and robotic automation, works that can only be done by human beings become even more valuable. Ideas become invaluable. Intellectual property rights become even more vital. It seems absurd, then, that ideas may be passed down, but there are legal impediments to allowing an heir to access and make money out of his/her parent's intellectual property. After all, the property is now his/hers.

Imagine Ainsley, a successful independent artist in 2018. He does everything on his computer. He records his music, types his lyrics and manuscripts on Google Docs, saves his ideas on Evernote or other note-taking applications, stores all his files on DropBox and Google Drive, edits his films, releases videos and music on Spotify, Soundcloud, YouTube, and more, communicate through email, manages his finances through online platforms and digital wallets, and interacts with his one-million strong following on various social media pages. This is all possible through a single computer and an internet connection. Now, what if Ainsley suddenly dies in a car crash on the way to a concert? Without a valid will, what happens to all his files, social media pages, online accounts, emails, everything stored online? Do his heirs have a legal right to them?

The possession of digital assets is a new phenomenon. As a byproduct of the integration of technology into one's daily life, a person acquires digital assets almost as much as property as traditionally defined. In brief, digital assets pertain to any form of data stored in a computer, whether online or offline and have a right of use. It is primarily defined as "digitally stored content or an online account owned by an individual." This includes social media accounts, emails, document files, etc. Property, as formulated in the Civil Code, on the other hand, categorizes property into movables or immovables. Digital assets or property, conceivably, do

not fall into either of these two categories. While the Civil Code contemplates intangible property (incorporeal rights), no sufficient scholarly discussion has yet been made expressly exploring the nature of a digital asset.

This study shall endeavor to determine *whether digital assets form part of a decedent's estate and are transmissible to one's heirs as a consequence.* This study shall mainly contemplate the characterization of digital assets and the effect of such characterization to their transmissibility (whether they may be included in the decedent's estate). Thus, the main focus of this thesis is the significance of assets to succession.

DEFINING DIGITAL ASSETS

In the context of assets as part of an estate lawyer and author Brian Sweigman define digital assets as electronic possessions, which may include important information that has both monetary and sentimental value.[1] The problem with his definition is that it suffers from over-breadth. Electronic possessions elude an exact definition. He attempts to qualify the definition by putting forth a social and personal perspective. He states:

> From a social perspective, a digital estate can include virtual property such as e-mails, digital photos, videos, tweets, texts, songs and e-books. As well, a digital estate can include online account information such as passwords, photos and message archives for websites or programs such as Facebook, LinkedIn, bank accounts PayPal and any other account information. Economic or business information such as domain names and online businesses can also be included in an individual's estate as well as benefit programs such as loyalty programs from hotels, air miles or other businesses. From a personal standpoint, pictures, videos, documents stored on electronic devices are included in an individual's digital estate. Any information, material, account information or benefits stored digitally (hereafter, "digital assets"), can be included in a digital estate.[2]

In an article by Professor Jamie Hopkins entitled "Afterlife in the Cloud: Managing a Digital Estate", digital assets were broadly defined as "any electronically stored information" that can be used for both business and social purposes. Business digital assets may be utilized by a business in terms of marketing, payroll, and storing of information, while social digital assets are considered as replacements for traditional assets, just as Facebook and uploaded photos have replaced traditional photo albums. This definition, too, suffers from being too broad. In the context of estate planning, it does not provide sufficient guidelines as to what assets a testator may or may not dispose of in his will.

The United States has recognized the need for a legal regime covering digital assets, concomitantly its transmissibility, and has thus drafted a statutory definition. In 2014, the Uniform Law Commission drafted the Uniform Fiduciary Access to Digital Assets Act (UFADAA). The UFADAA originally defined digital assets simply as "a record that is electronic." As with the definition forwarded by Sweigman, this statutory definition does not adequately identify what qualifies (or what does not qualify) as digital assets.

Apart from exacting a suitable definition, classification is important in probing further into the nature of digital assets. Three different typologies have been proposed by Margaret Van Houten, Noemi Cahn, and Samantha Haworth – a mere listing of assets, classification as

[1] BRIAN W. SWEIGMAN, CATCHING UP TO DIGITAL MEDIA, 33 Est. Tr. & Pensions J. 64, 65 (2013).
[2] *Id.*

to utility, and classification as to data type respectively. Van Houten,[3] being estate planning oriented, simply provides for a list of items that qualify as digital assets. These are:

1. Computers and their content
2. Tablets, smartphones, and their content
3. Social Media
4. Photos and Video
5. Contact Lists
6. Calendars
7. Online Accounts such as Amazon, iTunes, PayPal, Catalog Accounts and the like
8. Online Stores
9. Music
10. YouTube
11. The Electronic Library, Amazon Kindle, iBooks, Barnes & Noble
12. Gaming
13. Electronic Financial Account Records
14. Tax Returns
15. Electronic Medical Records
16. Documents stored in the cloud
17. Emails
18. Blogs
19. Websites[4]

Perhaps the most problematic aspect of Van Houten's listing is that it virtually encompasses every single contact with technology a person has with modern computing.

As opposed to Van Houten, Cahn's typology distinguishes digital assets in terms of their utility. She prefaces by stating that "…relatively little law specifically addresses the inheritance of digital assets. Although there are strong and persuasive arguments that on-line assets should be treated in the same way as brick-and-mortar assets, able to be marshaled by executors and personal representatives, these arguments are just beginning to be developed."[5] She provides for four types of digital assets: (1) personal assets; (2) social media assets; (3) financial assets; and (4) business accounts. While Cahn's typology is metes and bounds more erudite than that of Van Houten, one flaw is the lack of distinction and clarification as to the scope of social media assets. It is unclear whether social media assets include the accounts themselves, or merely the data created through the use of such accounts.

[3] Atty. Van Houten is a member of the Davis Brown Law Firm. She is a senior holder of the tax department and her main area of practice involves estate and tax planning, complex trust and administration matters, retirement planning. Her articles have consistently been cited in the literature of digital assets. See: https://www.davisbrownlaw.com/Margaret-Van-Houten.

[4] Margaret Van Houten, *What Are Digital Assets?*, available at www.davisbrownlaw.com/davis-brown-tax-law-blog-article.aspx?id=1849&Tax Law Blog: What our Estate Planning Clients Need To Know - What are Digital Assets?.

[5] NAOMI CAHN, POSTMORTEM LIFE ON-LINE, 25 Prob & Prop. 36, 36 (2011); "Naomi Cahn is the John Theodore Fey Research Professor of Law at the George Washington University Law School in Washington, D.C." She is also a committee member of the Uniform Law Commission.

Catherine Cates, having examined these previous classifications, finds that the typology proposed by Haworth builds upon these prior formulations. Haworth proposes classification in terms of access information, tangible digital assets, intangible digital assets, and metadata.[6] Haworth's formulation is a refinement of Cahn's. With this typology, digital assets are properly identified and categorized, providing for a competent foundation upon which to build the concepts of ownership rights and obligations, as well as that of transmission. The practical value of this typology is demonstrated through its use in litigation.

Considering the discussion so far, the author shall adhere to the definition of the revised UFADAA, marrying it with the typology proposed by Haworth. It is worth noting that, in general, digital assets hold sentimental and/or monetary value either intrinsically, or when passed down to one's heirs. Heirs may endeavor to monetize sentimental content such as licensing digitally stored photographs (for publishing), creating a posthumous book when the manuscript was found in Dropbox or Google Drive, or even the creating of a memorial through archiving the decedent's emails (in the case of celebrities or other influential figures). Tyler G. Tarney succinctly notes: "society has created tremendous value in the form of digital assets; x x x However, the current complexities in acquiring digital assets at death are increasingly forcing individuals and businesses to forfeit this value."[7]

Using Haworth's typology of digital assets, one can identify and differentiate the various types of digital assets in the hypothetical case of Ainsley. Ainsley's access information would be his login details for all his accounts – YouTube, Facebook, Twitter, Instagram, and the like. Tangible Digital Assets are seen in all his files – recorded music, lyrics, manuscripts, emails, pictures, videos, etc. Intangible Digital Assets are seen in his one-million-strong social media following – Facebook likes and comments, Instagram followers, website profiles, and more. Metadata is stored within Ainsley's tangible digital assets. At its most basic, this is illustrated by the background information of the photos he has taken – when and where they were taken, what camera was used, the file size, and other information describing the file it is housed in.

INADEQUACY OF CURRENT LEGAL REGIMES

In an article that won first place in the Real Property, Trust, and Estate Law 2012 Competition, Chelsea Ray elucidated three main problems that necessitate a regime that

[6] Samantha D. Haworth, Laying Your Online Self to Rest: Evaluating the Uniform Fiduciary Access to Digital Assets Act, 68 U. MIAMI L. REV. 535, 537 (2014); Samantha Haworth is a member of the Florida Bar, and her article, has been consistently and abundantly cited in the literature on digital assets since its publication by the Miami Law Review.

[7] Capel, *supra* at note 28, at 1214; Tyler G. Tarney is a litigator for Gordeon&Rees, and former Justice of the Sixth Circuit United States Court of Appeals. He graduated summa cum laude at the Capital University Law School, and was also the executive content and business editor of the Capital University Law Review.

dictates the characterization and handling of digital assets upon death.[8] These are post-mortem identity theft, content theft, and leaving such assets adrift in cyberspace.

First, when an individual dies, there exists a vacuum of ownership and control of one's digital assets. This presents a ripe opportunity for unscrupulous individuals to take on the identity of the deceased, employing several modi to obtain money through identity theft.

Second, in the same vein as online identities become especially vulnerable upon the death of the account holder, so too are works fixated online. Blogs and other forms of web content are susceptible to theft and copyright infringement.[9] Blogs and other forms of web content are protected by copyright laws – from the moment of fixation in the United States, and the moment of creation in the Philippines.[10] Thus, when a person exploits the works of a deceased individual, copyright infringement is committed to the detriment of the value of the estate.[11]

Lastly, "an act dealing specifically with the disposition of digital assets and accounts after death would provide personal representatives with guidelines for handling digital assets and accounts and would also give estate planners a starting point for dealing with the digital assets of clients."[12]

By providing a property regime governing digital assets, the law will be able to keep up with technological advancements. The law on succession provides for rules on the transfer of property that become operative immediately upon death because the law abhors a vacuum in ownership. The same should be said about digital assets. In terms of testate succession, a digital asset property regime allows decedents and their lawyers to be properly guided as to whether provisions of a will [estate plans] are in accordance with the law, data privacy, cybercrime, and the UFADAA in particular. In terms of intestate succession, a digital asset property regime considers whether or not they are transmissible upon death, why, and how.

A. THE PROBLEM WITH PRIVACY

The strong opposition of internet companies (ISPs) to the UFADAA reveals one overarching concern: privacy. Horton, citing Cahn's contribution to the Vanderbilt Law Review Symposium on the Role of Federal Law in Private Wealth Transfer, points out that the ISP's principal concern is the 1986 Stored Communications Act (SCA).[13] Section 2701 of the

[8] CHELSEA RAY, TIL DEATH DO US PART: A PROPOSAL FOR HANDLING DIGITAL ASSETS AFTER DEATH, 47 Real Prop. Tr. & Est. L.J. 583, 587 (2013).
[9] *Id.* at 593.
[10] An Act Prescribing the Intellectual Property Code and Establishing The Intellectual Property Office. Providing for its Power and Functions, and for Other Purposes (Intellectual Property Code), Republic Act No. 8792, §172 (1997); U.S. Copyright Act, 17 U.S.C. § 102(a) - Subject Matter of a Copyright.
[11] In the United States, copyrights may be transferred by any means of conveyance - by will or as personal property in intestate succession; see: 17 U.S.C. § 201(d) (2006).
[12] Ray, *supra* at note 8, at 595.
[13] David Horton, The Stored Communications Act and Digital Assets, 67 Vand. L. Rev. 1729, 1730 (2014).

SCA criminalizes unauthorized access to electronic communications, presenting a seemingly nasty glitch for fiduciaries attempting to marshal a decedent's digital assets. Section 2702 bars ISPs from disclosing a customer's private data without her "lawful consent." Noting that the SCA predates the rise of email, let alone the phenomenon of a valuable Twitter account, Cahn argues that the statute should not govern fiduciaries.[14]

The offense defined in Section 2701 is predicated on unauthorized access. It penalizes anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided or who exceeds an authorization to access…and thereby obtains, alters, or prevents authorized access to a[n]…electronic communication while it is in electronic storage."[15] Having been created in the 1980s, data was all offline and stored on local drives. Section 2701, in this context, pertains to the physical intrusion of a stranger into one's personal digital assets. Fiduciaries are reluctant to access a decedent's accounts because of the sweeping penalization. "Logging onto another's email account without permission" is within the ambit of Section 2701.[16] For fiduciaries, the problem is what constitutes sufficient permission. Would a decedent simply leaving his access information be sufficient? Or should it necessarily be provided for in the will? Is naming a digital executor sufficient to grant permission to access? Intestacy adds an even bigger wrinkle. The issue most specifically posed here is the lack of standards for sufficiency in indicating the testator's intention (whether naming a digital executor is enough, and grants sweeping authority over all his digital assets) or inferring the decedent's wishes on how to handle the assets he has left behind.

Section 2702 proves to be even more of a problem as it effectively bars ISPs from disclosing the contents of a digital account. Emails, messages, or images cannot be disclosed without the user's lawful consent.[17] Just like Section 2701, though, it would be difficult to properly define the standards of lawful consent in the context of death and succession.

In the Philippines, Section 2701 may correspond to the Cybercrime Prevention Act of 2012.[18] Meanwhile. Section 2702 corresponds to the Data Privacy Act of 2012.[19] Section 4(a)(1) of the Cybercrime Prevention Act punishes "access to the whole or any part of a computer system without right."[20] Access is defined as referring to the "instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network."[21]

---

[14] *Id.*
[15] *Id* at 1731.
[16] *Id.*
[17] *Id* at 1735.
[18] An Act Defining Cybercrime, Providing for The Prevention, Investigation, Suppression And The Imposition Of Penalties Therefor And For Other Purposes (Cybercrime Prevention Act of 2012), Republic Act 10175 (2012).
[19] An Act Protecting Individual Personal Information in Information And Communications Systems In The Government And The Private Sector, Creating For This Purpose A National Privacy Commission, And For Other Purposes (Data Privacy Act of 2012), Republic Act No. 10173 (2012).
[20] Cybercrime Prevention Act of 2012, §.4.
[21] *Id*, §.2.

Indeed, these concerns are not unfounded and provide for the very rationale as to why wholesale classification of digital assets as property of the decedent is ill-advised. Distinctions between them are more than warranted. If public and private law are to truly respect the wishes of the decedent, then these privacy concerns must be adequately addressed.

B. TERMS AND CONDITIONS - THE CONTRACT APPROACH

Apart from privacy issues relating to ISP and fiduciary liability, in the absence of a legal regime, digital assets are governed by the disparate Terms and Conditions (TOC) of various ISPs. There is no default rule. The disparate TOCs reflect varying approaches and goals of each provider accounting for the differences in the type of content at issue.

The first issue pertaining to TOCs relates to their binding effect on the deceased account user. Arguments have been made that TOCs are contracts of adhesion, rendering said terms inoperative. While it is true that TOCs qualify as contracts of adhesion, as in Philippine Law, it does not necessarily equate to the voiding of the contract. Several decided cases have somewhat put a closure on this issue. These cases provide for the validity of "click-wrap" and "browse-wrap" agreements. Clickwrap or shrinkwrap agreements are TOCs where a website or service requires a user to click "Agree" or "Continue" before any form of content on the website concerned may be used. A browse-wrap agreement, on the other hand, is an agreement where the TOCs are found in a hyperlink which must be clicked and viewed before agreeing to the terms.

The author, however, considers another view. Precisely because TOCs are contracts of adhesion, they must be strictly construed against the party drafting it and, in relation to the widespread and almost necessary use of social media and other online services, users would agree to the terms regardless of whether they have reservations to the same.

THE CONCEPT OF PROPERTY

A. PROPERTY UNDER THE CIVIL CODE

Property, as a concept, is economic in nature – "a mass of things or objects useful to human activity and which are necessary to live, for which reason they may one way or another be organized and distributed, but always for the use of man."[22] On the other hand, the concept of property must be distinguished from the *right to property*. Tolentino defines the right to property as "the juridical tie by virtue of which a person has the exclusive power to receive or obtain all the benefits from a thing, except those prohibited or restricted by law or by the rights of others."[23] A further distinction must be made between the *right to property* and *ownership*.

[22] ARTURO M. TOLENTINO, COMMENTARIES AND JURISPRUDENCE ON THE CIVIL CODE OF THE PHILIPPINES: Property 1 (1992 ed.); also see: Paras, *supra* at note 8, at 1; where he defines property as "an object, is that which is, or may be, appropriated".
[23] *Id* at 1.

While the right to property emphasizes the *vinculum juris*, *ownership* refers to the mass of rights over the thing.[24] Nonetheless, Tolentino explains that the difference is more historical than actual, and that the two terms are used interchangeably. [25]

Things are all objects that exist and can be of use to man, while property means all those that are already appropriated or are in the possession of man.[26] In effect, property becomes a conceptual subset of things, where the latter refers to those that are capable of being possessed, and the former refers to those already possessed and are found in man's patrimony.[27] From a juridical standpoint, the concept of things holds a more specific meaning. It is restricted to objects that can be of use to man (utility) – used for the satisfaction of human needs…even if it be intangible such as a right.[28] Things are considered property in a juridical sense when they are appropriated, but it is not necessary that the thing has an owner. It is already sufficient that it has been appropriated. [29]

Article 414 of the Civil Code uses the terms things and property interchangeably. The Civil Code contemplates property as things that are already possessed by man, and those that are capable of being possessed.[30] Hence, the requisites for the judicial recognition of a property or thing are:

(1) Utility, or the capacity to satisfy human wants.

(2) Individuality and substance, or separate and autonomous existence. The materials composing a thing are not things themselves. Physical unity often determines individuality.

(3) Susceptibility of being appropriated. Hence, those which cannot be appropriated because of their distance, depth, or immensity, cannot be considered as things; for instance, the sun, the stars, the ocean, the core of the earth, etc. Diffused forces of nature in their totality cannot be considered juridically as things such as light, rain, etc.; but they can be so considered if they can be appropriated in parts, such as electricity.[31]

It is also important to factor in the element of control, as held in a case before the Court of Appeals, holding that fish still swimming cannot be considered property until they are caught. "Until they are caught and safely deposited in a boat, a fisherman may not be considered the owner or to have control over them."[32] Observably, it is this element of control that most visibly demonstrates the right to property, the *vinculum juris* that an owner has over

[24] *Id.*
[25] Tolentino, s*upra* at note 91, at 1 citing 2 Valerde 34-35, 58-62.
[26] *Id.*
[27] *Id* at 2.
[28] *Id*.
[29] *Id*.
[30] *Id*.
[31] *Id* at 3 citing 1 Castan 256-258; Muñoz, p. 174; also see: Paras, *supra* at note 8, at 4.
[32] Tolentino, *supra* at note 91 at 3 citing Alvarado vs. Basa, Off. Gaz. Supp., October 11, 1941, p. 273.

his property. Likewise, rights as relations may also be recognized as property. In a juridical sense, property not only includes material objects but also intangibles such as rights.[33] However, it must be noted that what is being referred to here is that of relations, and not objects per se.[34] The further qualification must be made that only patrimonial rights may be juridically considered as things.[35]

B. THE CONCEPT OF AND LAWS ON INTELLECTUAL PROPERTY

Intellectual Property refers to "those property rights which result from the physical manifestation of original thought."[36] Still, mere ideas and mental conceptions are not protected by intellectual property law.[37] In order to be afforded protection, it must first be transformed into something tangible. In the Philippines, protection is afforded from the moment of creation: "When creations of mind are put in tangible form, however, there is [an] appropriate subject of property that is protected by the law."[38] Thus, apart from the Intellectual Property Code, the 1987 Constitution and the Civil Code provide for a principal anchor in the provision, exposition, and protection of intellectual property rights. Apart from the Intellectual Property Code, the 1987 Constitution and the Civil Code provide for a principal anchor in the provision, exposition, and protection of intellectual property rights.

Article XIV, Section 13 of the Constitution provides that:

> The State shall protect and secure the exclusive rights of scientists, inventors, artists, and other gifted citizens to their intellectual property and creations, particularly when beneficial to the people, for such period as may be provided by law.[39]

Observably, the Constitution provides for the definition and qualifications of copyright. A copyright is defined as " a) The exclusive right (or rights) of an author to the work of his authorship; b) For the recognition of a species of property categorized as intellectual that includes the output of creativity and genius; c) That intellectual property rights are ultimately ordered towards public benefit or welfare; d) That these rights be limited as to their duration.[40]

---

[33] *Id* at 4-5.
[34] *Id* citing 3 Manresa 11.
[35] *Id* at 5.
[36] *Id* citing Ballentine's Law Dictionary, 3d Ed.; [Intellectual Property Code] § 4 defines intellectual property according to its composition. Section 4 provides - *Definitions*. - 4.1. The term "intellectual property rights" consists of:

a) Copyright and Related Rights;
b) Trademarks and Service Marks;
c) Geographic Indications;
d) Industrial Designs;
e) Patents;
f) Layout-Designs (Topographies) of Integrated Circuits; and
g) Protection of Undisclosed Information (n, TRIPS).

[37] Aquino, *supra* at note 117, at 1.
[38] *Id* at 2 citing 63A Am Jur 3d, Property, §5.
[39] PHIL CONST. art. XIV, §13.
[40] Aquino, *supra* at note 117, at 4-5.

Article 721 of the Civil Code meanwhile establishes the rule on ownership of intellectual property, to wit:

> By intellectual creation, the following persons acquire ownership:
>
> (1) The author with regard to his literary, dramatic, historical, legal, philosophical, scientific, or other work;
>
> (2) The composer, as to his musical composition;
>
> (3) The painter, sculptor, or other artist, with respect to the product of his art;
>
> (4) The scientist or technologist or any other person with regard to his discovery or invention.[41]

Ownership vests through intellectual creation. Thus, a simple mechanical reproduction, copy, or repetition does not vest a person with ownership or title as regards such works. More relevant to the discussion on digital assets, the law recognizes the rights of ownership upon intellectual creation, prior to and without the need for any formality.

C. COPYRIGHTS

Section 172.1 of the Intellectual Property Code[42] and Article 4, paragraph 2 of the 1948 Berne Convention[43] establish that a right subsists from the moment of creation.[44] No formality is required for the protection of the law. It is enough that an idea has been expressed in tangible form. For a work to be afforded copyright protection, it must meet the twin requirements of originality and expression.[45] If a Haiku – a poem short enough to be memorized – for example, is created by an individual but never written nor expressed in whatever form, and only stays in the mind of the creator, it cannot be afforded copyright protection. Section 172.2 makes it clear that an idea need not be expressed in a specific form to be subject to copyright protection. It states: "protection vests by the sole fact of their creation irrespective of their mode or form of expression, as well as their content, quality, and purpose."[46]

---

[41] An Act to Ordain and Institute the Civil Code of The Philippines, (CIVIL CODE), Republic Act No. 386, art. 721, (1950).
[42] An Act Prescribing the Intellectual Property Code And Establishing The Intellectual Property Office, Providing For Its Powers And Functions, And For Other Purposes (INTELLECTUAL PROPERTY CODE), Republic Act No. 8293, §172.1 (1997).
[43] Berne convention for the protection of literary and artistic works, of September 9, 1886, completed at Paris on May 4, 1896, revised at Berlin on November 13, 1908, completed at Berne on March 20, 1914, revised at Rome on June 2, 1928, revised at Brussels on June 26, 1948, and revised at Stockholm on July 14, 1967, 4 U.N.T.C. 2 [hereinafter Berne Convention].
[44] Aquino, *supra* at note 117, at 15.
[45] *Id* at 16.
[46] *Id at 17 citing Intellectual Property Code, § 172.2.*

Copyright-protected works may be classified as either original[47] or derivative[48] as specified by Sections 172 and 173 of the Intellectual Property Code. A work is protected by copyright from the moment of creation[49] subject to several statutory limitations.[50] It subsists during the lifetime of the author, starting however, a copyright is not deemed as assigned or transferred *inter vivos*, "in whole or in part, unless there is a written indication of such intention."[51] Most importantly, however, is the individuality or separability of the concept of traditional property and intellectual property, while both being present in a single "thing." Section 181 provides:

> Copyright and Material Object. - The copyright is distinct from the property in the material object subject to it. Consequently, the transfer or assignment of the copyright shall not itself constitute a transfer of the material object. Nor shall a

[47] Intellectual Property Code, § 172. *Literary and Artistic Works*. - 172.1. Literary and artistic works, hereinafter referred to as "works", are original intellectual creations in the literary and artistic domain protected from the moment of their creation and shall include in particular:

(a) Books, pamphlets, articles and other writings;
(b) Periodicals and newspapers;
(c) Lectures, sermons, addresses, dissertations prepared for oral delivery, whether or not reduced in writing or other material form;
(d) Letters;
(e) Dramatic or dramatico-musical compositions; choreographic works or entertainment in dumb shows;
(f) Musical compositions, with or without words;
(g) Works of drawing, painting, architecture, sculpture, engraving, lithography or other works of art; models or designs for works of art;
(h) Original ornamental designs or models for articles of manufacture, whether or not registrable as an industrial design, and other works of applied art;
(i) Illustrations, maps, plans, sketches, charts and three-dimensional works relative to geography, topography, architecture or science;
(j) Drawings or plastic works of a scientific or technical character;
(k) Photographic works including works produced by a process analogous to photography; lantern slides;
(l) Audiovisual works and cinematographic works and works produced by a process analogous to cinematography or any process for making audio-visual recordings;
(m) Pictorial illustrations and advertisements;
(n) Computer programs; and
(o) Other literary, scholarly, scientific and artistic works.

[48] Intellectual Property Code, § 173. *Derivative Works*. - 173.1. The following derivative works shall also be protected by copyright:

(a) Dramatizations, translations, adaptations, abridgments, arrangements, and other alterations of literary or artistic works; and
(b) Collections of literary, scholarly or artistic works, and compilations of data and other materials which are original by reason of the selection or coordination or arrangement of their contents. (Sec. 2, [P] and [Q], P.D. No. 49)

§173.2. The works referred to in paragraphs (a) and (b) of Subsection 173.1 shall be protected as new works: Provided however, That such new work shall not affect the force of any subsisting copyright upon the original works employed or any part thereof, or be construed to imply any right to such use of the original works, or to secure or extend copyright in such original works. (Sec. 8, P.D. 49; Art. 10, TRIPS)

§174. *Published Edition of Work*. - In addition to the right to publish granted by the author, his heirs, or assigns, the publisher shall have a copyright consisting merely of the right of reproduction of the typographical arrangement of the published edition of the work. (n)

[49] INTELLECTUAL PROPERTY CODE, §172.

[50] The Intellectual Property Code, as a whole, in essence defines the statutory limitations on intellectual property. However, the author wishes to single out several relevant provisions that are readily observed in modern society, especially digital assets.

[51] *Id.*

transfer or assignment of the sole copy or of one or several copies of the work imply transfer or assignment of the copyright. (Sec. 16, P.D. No. 49)[52]

D. MORAL RIGHTS POST-MORTEM

A large subset of tangible digital assets falls under copyrightable works. Apart from economic rights,[53] moral rights also come into play. Determining the rights, obligations, and remedies of a deceased's heirs or legal personal representative in light of moral rights is crucial in understanding how copyrightable tangible digital assets are treated post-mortem.

The Intellectual Property Code provides for "1) the right of attribution (*droit à la paternité*); 2) the right to alter the work before its publication, or withhold the work's publication (*droit de retrait ou de repentir, droit de divulgation*); 3) the right to restrain the use of the artist's name with respect to any work not created by the artist, or to a distorted version of his or her work; and 4) the right of integrity (*droit au respect de l'oeuvre*)."[54] Section 193 states:

> Sec. 193. Scope of Moral Rights. - The author of a work shall, independently of the economic rights in Section 177 or the grant of an assignment or license with respect to such right, have the right:
>
> 193.1. To require that the authorship of the works be attributed to him, in particular, the right that his name, as far as practicable, be indicated in a prominent way on the copies, and in connection with the public use of his work;
>
> 193.2. To make any alterations of his work prior to, or to withhold it from publication;
>
> 193.3. To object to any distortion, mutilation or other modification of, or other derogatory action in relation to, his work which would be prejudicial to his honor or reputation; and
>
> 193.4. To restrain the use of his name with respect to any work not of his own creation or in a distorted version of his work.[55]

Section 198 of the Intellectual Property Code further provides for the term of the rights granted. While the exercise of moral rights is straightforward during the author's lifetime,

---

[52] INTELLECTUAL PROPERTY CODE, §181.
[53] The twin treaties of WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) further expand the rights granted under the Berne Convention; World Intellectual Property Organization, and United States. 1997. WIPO Copyright Treaty (WCT) (1996) and WIPO Performances and Phonograms Treaty (WPPT) (1996): message from the President of the United States transmitting World Intellectual Property Organization Copyright Treaty and the World Intellectual Property Organization Performances and Phonograms Treaty, done at Geneva on December 20, 1996, and signed by the United States on April 12, 1997. Washington: U.S. G.P.O.
[54] J. Sedfrey Santiago, In Focus: Beyond Copyright: The Moral Rights of Artists, National Commission for Culture and the Arts, *available at* http://ncca.gov.ph/about-culture-and-arts/in-focus/beyond-copyright-the-moral-rights-of-artists/ (last accessed Dec 19, 2018).
[55] INTELLECTUAL PROPERTY CODE, art. 193.

complications inevitably arise once he or she passes away. Unlike economic rights, the conduct of an heir or licensed personal representative is guided by the intention of the deceased author. The mindset is that of allegiance to the author, as opposed to the economic worth of the copyright -protected work.

The complications become apparent when the intentions of the deceased author are difficult to ascertain or conflict with the exercise of economic rights post-mortem.[56] Typified by the cases of Franz Kafka and Vladimir Nabokov,[57] the wishes of authors who leave strict instructions not to publish their works posthumously are not necessarily followed. These are clear examples of moral rights infringement. However, resolving the conflict between post-mortem enforcement and exercise of economic rights *vis-a-vis* moral rights is an entirely different discussion altogether.[58] Simply, the author wishes to point out that both moral and economic rights are operative over copyrightable tangible digital assets.

E. THE CIVIL CODE AND INTELLECTUAL PROPERTY IN RELATION TO DIGITAL ASSETS

Tangible digital assets may incorporate intellectual property or works that are protected by copyright in particular. Subject to any assignment *inter vivos,* the copyright forms part of the decedent's estate, and would naturally be accompanied by the material object, the tangible digital assets.

ISPs unanimously recognize ownership in favor of the account holder in their ISPs. Nonetheless, contractual recognition of ownership does not provide for any discourse as to the true nature of digital assets. Discernibly, this recognition is a manifestation of the *vinculum juris* as defined by Tolentino. Clearly, it is the owner of the tangible digital assets who has the "exclusive power to receive or obtain all the benefits from a thing, except those prohibited or

[56] J. Sedfrey Santiago, *supra* note 54, at 253.

[57] *Id* at 254; "Another notorious example is Franz Kafka's clear direction to his literary executor, Max Brod, to destroy all his unpublished manuscripts, letters and diaries, including the only copies of what are now considered Kafka's masterpieces, The Castle and The Trial. Instead, Brod preserved them all and published some posthumously, gaining some notoriety as editor. Vladimir Nabokov left strict instructions in his will to destroy his unfinished novel The Original of Laura, which he was writing at the time of his death in 1977. However, far from destroying the manuscript, Nabokov's son and executor, Dmitry Nabokov, published The Original of Laura in 2009."

[58] A series of articles by McCrutcheon may serve as a springboard for such discussion. See: McCutcheon, Jani, Death Rights: Legal Personal Representatives of Deceased Authors and the Posthumous Exercise of Moral Rights (August 27, 2015). Intellectual Property Quarterly, Forthcoming, 242, 247, *available* at SSRN: https://ssrn.com/abstract=2652135; McCutcheon, Jani, Dead Loss: Damages for Posthumous Breach of the Moral Right of Integrity (August 15, 2016). Melbourne University Law Review, Vol. 40, No. 1, 2016. *available at* https://ssrn.com/abstract=2824119; McCutcheon, Jani, The Honour of the Dead - The Moral Right of Integrity Post Mortem (August 31, 2015). *available at* https://ssrn.com/abstract=2653508 or http://dx.doi.org/10.2139/ssrn.2653508;

As well as an article by Edwards and Harbinja discussing the role of moral rights in post-mortem privacy: Edwards, Lilian and Harbinja, Edina, Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World (November 10, 2013). Cardozo Arts & Entertainment Law Journal, Vol. 32, No. 1, 2013. *available at* https://ssrn.com/abstract=2267388 or http://dx.doi.org/10.2139/ssrn.2267388.

restricted by law or by the rights of others."[59] When examined together with the laws on intellectual property, the rights granted by and limits of copyright law fall under the phrase "those prohibited by law or by the rights of others."

More rudimentary is that tangible digital assets conform to the three requisites of property under the Civil Code.

Utility – Tangible digital assets are utilitarian by nature. They are the principal media for storing and accessing information on computer devices. Countless computer files and other tangible digital assets are stored on servers online and drives offline for access by a user for the manipulation and preservation of information. Naomi Cahn's typology of digital assets even specifies and classifies the various forms of utility such assets possess.

Individuality – Each tangible asset is distinct. While as a whole, all forms of digital assets[60] are considered software, tangible digital assets may be distinguished from one another. Individual files may be manipulated and stored independently of each other. They may be organized, stored, arranged, and manipulated in a manner similar to traditional forms of documentation.

Susceptibility of being appropriated – Tangible digital assets always trace their genesis to intellectual creation.[61] That is, there is always one person who has put in the effort to create the file or asset in question. Alternatively, a tangible digital asset, prior to being created, may trace its origin to an actual file, such as a book published before the advent of PDFs. As parts of computer software that can be individually manipulated, and the principal author having discretion as regards its distribution, sometimes for a fee, tangible digital assets are clearly susceptible to the appropriations and actions of man.

F. REAL AND PERSONAL RIGHTS OF DIGITAL ASSETS - ISPS AS PLATFORMS, THE CONTRACT OF COMMODATUM

Thus far, what has been established is the real right of an owner over his tangible digital assets. An owner may enforce his rights against the whole world. As to the first requisite, the subject and object in question are the creator or uploader and his tangible digital assets, respectively. Second, it bears reiterating that there is a *vinculum juris* between the creator or uploader and his assets effectively recognized by the TOCs of each ISP. Thus, there is a general obligation for other persons in general, and ISPs in particular, to respect this relation. Lastly, laws have effective actions to protect this relation to some degree. One such law is the Cybercrime Prevention Act of 2012. Section 4 defines the acts that are punishable by law. Section 4(a) is of note. It defines offenses that undermine the confidentiality, integrity, and availability of computer data and systems[62] -- in effect protecting the rights of the owner of

[59] Tolentino, *supra* at *note* 91, at 1.
[60] See: Haworth's classification of digital assets in Chapter 1.
[61] CIVIL CODE, art. 712.
[62] Cybercrime Prevention Act, §4(a).

such assets. Meeting all the requisites for real rights, these are the reasons that the creator or uploader is called the owner of his files.

Additionally, there exists a personal right between the owner and the ISP. Meeting the first characteristic, the owner stands to be the active subject, while the ISP stands to be the passive subject. Because of the TOCs, the ISPs are bound to host, store, make accessible, transmit messages of the owner through their proprietary platforms. Clearly, the provision of cloud services, emails, and the like fall under the prestation of "to do." Second, there is a general obligation on the part of third persons to respect this relation. Third persons must respect the privacy and ownership of the assets stored online (on the ISP's service platform), and owners (as account holders) agree to take measures to preserve the security of their accounts.[63] Third, TOCs require ISPs to make their services readily available to the user and take all necessary measures to safeguard and preserve the data stored on their platform, but will not be liable for lost profits, revenue, data, etc.[64]

The Civil Code defines *commodatum* as a contract where "The bailee in *commodatum* acquires the used of the thing loaned but not its fruits; if any compensation is to be paid by him who acquires the use, the contract ceases to be a *commodatum.* (1941a)."[65]

This shows that a contract of *commodatum* is not on all fours with the TOCs governing intangible digital assets. Article 1935 requires that a contract of *commodatum* is essentially gratuitous. The fact that the services offered by the ISPs, by default, are free to use may qualify it as gratuitous, putting it within the ambit of Article 1935. Yet, after a certain extent, the service

[63] One such stipulated measure is that users agree to keep their access information confidential. Sharing of account name and other necessary login information constitute a violation of the TOCs.

[64] See: Google Warranties and Disclaimers and Liability for Our Services

"We provide our Services using a commercially reasonable level of skill and care and we hope that you will enjoy using them. But there are certain things that we don't promise about our Services…WHEN PERMITTED BY LAW, GOOGLE, AND GOOGLE'S SUPPLIERS AND DISTRIBUTORS, WILL NOT BE RESPONSIBLE FOR LOST PROFITS, REVENUES, OR DATA, FINANCIAL LOSSES OR INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES." *available at* https://policies.google.com/terms?hl=en&gl=US#toc-warranties-disclaimers.

DropBox "Services As Is" and "Limitation of Liability" - We strive to provide great Services, but there are certain things that we can't guarantee. TO THE FULLEST EXTENT PERMITTED BY LAW, DROPBOX AND ITS AFFILIATES, SUPPLIERS AND DISTRIBUTORS MAKE NO WARRANTIES, EITHER EXPRESS OR IMPLIED, ABOUT THE SERVICES. THE SERVICES ARE PROVIDED "AS IS." WE ALSO DISCLAIM ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. Some places don't allow the disclaimers in this paragraph, so they may not apply to you…WE DON'T EXCLUDE OR LIMIT OUR LIABILITY TO YOU WHERE IT WOULD BE ILLEGAL TO DO SO—THIS INCLUDES ANY LIABILITY FOR DROPBOX'S OR ITS AFFILIATES' FRAUD OR FRAUDULENT MISREPRESENTATION IN PROVIDING THE SERVICES. IN COUNTRIES WHERE THE FOLLOWING TYPES OF EXCLUSIONS AREN'T ALLOWED, WE'RE RESPONSIBLE TO YOU ONLY FOR LOSSES AND DAMAGES THAT ARE A REASONABLY FORESEEABLE RESULT OF OUR FAILURE TO USE REASONABLE CARE AND SKILL OR OUR BREACH OF OUR CONTRACT WITH YOU. THIS PARAGRAPH DOESN'T AFFECT CONSUMER RIGHTS THAT CAN'T BE WAIVED OR LIMITED BY ANY CONTRACT OR AGREEMENT. *available at* https://www.dropbox.com/terms2016.

[65] CIVIL CODE, art. 1935; arts. 1936-1952 also provide for other characteristics of *commodatum* - 1. Ordinarily not consumable (must return the exact same thing), 2. Ownership is not transferred to the bailee, 3. Gratuitous by nature, 4. Involves real or personal property, 5. Contract is personal in character, 6. loss is ordinarily suffered by the bailor, 7. contract for the purposes of use or temporary possession, 8. In case of urgent need, bailor may demand the return prior to the expiration of the period.

no longer becomes free, making the contract onerous;[66] and under the Civil Code, the agreement ceases to be a contract of *commodatum* if any compensation is paid by him.[67] Still, a bailor-bailee relationship is more apt, as opposed to a contract of deposit,[68] because ISPs also stipulate that, when applicable, they may use the assets stored on their platforms for purposes that further their operations and goals as a company.[69] In this light, ISPs do not merely store the assets as in a contract of deposit.

G. TRANSFERABILITY OF AND THE DISTINCTION BETWEEN THE COPYRIGHT AND MATERIALITY OF THE OBJECT

A question may be posed regarding the successional transfer of tangible digital assets whose intellectual property belongs to another. Put in question form: What about tangible digital assets whose licenses or copyright belong to another? Section 181 of the Intellectual Property Code provides a clear answer.[70]

This is akin to a physical copy of a book that has been reproduced multiple times. The owner of the book written by another author has ownership over the specific copy of the book, but the copyright remains with the author. The owner of the book and his heirs must respect the copyright of the author. This scenario is no different from a file downloaded online. Downloading produces a duplicate copy of the master file, just like another copy of a book. The copyright is retained by the creator of the file, but the enjoyment of the specific copy, subject to the rules restricting its use, is owned by the person who downloaded it, and in the future, his heirs who come into possession of such files.

Noting that the copyright of the file's transfers to the heir's intestate,[71] it would be a legal absurdity to create a divergence upon successional transfer between the copyright and the very thing (material object) that encapsulates it. If the intellectual property is inheritable, then

[66] If the amount of free storage is exceeded by the user, the user must pay for the storage on a monthly or annual basis.
[67] CIVIL CODE, art. 1935.
[68] Civil Code, art. 1962. A deposit is constituted from the moment a person receives a thing belonging to another, with the obligation of safely keeping it and of returning the same. If the safekeeping of the thing delivered is not the principal purpose of the contract, there is no deposit but some other contract. (1758a); A deposit is principally for the purpose of safekeeping and is generally gratuitous. It may be onerous if there is an agreement that it be so, or the depositary is engaged in the business of storing goods.
[69] See: Google Terms of Service "When you upload, submit, store, send or receive content to or through Google Drive, you give Google a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our services, and to develop new ones. This license continues even if you stop using our services unless you delete your content. Make sure you have the necessary rights to grant us this license for any content that you submit to Google Drive." *available at* https://www.google.com/drive/terms-of-service/ (last accessed August 15, 2018).

[70] INTELLECTUAL PROPERTY CODE, §181. *Copyright and Material Object*. - The copyright is distinct from the property in the material object subject to it. Consequently, the transfer or assignment of the copyright shall not itself constitute a transfer of the material object. Nor shall a transfer or assignment of the sole copy or of one or several copies of the work imply transfer or assignment of the copyright. (Sec. 16, P.D. No. 49).
[71] *Id*, §180-181.

so should the object where it is embodied. However, if the copyright belongs to a person other than the decedent, then an uncoupling would be viable and warranted. Upon transfer, the heirs only acquire the *vinculum juris* to the asset itself, while the intellectual property remains with the creator or his assigns.

H. NEW TECHNOLOGICAL DEVELOPMENTS: THE RISE OF NON-FUNGIBLE TOKENS (NFTS)

The classification of tangible digital assets as property under the Civil Code, coupled with the clarification between the distinction of copyright and the material object, provides elucidation on how the law ought to treat Non-Fungible Tokens (NFTs).

NFTs, by definition, are items that are unique, one-of-a-kind, and cannot be substituted for anything else.[72] In tech, NFTs are digital assets that represent real-world objects, albeit without an outright counterpart. Simply put, they are digital assets like anything that has thus far been discussed (e.g., documents, photos, etc.). However, NFTs are powered by blockchain technology and are, therefore, authenticated. This authentication is what gives these digital assets their unique properties, their non-fungibility. By virtue of authentication (acquiring a digital signature), these digital assets acquire their monetary worth.

NFTs currently find most applications in digital art and trading cards. While Leonardo da Vinci painted the Mona Lisa on a physical medium, a 21st-century digital artist may opt to create his/her magnum opus on a computer using software such as Adobe Photoshop, Corel Painter, Affinity Sketchbook, or Savage Interactive's ProCreate. Prior to NFTs, it would be difficult for a digital artist to properly monetize his/her wares. It is easy for any person to duplicate the artwork (file) after an initial download. By simply copying and pasting the file, a limitless amount of material objects may be created, diminishing its inherent monetary value as a work of art. The authentication provided by NFTs solves precisely this problem. If a digital artist opts to sell his work, selling it as an NFT warrant to both the buyer and seller that the piece of art concerned is genuine and verifiable. Even if other parties duplicate the said file multiples times, the presence of an NFT copy ensures that there is only one single authentic copy out in the world, everything else would be considered fake. With the advent of NFTs, the next Mona Lisa may be created on a digital-only medium, but now would sell just as much.

Using this same scenario to synthesize, it would be possible for a digital artwork to have three layers of property rights: (1) The copyright, (2) The authentic material object (NFT), and (3) Any other material object not authenticated by NFT. It must be clarified that normal

[72] Robyn Conti, What You Need To Know About Non-Fungible Tokens (NFTs) Forbes (2021), *available at* https://www.forbes.com/advisor/investing/nft-non-fungible-token/ (last accessed May 9, 2021); Mitchell Clark, NFTs, explained The Verge (2021), *available at* https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq (last accessed May 9, 2021); What are NFTs and why are some worth millions?, BBC News (2021), available at https://www.bbc.com/news/technology-56371912 (last accessed May 9, 2021).

digital assets not covered by NFT technology are considered to be subject to the rules already priorly discussed. All three properties follow the same rules and principles of succession law.

I. AINSLEY'S CASE - APPLYING THE PRINCIPLES OF PROPERTY TO THE HYPOTHETICAL SCENARIO

In the main hypothetical case presented by this article, it can be concluded that the files and emails belong to the deceased, Ainsley. These include all his music, both released and unreleased, his lyrics saved in various file formats, manuscripts, sheet music in PDF format, pictures, videos, email messages, and many more. Having died without a will, and with all his assets stored on the cloud (Google Drive, DropBox, OneDrive, iCloud, and Yahoo!), his heirs must request for these files from each ISP. Without designating tangible digital assets as property, it is unclear if the heirs have a cause of action against the ISPs. Instead, they are left at the mercy of the varying TOCs. Each ISP has its own set of rules and policies governing this type of situation, and may or may not result in the recovery of the assets. In fact, an ISP may stipulate that digital asset are purely personal and non-transmissible. A user may be completely unaware of such a condition because rarely does anyone read the TOCs in full. The TOCs are nevertheless considered valid because they are "clickwrap agreements." Classifying tangible digital assets as property establishes a clear rule of law. The heirs have a cause of action against the ISPs for the transfer of the assets because such a classification has established a legal right, subject to the rules and policies of data privacy. The heirs have no right against the account itself because it is a personal right established by the service agreement. It necessarily extinguishes upon death.

PRIVACY ISSUES OF THE DECEASED UPON TRANSFER OF ASSETS

While it is easy to simply extend the concept of property under the Civil Code to digital assets as a premise for their transmissibility, straightforwardly doing so would put privacy issues – the wishes of the deceased in particular – at grave risk. Two issues are identified: the first is whether the deceased is afforded [posthumous] privacy protection and whether disclosure of information or assets against his wishes would be a violation of such. The second is providing for a manner of transfer without violating the decedent's wishes, both for testate and intestate succession. In fine, then, it is easy to see that the problem is not the classification of the assets per se, but rather, how the right to privacy of the deceased is protected in the transfer of these assets upon succession.

To address the privacy issue, one legal scholar is of the view that "when a person leaves digital assets intestate, courts should destroy those assets unless a potential beneficiary can demonstrate the deceased's intent."[73] The basis for his argument is that digital assets (not just tangible digital assets) reveal significant personal information. He draws a parallel with the treatment of a deceased's preserved sperm. In the absence of explicit intent, posthumous

[73] Kutler, *Supra* at Note 172, at 1662.

conception is not allowed and the pre-embryonic material must be disposed of.[74] This is further buttressed by American jurisprudence, declaring that actual express consent is needed for the transfer of assets.[75]

A. PRIVACY RIGHTS OF THE DECEASED IN THE PHILIPPINES

It is elementary in Civil Law that civil personality and juridical capacity are extinguished upon death.[76] Rule 3, Section 16 of the Rules of Court emphasizes this by expressing that the deceased is replaced by the estate during the pendency of a suit.[77] With this in mind, it is straightforward to argue that deceased persons are not afforded privacy rights.

Veritably, this was the ruling by the Supreme Court in *Zarate v. Aquino III*.[78] *Zarate* involves a petition for the Writ of Amparo and the Writ of Habeas Data. The petitioners are members of progressive party-lists and/or national/religious organizations and assert that they have been identified as "communist front" organizations by the military and the police. Relevant to the discussion on the privacy rights of the deceased is the issue of legal standing by the heirs of Crispin Beltran. Noting that the former party-list representative died on May 20, 2008, the Court applied Section 6 of the Rule on the Writ of Habeas Data. The Court stated that the petition for the Writ of Habeas Data presupposes that the subject is still alive.[79] The rationale is that the subject sought to be protected by the extraordinary remedy no longer exists. Hence, the heirs have no legal standing before the Court.

It seems a contradiction, then, that the Data Privacy Act provides for the transmissibility of rights of the data subject.[80] Thematically, the rights granted under Section 16 grant an individual the rights to 1) be informed and 2) be granted access. In relation to digital assets, the author notes that both *Zarate* and the Data Privacy Act pertain to personal information.[81] The principles established may not be wholly applicable to tangible digital assets. Nonetheless, an

---

[74] *Id* citing Kirsten Rabe Smolensky, Rights of the Dead, 37 HOFSTRA L. REV. 763, 784 (2009).

[75] Michael Hellbusch, Digital Assets of the Deceased, Privacy, and the Law, (A presentation for the South Bay Estate Planning Council), 12-14, available at http://sbepc.org/wp-content/uploads/2016/08/December-presentation.pdf (last accessed August 15, 2018).

[76] CIVIL CODE, arts. 37 & 42.

[77] Disini & Disini Law Office, Privacy Rights of the Deceased, available at https://elegal.ph/privacy-rights-of-the-deceased/ citing Rules of Court, Rule 3, § 16.

[78] Zarate v. Aquino III, G.R. 220028, November 10, 2015.

[79] *Id*. "Although the petition for a writ of habeas data may be filed by family member, or even relatives, on behalf of the aggrieved party, the Habeas Data Rule presupposes that the aggrieved party is still alive as Section 6 of the said Rule requires the petitioner to show how the violation of the aggrieved party's right to privacy or threats of such violation affect the aggrieved party's right to life, liberty or security. Given the obtaining circumstances, petitioner Heirs of Crispin Beltran do not have the legal standing to file the present petition.||| (Zarate v. Aquino III, G.R. No. 220028 (Notice), [November 10, 2015])"

[80] Data Privacy Act §16 & 17; SEC. 17. Transmissibility of Rights of the Data Subject. – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

[81] *Id: "*Personal information' 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" See also: §3(c) - Data subject refers to an individual whose personal information is processed.

individual's digital assets, while not considered as personal information per se, reveal a significant amount of personal information, developed over time.[82] Thus, *Zarate* and the Data Privacy Act may still have a degree of coverage. Such coverage, though, is purely speculative at this point.[83] Despite the rights granted by Section 16, and the transmissibility of rights by Section 17, it is insufficient to declare that deceased persons have privacy rights. Reading the provisions of the Data Privacy Act as a whole, the rights granted by the law have limited application because the personal information being referred to is those information personal to an individual that is inevitably shared to others[84] over the course of daily life and transactions. Therefore, tangible digital assets stored on a private platform are beyond the ambit of the Data Privacy Act.

By default, then, the rule would seem to be that the deceased do not possess express privacy rights. Yet, concluding that the deceased do not have privacy rights does not automatically permit the wholesale transfer of tangible digital assets, disregarding the wishes of the deceased should there be any. While the deceased does not have any express privacy rights, they nonetheless have implied or residual privacy rights. This is manifested in organ donation, the disposition and following their wishes as provided for in a last will and testament, and more.[85] The wishes of the deceased, if they have been sufficiently manifested, always supersede the wishes of his family.

Precisely because tangible digital assets reveal a significant amount of information about a person over a period of time, then there should be even more reason to protect the privacy and dignity[86] of a person after death.

The problem now is how to provide for a mechanism that effectively filters tangible digital assets during their transfer – one that guarantees that the files and correspondences that the deceased wished to remain confidential, stay confidential – without the decedent having left a will.

The author submits that the solution to this dilemma may be found in the concept of reasonable expectation of privacy. Drawing an analogy to physical property, the belongings of

[82] Chu, *supra* at Note 198, at 265.

[83] This matter deserves its own thesis. It is recommended that future research be done examining the applicability of the Zarate ruling and the Data Privacy Act to tangible digital assets.

[84] Data Privacy Act §3(h): Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

(1) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

[85] Chu, *Supra* at Note 198, at 271-272.

[86] *Id* at 272: "Privacy and dignity are two separate, but closely interrelated concepts. Privacy is "about the protection of human autonomy and dignity—the right to control the dissemination of information about one's private life." citing N. A. Moreham, *Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort*, *in* LAW, LIBERTY, LEGISLATION 231–248 (Jeremy Finn & Stephen Todd, eds., 2008), *available at* http://www.victoria.ac.nz/law/about/staff/publications-nicole-moreham/nm-law-liberty-legislation.pdf.

a deceased person who has died intestate are freely handled by his heirs. A notebook or journal left on top of a table inside the decedent's room, for example, may freely be read by his heirs, even if he does not want them to. Books, DVDs, VHS tapes, and LP Records, too, found in the decedent's house now belong to his heirs,[87] and may be freely used by them. Now, what if the belonging in question was a handwritten letter? The wishes of the decedent as regards its confidentiality may be inferred by its location and manner of safekeeping. If it was simply placed on top of his desk, then it would be reasonable to infer that the contents of the letter are not sensitive and that it would be alright for others to read. If the letter was crumpled, slightly burnt, found in the trash, or stored in a safe, it would also be reasonable to infer that the contents are confidential, and subsequent disclosure would require his consent.

In *Pollo v. Constantino-David*,[88] Justice Bersamin in his concurring and dissenting opinion elaborates on the concept of privacy. First, he quotes torts scholar William Prosser in identifying the four types of torts in the invasion of privacy: "(a) the intrusion upon the plaintiffs seclusion or solitude, or into his private affairs; (b) the public disclosure of embarrassing private facts about the plaintiff; (c) the publicity that places the plaintiff in a false light in the public eye; and (d) the appropriation, for the defendants advantage, of the plaintiffs name or likeness."[89] In relation to digital assets, the transfer of files that the decedent may wish to keep confidential may result in the second or third type of torts.

Citing *Roe v. Wade,*[90] Justice Bersamin explains the notion of "decisional privacy." In the context of *Roe v. Wade*, decisional privacy is broad enough to encompass "a woman's decision whether or not to terminate her pregnancy."[91] The doctrine is applicable in the Philippines as exemplified by the case of *Estrada v. Escritor*.[92] Applying this to the transfer of tangible digital assets through succession, the intent of the decedent as to what assets (and therefore, information) are inherited by his heirs fall squarely within "decisional privacy." In the absence of a will, though, it would be almost impossible to ascertain the decedent's decision. This is where the "reasonable expectation of privacy" comes in.

The "reasonable expectation of privacy" test was introduced by Justice Harlan in *Katz v. United States*.[93] Justice Harlan elucidates that the test has a two-fold requirement: "1) that a person has exhibited an actual (subjective) expectation of privacy and; 2) that the expectation be one that society is prepared to recognize as reasonable."[94] The author forwards that this test may be used in ascertaining those tangible digital assets that are transmissible to the heirs, and those that must be extinguished upon death. As in a journal or a computer that has been left lying around the room, without much in the way of keeping them hidden, there can be no reasonable expectation of privacy on the part of the decedent.

---

[87] CIVIL CODE, arts. 776, 777.
[88] Pollo v. Constantino-David, G.R. 181881, 675 Phil. 225-300, (2011) (J. Bersamin, concurring and dissenting opinion).
[89] *Id.*
[90] Roe v. Wade, 410 U.S. 113 (1973).
[91] *Constantino-David,* 675 Phil.
[92] Estrada v. Escritor, AM P-02-1651, (2003).
[93] Katz v. United States, 389 U.S. 347 (1967).
[94] *Constantino-David,* 675 Phil.

CONCLUSION AND RECOMMENDATION

The myriad of legal issues pertaining to the classification and transmission of digital assets are all premised on two factors: 1) the lack of a definition and 2) the absence of provisions for a manner of transmission that respects the decisional privacy of the decedent.

The emphasis of literature on the transmissibility of digital assets has thus far been on the significance of estate planning and a digital executor. The reality, however, is that the dominant mode of succession is intestate. This means that the heirs, along with the digital executor, are clueless as to the wishes of the deceased. The digital executor, in particular, may be perplexed by the nature and legal implications of his duties. Without a declaration that digital assets are property, it is unclear whether he may be given access by the ISPs. Furthermore, if a decedent had planned for his digital estate and had given the future executor his account information, he would violate the TOCs, and subsequent access by the digital executor may be considered illegal access punishable by the Cybercrime Prevention Act. The legal issues with the current state of the law may be summarized as follows:[95]

1. Contract Law - The TOCs are contractual agreements between the user and the ISP. These terms include confidentiality and non-sharing of access information. Even if the user is unaware of such terms, they are nonetheless binding because of the validity of "click-wrap" agreements. This prevents access by a fiduciary who has been given access to information.

2. Criminal Law - The Cybercrime Prevention Act punishes "illegal access". It has yet to be settled if access by a fiduciary would constitute such an offense. Without the declaration that tangible digital assets are property, it is uncertain if heirs have a legal right to the same, which makes them susceptible to liability for "access without right."
3. Privacy Law - The Data Privacy Act does not cover personal information stored within tangible digital assets. The law concerns itself with the regulation of the handling of personal information made available to institutions and agencies through daily transactions. It is also unclear if privacy protection is extended to the deceased.

4. Property and Succession Law - In the absence of a definition of digital assets, tangible digital assets specifically, there is no foundation for successional rights. It is unsettled if the heirs have a right to the tangible digital assets of the decedent.

5. Intellectual Property Law - The copyrights embodied in a decedent's assets form part of his estate. However, without the declaration that the tangible digital assets are property, the material object, the very object (file) housing the intellectual property, would be separated from the copyright itself.

6. Estate Administration - The digital executor must make an inventory of all the decedent's property. However, because there is no declaration that tangible digital assets are the property by nature, the executor is currently uncertain if they should be included as part of the digital estate. The actions that may or may not subject a digital

[95] NSW Law Reform Commission, *availble at* http://www.lawreform.justice.nsw.gov.au/Pages/lrc/lrc_current_projects/Digital%20assets/Background.aspx.

executor to liability are also unresolved. There is an absence of rules that clearly define the authority and possible liabilities of a digital executor. Without these rules, a digital executor is unguided in the exercise of his powers.

7. Conflict of Laws - Due to ISPs being multi-national corporations, and the inherent cross-border character of the internet, there are bound to be several issues as to what law must be applied in certain situations. Article 16 of the Civil Code provides that real and personal property are subject to the law of the country where they are situated, but for succession, the nationality rule must be applied.[96] Yet, the TOCs are governed by their laws. Hypothetically, what law will govern if the asset is habitually accessed in the Philippines by a Filipino, but stored on Indian servers, and owned by an American company?

Simply put, there is no clear rule of law. Multiple branches of law serve as barriers to the lawful transmission of assets. A two-fold solution is provided by this thesis: recognition of tangible digital assets as property, and recognition of privacy rights of the deceased.

The first is that tangible digital assets must be recognized as property by nature. There is no legal barrier to this declaration because tangible digital assets conform with the requisites of property under the Civil Code. However, this is only a fundamental conceptual fit. The rights, obligations, and remedies granted to owners in the Civil Code cannot apply to tangible digital assets because of their incompatible natures. Tangible digital assets, though property by nature, do not fit with the concepts of accession, easements, co-ownership, usufruct, donation, and the like. These rights, obligations, and remedies are clearly geared towards immovable and movable properties defined in Article 414. The service agreement between an owner and the ISP, as well, may be subject to the provisions on *commodatum*. The arrangement bears all the marks of a contract of *commodatum*, except that in some cases, the arrangement is no longer gratuitous. There is no problem in the application of intellectual property laws to tangible digital assets. They clearly belong to the creator and may validly be bequeathed to the heirs, subject to the formalities required by law. Copyrights may be embedded in each asset and the intellectual property code is sufficient in providing for the protection of the copyrights upon transfer through succession.

Second, the privacy rights of the deceased must be expressly recognized, and subsequently, mechanisms must be set up by law to protect it. Through the recognition of the privacy rights of the deceased, mechanisms may be put in place such that the transfer of tangible digital assets through succession does not result in the four types of injury that are related to privacy torts. At least for now, there is a sufficient legal basis to consider the residual privacy rights of the deceased. Still, an express recognition would be a robust solution. No solution allowing parties to sift through assets according to their confidentiality or sensitivity has yet been devised. In the absence of a will, the "reasonable expectation of privacy" may be a suitable test to determine if a decedent had wanted such assets transmitted or destroyed.

[96] CIVIL CODE, art. 16.

In fine, classifying tangible digital assets as property establishes the legal right of the heirs, and legislating privacy mechanisms subsequently protects the decisional privacy of the deceased upon transfer.

ABOUT THE THESIS

This thesis was a finalist in a Dissertation Writing Contest sponsored by the Foundation for Liberty and Prosperity in 2019.

ABOUT THE AUTHOR

Justin Ian M. Manjares graduated from the Ateneo Law School in 2021. He passed the February 2022 Bar Examinations. He is currently the Associate Director for Secretariat and Special Programs in the National Legal Education Advancement Program.

ARTICLES

ONLINE JUSTICE: A LOOK AT THE COURT'S VIDEOCONFERENCING GUIDELINES TO DECONGEST DOCKETS FOR PDLS (PERSONS DEPRIVED OF LIBERTY)

Judge Mary Rocelyn Lim & Atty. Edda Marie M. Sastine-Advincula

Abstract: The integrity and sanctity of our judicial system has long been tarnished by the perpetually-entrenched crisis of clogged dockets, even at the trial court level. Time and again, the Supreme Court recognized the need to implement existing policies laid down by the Constitution, the laws and the rules respecting the Rights of the Accused in the context of decongesting our detention jails and humanizing the conditions of detained persons pending their hearings.

Recognizing the ways in which the Supreme Court has attempted to impose and re-impose jail decongestion is always keenly balanced with the ever-present role of the State to maintain peace and order. Yet within the legal paradigm in the Philippine criminal law system, there is a higher moral imperative towards respecting human rights, especially the constitutional framework on liberty.

The crisis is made even more palpable when considering the exponential increase of PDLs (Persons Deprived of Liberty) over the years due merely to the lack of rational, systems-based techniques in jail decongestion. This reportorial study delves into the ways that the present technology affects jail decongestion. Long before the COVID-19 Pandemic, online hearings have slowly started taking root as the "new normal" in Western jurisdictions. From the perspective of both a practitioner and a trial court judge, this study contends that with a few procedural tweaks, online hearings may be the catalyst needed to solve the bottlenecks in the judicial system.

The court system needs to capitalize on this prevalence of online hearings now, while establishing it as a long-term solution for PDLs. In other words, the goal is to transform the bane of the pandemic into a boon for jail decongestion. The following are the mechanisms to be discussed:

Online arraignments – Make arraignments faster, while also weeding out those cases susceptible to plea bargaining;

Online raffle – An online system for this may easily distribute and assign cases, identifying judges assigned to each case, at the outset (before CAM, and before preliminary conferences);

Online bail hearings – Can instantly grant bail or release upon recognizance;

Online trial - Judges may proceed with demurrer/dismissal on the merits. Judges may also weigh merits of affirmative defenses at the get-go (online hearing on affirmative defenses).

Needless to say, these mechanisms require the concomitant changes to the procedural rules, such as requiring written submissions. At present, procedural rules require certain submissions in writing affect the fluidity of online hearings.

THE BURGEONING ROLE OF ONLINE TECHNOLOGY

The integrity and sanctity of our judicial system have long been tarnished by the perpetually entrenched crisis of clogged dockets, even at the trial court level. Time and again, the Supreme Court recognized the need to implement existing policies laid down by the Constitution, the laws, and the rules respecting the rights of the accused in the context of decongesting our detention jails and humanizing the conditions of detained persons pending their hearings.

The need for decongestion is made even more palpable when considering the exponential increase of PDLs (Persons Deprived of Liberty) over the years due merely to the lack of rational, systems-based techniques in jail decongestion. This exploratory study delves into the ways technology may be harnessed via online hearings to specifically address jail decongestion. Long before the COVID-19 pandemic, online hearings have slowly started taking root as the "new normal" in Western jurisdictions. From the perspective of both a practitioner and a trial court judge, this study contends that with a few procedural tweaks, online hearings may be the catalyst needed to solve the bottlenecks in the judicial system. The author contend that the court system needs to capitalize on this prevalence of online hearings now while establishing it as a long-term solution for PDLs. In other words, the goal is to utilize the bane of the pandemic and the development of videoconferencing technology into a boon for jail decongestion. The following are several tangible online hearing mechanisms for PDLs:

1. Online Arraignments – Make arraignments faster, while also weeding out those cases susceptible to plea bargaining;
2. Online Raffle – Immediately assign and distribute cases, which enables judges assigned to each case to act at the outset (before CAM, and before preliminary conferences);
3. Online Bail Hearings – Facilitate early releases through bail or recognizance;
4. Online Trial – Move forward to remedies such as demurrer or dismissal on the merits or affirmative defenses.

Needless to say, these mechanisms require concomitant changes to the procedural rules, such as requiring written submissions, among others. At present, the rules include the requirement of written motions to quash and written comments so judges can *motu proprio* dismiss the case when warranted.

Lastly, while this article recognizes ways in which online technology assists courts in imposing measures toward jail decongestion, there is a caveat. During the pandemic, to ensure that the business of the courts is not derailed, the role of videoconferencing technology has burgeoned substantially, to the probable detriment of valid constitutional concerns. Such must always be keenly balanced with due process and the Rights of the Accused, specifically the Confrontation Clause, or the right to confront one's accusers. Within the Philippine criminal law system, there is a higher moral imperative toward respecting human rights, especially the constitutional framework on liberty.

A.M. 20-12-01-SC

On 9 December 2020, the Supreme Court issued comprehensive guidelines on the conduct of videoconferencing, cited as A.M. 20-12-01-SC. The issuance categorically declares that courts may *motu proprio* order those hearings involving PDLs to be conducted through videoconferencing.[1]

Videoconferencing utilizes a technology platform, currently Microsoft Teams, to transmit video, audio, and data that allow participants in different physical locations to simultaneously communicate by seeing and hearing each other.[2] The consequence of this real-time electronic transmission is the immediacy of case milestones such as arraignment, raffle, bail, and trial. The issuance of release orders is made faster through this mechanism.

A. ONLINE ARRAIGNMENT

According to the Revised Guidelines for Continuous Trial of Criminal Cases, the arraignment and pre-trial of the accused shall be set within ten (10) calendar days from the date of the receipt of the records.

Videoconferencing allows for the immediate arraignment of the accused. Judges and lawyers need not exhaust that period, and may instantly schedule the arraignment of PDLs. It is not impossible to set the hearing for the very next day after the judges have studied the records of the criminal case.

[1] RE: PROPOSED GUIDELINES ON THE CONDUCT OF VIDEOCONFERENCING, A.M. No. 20-12-01-SC, § II (1) (Dec. 9, 2020).
[2] *Id.* § I (2) (a).

Videoconferencing no longer requires the physical presence of the PDL in court. As a result, courts need not deal with the difficulty of demanding the transport of PDLs from their respective detention centers for their arraignment.

As a concrete example, PDLs of a court, say in Region 4, may have been detained in another province, such as Region 2. According to the Rules of Criminal Procedure, law enforcers may enforce the warrant at *any* place, and thus, the place of apprehension of a PDL is not necessarily within the locality of a court. If physical presence is still required, the detention center will not be able to bring the PDL to court right the next day. Logistical barriers will prevent the immediate arraignment of the accused.

Arraignment is an important milestone in criminal procedure. An immediate arraignment opens the opportunity for the judges, prosecutors, and Public Attorney's Office (PAO) lawyers to converse with the PDLs. The latter will not just enter their plea, but will also speak about matters that lead to their immediate release.

Among many other legal consequences, arraignment allows the accused to enter a plea.[3] If the accused, who is currently a PDL, pleads "guilty" to the crime as charged, or plea bargains to a lesser offense, his plea will automatically result in his release from detention if he has successfully availed of subsidiary imprisonment. Pleading "not guilty" may also result in the automatic release of the PDL if the parties agree to provisionally dismiss the case.

Those who plead "guilty" will be immediately released if they have already served their sentence. Those who plead "not guilty" will be released on recognizance if they have served the minimum of the imprisonment term of the crime charged.

These four (4) distinct modes of early release will decongest jails:

a. Subsidiary Imprisonment

In pleading "guilty" to the crime as charged, the accused agrees to serve the sentence to be imposed by the court. For example, in first-level courts, some courts may impose a PHP 1,000 fine on those who admitted to the crime of illegal gambling.[4] Illegal gambling, like unauthorized cockfights or *tupada*, *cara y cruz, tong-its*, and *mahjong* have several players and bettors that populate detention centers.

[3] 2000 REVISED RULES OF CRIMINAL PROCEDURE, rule 116, § 1 (a).
[4] Prescribing Stiffer Penalties on Illegal Gambling, Presidential Decree No. 1602, (1978) (as amended).

Public defenders raise that their PDLs do not have sufficient resources to pay for PHP 1,000. They would then invoke the provisions of Article 39 of the Revised Penal Code and apply for a subsidiary penalty.

The rate of one day of detention for every amount equivalent to the prevailing highest minimum wage rate in the Philippines will then be credited in favor of the PDL.[5] In our example, assuming that the minimum wage is at PHP 500, the subsidiary penalty of the PDL is two (2) days of imprisonment (1,000 / 500). In most instances, the PDL had already been detained for two (2) days,[6] and thus eligible for release. Since PDLs in illegal gambling are plenty, a considerable reduction in the constriction of jail cells can be felt.

A similar situation transpires in plea bargaining. In that scenario, PDLs enter a plea of guilt to a lower offense (for example, from qualified theft to simple theft).[7] If they avail of the benefits of the subsidiary penalty, they will also be quickly released from detention.

b. Provisional Dismissal

PDLs who plead "not guilty" may entertain the possibility of an amicable settlement with the aggrieved private party. In OCA Circular No. 127-2021, the Supreme Court urged judges to strongly encourage litigants to resort to alternative dispute resolution mechanisms for a speedier disposition of cases affecting PDLs.

In practice, judges are expected to talk in open court to the litigants, through their legal representatives (usually the handling prosecutor and the PAO lawyer), about the possibility of threshing out their differences by themselves. If there is a possibility of settlement, judges may provisionally dismiss the case after obtaining consent from the prosecution and the defense.

Within a period of a year for first-level courts, and two years for second-level courts, the parties may agree to monetize their grievances, or simply forgive one another. If settlement does not materialize, the prosecution may revive the case within that one-year or two-year period. At all events, the provisional dismissal of the case results in the release of the PDL from detention.[8]

To illustrate, in an unjust vexation case, the accused, who happens to be the neighbor of the private complainant, allegedly annoyed the latter by hurling insults.[9] The private complainant, if asked, may be open to the possibility of forgiving their repentant accused and restoring their

[5] An Act Amending Article 39 of Act No. 3815, as Amended, Otherwise Known as the Revised Penal Code, Republic Act No. 10159, (2012).
[6] N.B. After detaining the accused, they will still be subjected to booking procedures and inquest proceedings, which takes time.
[7] REVISED RULES OF CRIMINAL PROCEDURE, rule 116, § 2.
[8] *Id.* rule 116, § 8.
[9] An Act Revising the Penal Code and Other Penal Laws [REV. PENAL CODE], Republic Act No. 3815, art. 287 (1930).

[88] *Id.*
[89] Amnesty International, *supra* note 79.

neighborly relationship. To expedite reconciliation talks, which would be difficult if one of the parties is inside a detention center, the prosecution would agree to provisionally dismiss the case; and the accused would consent. Right after the arraignment, the judge would issue an order provisionally dismissing the accused and directing the jail officer to release the accused from detention.

Other PDLs and private complainants may follow suit, thus paving the way for more releases from detention centers.

c. Service of Sentence

As mentioned, during the arraignment of PDLs, they are required to enter a plea of either "guilty" or "not guilty" to the crime charged. If the accused pleads guilty, the case is finished, and an imprisonment term will be handed down. Judges will credit the number of days that they have served in detention.

For example, in crimes covered by the Revised Rule in Summary Procedure, the jail sentence does not exceed six (6) months.[10] If the PDLs have already been in the detention center for at least a month, and the imposed penalty is one (1) month, they may be immediately released for having already served sentence.

The wording of the Rules on Criminal Procedure is immediate and automatic. According to Section 16, Rule 114, "when a person has been in custody for a period equal to or more than the possible maximum imprisonment prescribed for the offense charged, he shall be released immediately."[11]

d. Release on Recognizance

It is logical to expect that PDLs will plead "not guilty" if they are innocent of the crime. If they do not have money to file for bail, they must await trial inside detention centers.

Crimes under the jurisdiction of first-level courts and governed by Revised Rule in Summary Procedure do not have jail sentences exceeding six (6) months. Under Section 16, Rule 114, "a person in custody for a period equal to or more than the minimum of the principal penalty prescribed for the offense charged, without application of the Indeterminate Sentence Law or any modifying circumstance, shall be released on a reduced bail or his recognizance, at the discretion of the court."[12]

[10] RE: PROPOSED GUIDELINES ON THE CONDUCT OF VIDEOCONFERENCING, § 1 (B).
[11] REVISED RULES ON CRIMINAL PROCEDURE, rule 114, §16.
[12] *Id.*

According to OCA Circular No. 91-2020, entitled *Release of Qualified Persons Deprived of Liberty*, all courts must immediately act *motu proprio* on cases of PDLs who have been detained for a period at least equal to the minimum of the penalty for the offense charged, and if warranted, may release such detainees on their recognizance, provided that the court is assured of where the accused can be located while their cases are an on-going trial.[13] The accused must provide their contact numbers and exact address where they will be residing, as well as the contact numbers of at least two (2) of their nearest of kins with their exact addresses as well.

Thus, if the PDLs have already been in the detention center for at least a month, and the imposable penalty is three (3) months, they may be immediately released for having already served the minimum penalty. No other requirement is necessary save for those mentioned in the latest circular.

B. ONLINE RAFFLE

The precursor of arraignment is the receipt of the records of the cases assigned to a particular court. In courts with multiple branches, such as those in the National Capital Judicial Region and major cities in the provinces, the assignment of cases must only be through a raffle. Emphatically, no "case shall be assigned to any branch of a multiple-branch court without being raffled."[14]

The raffle of cases is conducted electronically for eCourt stations.[15] For stations not yet equipped with the platform, the raffle shall be done in open court, with the attendance of the members of the Raffle Committee.[16]

In the first months of the pandemic, the physical closure of the courts compounded the problem of jail congestion. Cases were not raffled, which led to the accumulation of unheard cases. The Supreme Court assigned judges on duty to act upon bail applications; but still, the benefits of arraignment were not realized by this stop-gap measure.

Eventually, the Supreme Court took a bold step by allowing a raffle of cases through videoconferencing. The explanation follows:

---

[13] Office of the Court Administrator, Release of Qualified Persons Deprived of Liberty, OCA Circular No. 91-2020 (Apr. 20, 2020).
[14] GUIDELINES ON THE SELECTION AND APPOINTMENT OF EXECUTIVE JUDGES, A.M. No. 03-8-02-SC, Chapter V, § 2, (Jan. 27, 2004).
[15] Office of the Court Administrator, Resumption of Raffle of Cases through Videoconferencing, OCA Circular No. 94-2020, (May 8, 2020).
[16] GUIDELINES ON THE SELECTION AND APPOINTMENT OF EXECUTIVE JUDGES, A.M. No. 03-8-02-SC, Chapter V, § 4, (Jan. 27, 2004).

> Under par. 9, OCA Circular 89-2020, "the raffle of newly-filed cases during this public health emergency (has been) SUSPENDED." While the suspension of the raffle of newly-filed cases has been lifted in areas under General Community Quarantine (GCQ), the raffle of cases remains suspended in areas under Enhanced Community Quarantine (ECQ). This has resulted in the accumulation of "unraffled" cases, which, if raffled and acted upon in due course, may result in the expeditious termination of cases and consequent release of Persons Deprived of Liberty (PDLs).[17]

In the raffle of cases through videoconferencing, the clerk of court of the Office of the Clerk of Court would record the random drawing of cases conducted by the Raffle Committee, with the judges and stenographers appearing virtually.

In effect, the physical closure of the courts no longer posed a barrier to the assignment of cases. Judges, to whom cases were raffled, have three options:

First, they may set the case for arraignment. As explained in the preceding section, the immediate arraignment of PDLs lets courts issue release orders, resulting in a reduction of inmates inside jail facilities.

Second, judges may require prosecutors to present additional evidence in case of doubt as to the existence of probable cause to continue with the trial of the accused.[18]

Third, judges may outrightly dismiss the case for want of probable cause.

To be sure, the Rules of Criminal Procedure[19] and the Revised Rule on Summary Procedure[20] give courts the third option. Judges may order the immediate dismissal of cases for want of probable cause.

Litigants and prosecutors are aware that although the Revised Guidelines for Continuous Trial of Criminal Cases declared motions for judicial determination of probable cause as prohibited filing,[21] still, jurisprudence anchors the discretion of judges to declare cases as inadequate to proceed to trial.

---

[17] Office of the Court Administrator, Resumption of Raffle of Cases through Videoconferencing, OCA Circular No. 94-2020, (May 8, 2020).
[18] REVISED RULES OF CRIMINAL PROCEDURE, rule 112, § 6.
[19] *Id.*
[20] THE 1991 REVISED RULES ON SUMMARY PROCEDURE, (Resolution Of The Court En Banc Dated October 15, 1991 Providing For The Revised Rule On Summary Procedure For Metropolitan Trial Courts, Municipal Trial Courts In Cities, Municipal Trial Courts and Municipal Circuit Trial Courts) § 12 (a) (Oct. 15, 1991).
[21] RE: PROPOSED GUIDELINES ON THE CONDUCT OF VIDEOCONFERENCING, § III (2).

In *People v. Lim*, the Supreme Court pronounced that poorly built cases should no longer congest the dockets of the courts. Prosecutors were reminded to complete the supporting documents in the Information that they filed in the courts; otherwise, judges may dismiss the case outright for lack of probable cause.[22]

The dismissal orders are accompanied by directives to release the accused from detention. If all cases are duly raffled, innocent PDLs are expected to be released, which curbs the congestion rate in prison cells.

C. ONLINE BAIL

Bail is a constitutionally enshrined right.[23] Pragmatically, this means that bail applications of PDLs are urgent matters that judges are expected to resolve immediately. The Revised Guidelines for Continuous Trial of Criminal Cases requires that bail petitions "shall be set for summary hearing after arraignment and pre-trial" and must be resolved "within a non-extendible period of thirty (30) calendar days from the date of the first hearing, except in drug cases which shall be heard and resolved within twenty (20) calendar days."[24]

Without the videoconferencing platform, courts face the same dilemma of transporting the accused, the witnesses, and the private complainant. The waiting period for the delivery and the receipt of notices and subpoenas means more jail time and delays in the release of PDLs.

Now, bail petitions may be acted upon electronically. The relatives of the PDLs, and even the accused themselves, may inquire about the process and the requirements to successfully secure a release order through a bail application. Courts may issue online orders to be sent to the email addresses of the custodial center, the PAO, and the prosecution setting the date of the hearing immediately. During the online hearing, the parties may agree to release the accused on ordinary bail, reduced bail, or allow the accused to be released on recognizance.

Administrative Circular 38-2020 (AC 38-2020), otherwise known as *Reduced Bail and Recognizance as Modes for Releasing Indigent Persons Deprived of Liberty during this Period of Public Health Emergency, Pending Resolution of Their Cases*, further complements the online bail.[25]

---

[22] People v. Lim, G.R. No. 231989, (2018).
[23] PHIL. CONST., art. III, § 13.
[24] RE: PROPOSED GUIDELINES ON THE CONDUCT OF VIDEOCONFERENCING, § III (10).
[25] Supreme Court of the Philippines, *Reduced Bail and Recognizance as Modes of Releasing Indigent Persosn Deprived of Liberty During this Period of Public Health Emergency, Pending Resolution of their Cases*, Administrative Circular No. 38-2020 (Apr. 30, 2020).

AC 38-2020 drastically reduced the bail of PDLs. With lower bail amounts, the Supreme Court hopes that indigent PDLs can now apply for provisional liberty and be released from detention.

For those charged with a crime punishable with the maximum period of *prision correccional* or six (6) months and one (1) day to six (6) years, the bail shall be computed by getting the medium period multiplied by PHP 1,000 for every year of imprisonment. The imprisonment term for illegal gambling is *prision correcional* in its medium period or from two (2) years, four (4) months, and one (1) day to four (4) years and two (2) months. PDLs may then apply for bail at the reduced amount of PHP 2,000.

If the imposable sentence of the PDLs does not amount to a year, such as those punished by *arresto menor* and *arresto mayor*, courts may release PDLs on recognizance.

The prerequisite of reduced bail is an online hearing. AC 38-2020 states that indigent PDLs who have not yet been arraigned must first be arraigned before being granted bail or recognizance, which arraignment and release on bail or recognizance may be conducted through videoconferencing.

At all events, the judge acting on the bail application will issue electronic release orders. The swift transmission of data in electronic channels directly affects the ease of jail decongestion.

D. ONLINE TRIAL

Judges, litigants, and lawyers may have different sets of experience in online trials. One thing is for sure, online trials allow criminal cases of PDLs to progress from arraignment and pre-trial to the presentation of prosecution's evidence. At the end of that milestone, the defense may move for the dismissal of the case by filing a Demurrer to Evidence.

Demurrer to Evidence, according to Section 23, Rule 119 of the Rules of Criminal Procedure, allows the accused to ask the courts for the dismissal of the action, on the ground of insufficiency of evidence presented by the prosecution.[26] Logically, if the remedy is granted, the accused no longer has to endure the presentation of defense evidence since the demurrer results in the dismissal of the case. The dismissal of the case, accompanied by the release order for PDLs, would decongest detention centers.

With the online trial, the prosecution, who is expected to be capable of accessing the videoconference hearings, can move the trial towards the completion of its presentation of

[26] REVISED RULES ON CRIMINAL PROCEDURE, rule 119, §23.

evidence. If the trial stagnates, because of the difficulties of physical hearings, the defense will not be able to avail of Demurrer to Evidence.

Aside from a Demurrer to Evidence, the Rules of Criminal Procedure and the Revised Guidelines on Continuous Trial have recognized motions that allow for the release of PDLs. Among others, the following motions may directly or indirectly result in the release of PDLs, to wit:[27] (1) Motion to Withdraw Information; (2) Motion to Downgrade the Charge in the Original Information; (3) Motion to Exclude an Accused; (4) Motion to Quash Warrant of Arrest; (5) Motion to Suspend Proceedings on the ground of prejudicial question;[28] (6) Motion to Quash Information because the facts charged do not constitute an offense, lack of jurisdiction, extinction of criminal action or liability, and double jeopardy; (7) Motion to Discharge the Accuse as a State Witness; and (8) Motion to Dismiss on the ground of denial of the accused's right to a speedy trial.[29]

According to the Revised Guidelines for Continuous Trial of Criminal Cases, judges may hear these motions before resolving them.[30] The benefit of setting the case for an online trial facilitates the immediate scheduling of the hearing of these motions. Within a non-extendible period of ten (10) calendar days thereafter, the court must resolve, and if meritorious, issue the concomitant release orders.[31]

PROCEDURAL SPEED BUMPS

A. ONLINE ARRAIGNMENT

As earlier discussed, after PDLs had been arraigned, they are immediately released through subsidiary penalty, provisional dismissal, service of sentence, or recognizance.

However, under Rule 117, Section 9 of the Rules of Criminal Procedure, arraignment cuts off several remedies. An accused who enters a plea can no longer move to quash the Information on the following grounds: (1) lack of jurisdiction over the person of the accused; (2) lack of authority of the officer to file an Information; (3) lack of conformity to form; (4) failure to charge a single offense; and (5) legal excuse or justification.

Emphatically, Rule 114, Section 26 of the Rules of Criminal Procedure states that the validity of the arrest of the PDL and the absence of preliminary investigation could no longer be assailed if these grounds are not raised before the arraignment of the PDL. These grounds for

[27] RE: PROPOSED GUIDELINES ON THE CONDUCT OF VIDEOCONFERENCING, § III (2) (c).
[28] N.B. Discretionary on the court and affected by the consent of the parties.
[29] REVISED RULES OF CRIMINAL PROCEDURE, rule 119, § 9.
[30] REVISED GUIDELINES FOR CONTINUOUS TRIAL OF CRIMINAL CASES, A.M. No. 15-06-10-SC (Apr. 25, 2017)/
[31] RE: PROPOSED GUIDELINES ON THE CONDUCT OF VIDEOCONFERENCING, § III (2) (c).

quashal, according to Rule 117, Section 2, shall be "in writing, signed by the accused or his counsel and shall distinctly specify its factual and legal grounds."

There lies the difficulty. A motion to quash questioning the legality of the arrest must be in writing. It must be physically signed by the PDLs and their counsel, which, if indigent, are usually represented by the Public Attorney's Office.

Requiring a written motion to quash disparages the swiftness of online arraignments. An arraignment scheduled the next day may be stalled if the defense asks for time to file a written Motion to Quash on the ground of invalidity of the arrest. The public defenders will expose themselves to the difficulty of securing the signatures of PDLs, who are locked up inside the detention centers.

As a possible avenue for amendment, motions to quash on the ground of illegal arrest should be allowed to be made orally.

The Rules of Criminal Procedure, under Rule 113, Section 5, confines warrantless arrest to only three instances*:* (1) *in flagrante delicto* arrest; (2) hot pursuit; and (3) arrest of an escaped prisoner.[32] These kinds of arrests are subjected to inquest proceedings, as there are no warrants of arrest. Judges can effortlessly surmise in the attached sworn statements of the arresting officers whether the accused committed the crime in their presence. Judges can detect whether the law enforcers have personal knowledge of circumstances that led them to conclude that the accused must be arrested. No other additional record needs to be perused.

The Bill of Rights protects all persons from illegal warrantless arrests. Law enforcers, who simply hear about the commission of the crime, have no clear justification to detain the alleged perpetrator.[33] Preliminary investigation resolutions, and not inquest proceedings, should be present in the records to determine the validity of the detention. If that record is absent in one of the attachments in the Information filed before the courts, oral motions to quash the arrest could be instantly resolved by the judge.

Furthermore, the Rules of Criminal Procedure must be harmonized. Rule 117, Section 2 requires a motion to quash to be in writing; while Rule 114, Section 26 does not. The latter mentions that PDLs must raise the invalidity of the arrest before entering a plea. Given the conflict in these provisions, there is room to argue that quashing the warrant of arrest (or warrantless arrest) need not be in writing.

[32] Porteria v. People*,* G.R. No. 233777, 898 SCRA 106 (2019); People v. Chua Ho San*,* G.R. No. 128222, 308 SCRA 432 (1999).
[33] People v. Comprado, G.R. No. 213225, 860 SCRA 420 (2018).

B. ONLINE RAFFLE

Presiding judges act on cases after these had been raffled to them. However, for non-eCourt stations, the rules on the physical raffle,[34] and even an online raffle under OCA Circular No. 94-2020 (Resumption of Raffle of Cases through Videoconferencing)[35] dictate that the raffle of cases in multiple-branch courts is only every Monday and/or Thursday, at 2:00 p.m., as warranted by the number of cases to be raffled.

Hence, PDLs detained on a Tuesday will have to wait until Thursday afternoon, before the criminal action may be acted upon by the presiding judge. Worse, if the case was not raffled on that Thursday afternoon due to the number of cases filed, work suspension, typhoon cancellation, etc., a whole week would have to pass before the raffle of the case.

In decongesting detention centers, every single day counts. Raffle dates must be adjusted to pursue the purpose of jail decongestion. The Supreme Court may mechanize the rules on an electronic raffle to allow real-time raffle of cases involving PDLs. As soon as the case is raffled, the judge to whom the case is assigned may immediately issue release orders secured through applications for bail or recognizance, or after arraignment proceedings.

The rules on raffles provide for the special raffle on urgent matters, worded in this way:[36] "there shall be no special raffle of any case except in petitions for the writ of habeas corpus, applications for bail in cases where the complaint or information has not yet been filed with the court, applications for the issuance of a temporary restraining order (TRO), cases involving foreign tourists, cases with motions for special raffle accompanied by a motion for reduction of bail, and applications for the issuance of search warrants."

Cases involving PDLs are not enumerated in the list. Based on *ejusdem generis*,[37] one might contend that the general term "urgent matters" impliedly includes crimes involving PDLs. Equally, however, applying *expresio unius est exclusio alterius,*[38] executive judges may refrain from the daily raffle of PDL cases considering their exclusion in the enumeration.

---

[34] GUIDELINES ON THE SELECTION AND DESIGNATION OF EXECUTIVE JUDGES AND DEFINING THEIR POWERS, PREROGATIVES AND DUTIES, A.M. No. 03-8-02-SC , Chapter V, § 2.
[35] Item 2.
[36] GUIDELINES ON THE SELECTION AND DESIGNATION OF EXECUTIVE JUDGES AND DEFINING THEIR POWERS, PREROGATIVES AND DUTIES, A.M. No. 03-8-02-SC , Chapter V, § 6.
[37] Pelizloy Realty Corp. v. Province of Benguet, G.R. No. 183137, 695 SCRA 491 (2013). Under the principle of ejusdem generis, "where a general word or phrase follows an enumeration of particular and specific words of the same class or where the latter follow the former, the general word or phrase is to be construed to include, or to be restricted to persons, things or cases akin to, resembling, or of the same kind or class as those specifically mentioned."
[38] Centeno v. Villalon-Pornillos, G.R. No. 113092, 236 SCRA 197 (1994). Where a statute, by its terms, is expressly limited to certain matters, it may not, by interpretation or construction, be extended to others. The rule proceeds from the premise that the legislature would not have made specified enumerations in a statute had the intention been not to restrict its meaning and to confine its terms to those expressly mentioned.

To provide clarity, the codification of the Guidelines on the Conduct of Videoconferencing should particularly state whether the online raffle of cases of PDL should be strictly limited to Mondays and Thursdays only. In keeping with the spirit of case decongestion, PDL cases should be permitted to be raffled daily, via videoconferencing.

C. ONLINE BAIL

In the 2020 ruling of the Supreme Court in *Office of the Court Administrator v. Flor, Jr.*,[39] citing its 2011 ruling in *Gacal v. Infante* and its 1997 ruling in *Cortes v. Catral,*[40] courts were reminded about the duties of judges in resolving bail applications. In all cases, whether the bail is a matter of right or discretion, judges must notify the prosecution of the hearing on the bail application, or require its recommendation. A hearing on the bail is necessary only when bail is a matter of discretion.

In *People v. Valdez*,[41] the Supreme Court categorically said that since the accused is "entitled to bail as a matter of right, a summary hearing on bail application is, therefore, unnecessary."

However, in *Ruiz v. Beldia, Jr.,*[42] the Supreme Court cited as one of the transgressions of the judge his failure to hear the bail of the accused.

That kind of administrative sanction[43] may dissuade judges from issuing electronic release orders on bail applications that were not subjected to a summary hearing. To remove any hesitation and confusion, the present set of rules on online bail applications should particularize that a summary hearing is unnecessary in bail applications of bailable offenses, provided that the Information already states the recommended bail of the prosecution. Needless to say, the prosecution should file an Information with recommended bail to do away with the logistical difficulty of setting the bail application for a hearing.

D. ONLINE TRIAL

Following the wordings of Rule 117, Section 2 of the Rules of Criminal Procedure, all motions to quash shall be "in writing, signed by the accused or his counsel and shall distinctly

[39] Office of the Court Administrator v. Flor, Jr., A.M. No. RTJ-17-2503, (2020).
[40] Cortes v. Catral, 279 SCRA 1 (1997).
[41] People v. Valdez, 776 SCRA 672 (2015).
[42] Ruiz vs. Beldia, Jr., 451 SCRA 402 (2005).
[43] N.B. N.B. Among others, the respondent judge was found to have acted on the bail application (1) without a formal petition for bail; (2) outside his jurisdiction; and (3) over his authority as assisting judge.

specify its factual and legal grounds."[44] However, during the trial, certain affirmative defenses may be argued orally and need not be exhaustively discussed in writing.

Motions to Quash Information, on the ground of lack of jurisdiction, primarily concern questions of law that may easily be resolved. If the prosecution has already concluded the presentation of evidence, the defense should be allowed to argue that none of the elements transpired in the territorial jurisdiction of the Court.[45] The judge can easily resolve the verbal motion via open court order.

The same goes true for Motions to Quash the Information on the ground of prescription. At the onset, even during pretrial, parties may argue that at the institution of the complaint, the criminal action or the penalty has already been prescribed. The judge, through simple mathematical reckoning, can easily resolve the verbal motion via open court order. In gist, according to Article 90 of the Revised Penal Code, prescription runs from the discovery of the crime, and is then interrupted when the offended party, the authorities, or their agents file a complaint or information.

In the crime of slight physical injuries,[46] for example, Article 91 of the Revised Penal Code provides that the crime would have prescribed if more than two (2) months had elapsed from the date of the injury until the filing of the Affidavit Complaint before the Office of the City Prosecutor.

That fact is easily identifiable in the records. To require that the arguments be reduced to a Motion to Quash would be a procedural bump in the swiftness offered by online trials.

REVIEW OF DUE PROCESS CONCERNS IN AMERICAN JURISDICTION

Beyond the procedural concerns in online mechanisms, the overarching human rights framework must be operationalized.

During the pandemic, the Philippine judicial system has tried its best to keep up with its burgeoning dockets, giving primordial importance to the rights of PDLs, while still adhering to national Inter-Agency Task Force health protocols. But in terms of maximizing technology use specifically for court procedures, it is woefully left behind by its Western counterparts.

The United States Supreme Court, for example, has started developing a healthy, jurisprudential compendium addressing possible constitutional issues. Criminal courts throughout

[44] REVISED RULES OF CRIMINAL PROCEDURE, rule 117, §2.
[45] Evangelista v. People, 620 SCRA 134 (2010).
[46] REV. PENAL CODE, art. 266.

the United States have relied upon Zoom and other videoconferencing technologies[47] to help maintain a functioning criminal justice system. However, claims that due process rights are undermined by the use of videoconferencing technology deserve the judiciary's attention, particularly the right to effective assistance of counsel and the right to confront adverse witnesses.

According to former prosecutor Brandon Marc Draper, such technology, in place of in-person trials, potentially violates several constitutional rights afforded to the accused, and might force them to choose to exercise one right guaranteed to them by the Sixth Amendment at the expense of another. Specifically, the accused might now confront two critical constitutional choices: (1) the right to a speedy trial versus the right to a jury trial; and (2) the right to a speedy trial versus the right to confront their accusers, viz.:

> Assuming the accused determines that he may receive a fair Zoom trial, he must then weigh his right to a speedy trial versus his right to confront his accusers. In *Maryland v. Craig*, the Supreme Court carved out a limited exception to the face-to-face requirement of the Confrontation Clause, holding that a "defendant's right to confront accusatory witnesses may be satisfied absent a physical, face-to-face confrontation at trial only where denial of such confrontation is necessary to further an important public policy and only where the reliability of the testimony is otherwise assured." Stay-at-home orders and other social distancing guidelines almost certainly fulfill the "important public policy" prong of *Craig*. But how can the "reliability" prong be fulfilled when there is no way to be in the same room as an accuser to confirm that his testimony is genuine or being fed to him off-screen? Does the potential for contempt charges adequately protect the defendant's rights given these concerns? Ultimately, any virtual confrontation will compromise an accused's Sixth Amendment confrontation right. The choice is stark: relax the confrontation right and proceed to trial or await a delayed trial, possibly at risk of exposure to a potentially lethal virus.[48]

Meanwhile, in *John Vazquez Diaz v. Commonwealth,* a Suffolk Superior Court judge ordered a defendant to have a hearing via Zoom. Diaz argued before the Supreme Judicial Court that a video hearing violates his rights.[49] The case precisely raises questions about how to balance health and safety concerns with a defendant's right to a fair court process – and, according to some commentators, about how the pandemic is affecting existing racial disparities within the American criminal justice system. Diaz's attorneys argued in court briefs that this would "violate his constitutional rights to confront the witnesses against him, to be present at the hearing, to a public hearing, and to the effective assistance of counsel." The other side stressed the public health dangers posed by the COVID-19 pandemic, and the risks to all participants and workers if a

[47] Laura Kusisto, Coronavirus Forces Courts to Experiment, THE WALL STREET JOURNAL, March 28, 2020, *available at* https://www.wsj.com/articles/coronavirus-forces-courts-to-experiment-11585387800 (last accessed Feb. 3, 2022).
[48] Brandon Marc Draper, "Zoom Justice: When Constitutional Rights Collide in Cyberspace," Northwestern University Law Review, 7 May 2020.
[49] Vasquez Diaz vs. Commonwealth, 487 Mass. 336 (2021).

hearing is held in person, noting also the burden placed on jails if inmates returning from the court must be quarantined.

According to Vazquez Diaz's court filing, the jail's COVID-19 restrictions mean his attorneys could not be in a room with him during the hearing, so he would have to participate alone from jail, with an audio interpreter providing the Spanish translation. He would have to communicate with his attorneys only through a breakout Zoom room, which he argues would inhibit their communication. His uncle, with whom he had been living, does not have a device that would let him use Zoom to watch the hearing, though he could listen by phone. The attorneys argue that a virtual hearing has qualitative differences from an in-person hearing, and defendants have had worse outcomes after Zoom hearings. A recent study by the Committee for Public Counsel Services of bail review hearings in Bristol County Superior Court found that bail was reduced by a lower amount in cases when a hearing was held virtually. The government's interest in clearing a backlog of cases that have accumulated during the pandemic cannot outweigh Mr. Vazquez Diaz's right to an in-court proceeding," they wrote.

Vazquez Diaz counters that a virtual hearing loses the solemnity of a courtroom, is subject to internet-based disruptions, and eliminates non-verbal cues from a witness's body language. He claims that the constitutional requirement that a defendant be allowed to confront a witness "face-to-face" cannot be met via videoconference when it is impossible to know if a witness is even looking at a defendant.

His brief further argues that the right to a public trial cannot be achieved via videoconference when the link is only made public upon request – and can only be watched by those with internet access and devices:

> Holding a suppression hearing in a way that precludes perhaps a third of the population from watching even a digitalized facsimile of the proceedings on a device — never mind participating in and serving as a check upon the judicial process — is tantamount to posting a court officer at the courtroom door with instructions to turn away every third person who seeks to enter.[50]

The Supreme Court acknowledged in its earliest interpretations that the right of confrontation is not absolute, as it "must occasionally give way to considerations of public policy and the necessities of the case." One of the oldest exceptions to confrontation is the hearsay exception. As early as 1895, the Supreme Court considered in *Mattox v. the United States* whether the defendant's constitutional right to confrontation had been violated by admitting to the jury prior testimony of two deceased witnesses. There, after a jury convicted the defendant of murder, the

[50] Shira Schoenberg, "Defendant demands in-person day in court," https://clinics.law.harvard.edu/blog/2020/12/defendant-demands-in-person-not-virtual-day-in-court/

Court reversed the district court's judgment under the defendant's writ of error and remanded the case for a new trial.

The Philippines' own Supreme Court promulgated Videoconferencing Guidelines, but has yet to have the opportunity to interpret the confrontation clause in juxtaposition with this issuance. However, in *Kim Liong v. People*,[51] the Court, through Justice Marvic Leonen, had the opportunity to discuss the confrontation clause, the right to cross-examine, and its limits:

> The fundamental rights of the accused are provided in Article Ill, Section 14 of the 1987 Constitution:
>
> Section 14. (1) No person shall be held to answer for a criminal offense without due process of law.
> (2) In all criminal prosecutions, the accused shall be presumed innocent until the contrary is proved, and shall enjoy the right to be heard by himself and counsel, to be informed of the nature and cause of the accusation against him, to have a speedy, impartial, and public trial, to meet the witnesses face to face, and to have compulsory process to secure the attendance of witnesses and the production of evidence in his behalf. However, after arraignment, trial may proceed notwithstanding the absence of the accused provided that he has been duly notified and his failure to appear is unjustifiable.
>
> **"To meet the witnesses face to face" is the right of confrontation. Subsumed in this right to confront is the right of an accused to cross-examine the witnesses against him or her, i.e., to propound questions on matters stated during direct examination, or connected with it**. The cross-examination may be done "with sufficient fullness and freedom to test [the witness'] accuracy and truthfulness and freedom from interest or bias, or the reverse, and to elicit all important facts bearing upon the issue."
>
> (emphasis supplied)
>
> Rule 115 of the Rules of Court with its lone section is devoted entirely to the rights of the accused during trial. Rule 115, Section 1 (f) on the right to cross-examine provides:
>
> Section 1. *Rights of accused at the trial.* - In all criminal prosecutions, the accused shall be entitled to the following rights:
> . . . .
> (f) To confront and cross-examine the witnesses against him at the trial. Either party may utilize as part of its evidence the testimony of a witness who is deceased, out of or cannot with due diligence be found in the Philippines, unavailable, or otherwise unable to testify, given in another case or proceeding, judicial or

[51] Kim Liong v. People, G.R. No. 200630 (2018).

> administrative, involving the same parties and subject matter, the adverse party having the opportunity to cross-examine him.
>
> Denying an accused the right to cross-examine will render the testimony of the witness incomplete and inadmissible in evidence. "[W]hen cross-examination is not and cannot be done or completed due to causes attributable to the party offering the witness, the uncompleted testimony is thereby rendered incompetent." However, like any right, the right to cross-examine may be waived. It "is a personal one which may be waived expressly or impliedly by conduct amounting to a renunciation of the right of cross-examination." When an accused is given the opportunity to cross-examine a witness but fails to avail of it, the accused shall be deemed to have waived this right. The witness' testimony given during direct examination will remain on record. If this testimony is used against the accused, there will be no violation of the right of confrontation.[52]
>
> In *People v. Narca,* the trial court deferred to another date the cross-examination of the prosecution witness on the instance of the accused. However, in the interim, the prosecution witness was murdered. Thus, the accused moved that the testimony of the prosecution witness be stricken off the record for lack of cross-examination. This Court rejected the argument, finding that the accused waived their right to cross-examine the prosecution witness when they moved for postponement. It said that "mere *opportunity and not actual* cross-examination is the essence of the right to cross-examine."[53]

By analogy, it can thus be said that the use of videoconferencing technology will not be considered violative of the right of confrontation if the elements above are still present. So long as the accused was allowed to confront the witnesses – even if he later waived such opportunity – the right is intact. However, it remains to be seen what the impact the phrase "face to face" will pose on the Philippine Supreme Court's adoption of videoconferencing. It must be noted that while the American Constitution never defined the right of confrontation as one that must take place "face to face," the Philippine Constitution employed this phrase.

In the landmark case of *Crawford v. Washington*, the US Supreme Court expounded the relationship between hearsay and the Confrontation Clause.[54] The Court held that an out-of-court statement that is "testimonial" in nature may not be admitted in criminal cases unless the declarant is unavailable to testify at the trial and the defendant had a prior opportunity to cross-examine him. On appeal before the Court, Coy argued that the procedure deprived him of his right to a face-to-face confrontation with adverse witnesses. The Court agreed and reversed his conviction. Writing for the majority, Justice Scalia focused on the importance of requiring face-to-face confrontation, noting that physical confrontation makes it less likely that a witness will lie on the stand as "[i]t is

[52] REVISED RULES OF CRIMINAL PROCEDURE, rule 116, § 1 (a).
[53] Kim Liong v. People, G.R. No. 200630 (2018).
[54] Crawford v. Washington, 541 U.S. 36 (2004).

always more difficult to tell a lie about a person to his face than behind his back." Even if the witness does lie, it will likely be less convincing when recited before the defendant. Furthermore, the trier of fact will have a better opportunity to draw its conclusions on the veracity of the testimony based on the witness's demeanor.

While the Court noted that "rights conferred by the Confrontation Clause are not absolute, and may give way to other important interests," it declined to address whether there were any exceptions. Rather, the Court expressed that if any exceptions existed, they would be permitted "only when necessary to further an important public policy."

The language of the Confrontation Clause uses the word "confronted." While this has often been interpreted as in-person confrontation, the language itself is ambiguous enough that it may not *per se* prohibit the use of videoconference technology. But again, unlike in the Philippine Constitution, nowhere in the text of the Sixth Amendment do the words "face-to-face" or "physical" appear. Justice Scalia, among other critics, argues that video conference testimony "improperly substitutes" 'virtual confrontation' for the real thing required by the Confrontation Clause in a criminal trial. However, with the arrival of new technology, Americans have generally become increasingly less likely to participate in face-to-face interactions.[55]

Perhaps the major factor that could force courts to further accept videoconference technology is public acceptance. People are still worried that the distance or insulation between the defendant and witness could hinder the purpose of the Confrontation Clause. However, as videoconference technology continues to become more commonplace, these fears may diminish with time. Courts are usually a couple of years behind the general public's acceptance of technology. As long as avenues remain within the law to promulgate the use of videoconference technology in the courtroom, public acceptance may push the use of this technology further.[56]

ABOUT THE AUTHORS

Judge Roqs Guillano credits her FEU-IL education for her brave journey to public service. She also thanks Atty. Advincula, her cubicle mate at the Supreme Court of the Philippines – Office of the Chief Justice Maria Lourdes P.A. Sereno, for this journal, and for their parallel quests to enjoy being boymoms.

Atty. Advincula was Vice Chairperson of the Philippine Law Journal, University of the Philippines College of Law. She moved back to her hometown, Iligan City, after giving birth to twin boys.

[55] Hadley Perry, "Virtually Face-to-Face: The Confrontation Clause and the Use of Two-Way Video Testimony," Issue 2, Vol. 13, Roger Williams University Law Review, Spring 2008.
[56] Russel Kostelak, "Videoconference Technology and the Confrontation Clause," Cornell Law JD Student Research Papers (Apr. 24, 2014).

THE FAR EASTERN
LAW REVIEW
VOLUME LI | 2021

SOCIAL MEDIA ALGORITHMS: IMPACT ON HUMAN RIGHTS AND ALGORITHM REGULATION METHODS

Benjamin Niel Dabuet

Abstract: The increasing reliance on algorithms and Artificial Intelligence (AI) in our social systems present novel problems that affect human rights. The Cambridge Analytica scandal revealed to the world the impact and reach of algorithms at a global scale. This paper examines how social media, while utilizing algorithms for efficiency and profit, has underlying effects on human rights, namely: the right to privacy, freedom of expression, right to health, right to due process and free trial, and right against discrimination. Recognizing the lack of efficacy of International Human Rights Law (IHRL) on private entities, this paper reviews different public and private regulations intended to control intermediaries like Facebook and Google, and more relevantly regulate the design of algorithms. Lastly, this paper examines the literature supporting the use of international human rights law (IHRL) as a framework for algorithmic accountability legislation and argues that subsequent algorithm design should have human rights in mind.

Keywords: human rights, artificial intelligence, algorithms, accountability, Cambridge Analytica, social media.

Documentaries like The Social Dilemma[1] and The Big Hack[2] center on the concern with algorithms and Artificial Intelligence (AI) being at the focal point of major events of humanity in the past decades. They depict how algorithms through social media have been able to influence large groups of people for capitalistic purposes. They reveal how popular websites, such as Google and Facebook, surreptitiously gather data from their users and employ massive subliminal cues to change the user's behavior and perception.[3] They also show that algorithms can create massive social impact when used on a global scale and warn dangers when left unregulated.

Algorithms and other terms, such as "artificial intelligence" and "big data," are some of the words being used by companies and experts in the tech industry as our society ushers to an automated future. For the unversed, an algorithm, as defined by the Oxford Dictionary, is "a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer."[4] Its modern application follows a sophisticated analysis of data sets (often termed as "big data") to predict future outcomes, execute complex tasks beyond the capacity

[1] THE SOCIAL DILEMMA (Netflix, 2020).
[2] THE BIG HACK (Netflix, 2019).
[3] THE SOCIAL DILEMMA, *supra* note 1.
[4] *Algorithm,* OXFORD ENGLISH DICTIONARY (5th ed. 2002).

of humans, and have the ability to learn and improve oneself, among others.[5] These algorithms can exist in an intricate, interconnected global network of algorithms whose outputs could be used as new data by subsequent algorithms.

The efficiency of algorithms in handling big data and transforming its output, alongside other algorithmic systems, to consumable pieces of information has found itself positioned in place of human decision-making,[6] such as personalized search engines, newsfeeds, targeted ads, dating applications, determining credit scores, self-driving cars, several judicial services, and other digital services.[7]

Social media relies heavily on the use of algorithms for the following activities: organizing similar posts and interests, matching people with similar backgrounds, demographics, and interests, and providing more content based on the user's likes and traffic history. Intermediaries or companies like Google, Facebook, Twitter, Instagram, and YouTube use these algorithms to sift through and organize all the content being posted which spans by the tens of millions a day. Algorithms analyze the user's internet traffic within the site to curate and personalize the user's feed. It notes the pages viewed, videos watched, photos liked, etc. The main goal of these algorithms is to increase the time spent by the user on the site. The monetization model of social media is also dependent on algorithms, the data collected per person is used to determine what ads to show the user.[8]

For the sixth consecutive year, the Philippines remained on top when it comes to social media usage.[9] In 2021, Filipinos spent about 4 hours and 15 minutes each day on social media, exceeding its record in 2020.[10] It is a far cry from the global average of 2 hours and 25 minutes, which makes Filipinos the best market for social media marketing.[11] This increase is largely attributed to the COVID-19 pandemic and the demand for information about the disease, news on its transmission, and its effects on society. Additionally, most students and people in the workforce were mandated to have work from home schemes, which heavily relied on the use of social media platforms to communicate.

---

[5] *Algorithmic Accountability: A Primer*, DATA AND SOCIETY 2 (Apr. 18, 2018), https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf.

[6] *Id.*

[7] Nathanael J. Fast & Arthur S. Jago, *Privacy Matters… Or Does It? Algorithm Rationalization, and the Erosion of Concern for Privacy*, 31 CURRENT OPINION IN PSYCHOLOGY 44, 45 (2020).

[8] Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L & TECH. 106, 124 (2019).

[9] Kyle Chua, *PH Remains Top in Social Media, Internet Usage Worldwide -report,* RAPPLER (Jan. 28, 2021, 3:15 P.M.), https://www.rappler.com/technology/internet-culture/hootsuite-we-are-social-2021-philippines-top-social-media-internet-usage/.

[10] *Id.*

[11] *Id.*

Undeniably, algorithms can be useful in making our experience in social media more personal. Consumption of content becomes streamlined and quicker when the things that align with our personal interests are the ones we see. However, issues arise when algorithms are used to influence the decisions of unwitting people and become the basis for manipulation and discrimination.

A perfect example of the dangers of algorithms is the recent scandal of Cambridge Analytica, a behavior change agency, as featured on The Big Hack.[12] Cambridge Analytica was exposed for collecting information of Facebook users from specific countries and profiling them for targeted political ads, which have been found to have influenced the Brexit referendum and the elections in the United States and the Philippines.[13] It is estimated that Cambridge Analytica has 5,000 data points per person logged in its system.[14] Its parent company, the SCL Group, a behavioral research, and strategic communications company, was found to have been involved with the elections of several developing countries since 1990.[15] Prior to that, the SCL Group was involved as a defense contractor to the U.S. Marines, where it experimented on psychological warfare.[16] Hence, SCL has been instrumental in major events across the globe where it has helped influence outcomes in favor of partisan groups for money. A study by Agudo and Matute confirmed that algorithms can be used to influence an individual's willingness to vote for a particular politician through explicit persuasion.[17] The same study concluded that algorithmic manipulation may also work on dating through covert persuasion.[18] This means that algorithmic suggestions can be used to change a person's perception and ultimately affect decisions and behavior.

Modern algorithms are used as a basis for decisions. Some sectors that have become highly automated involve the use of algorithms within decision-making processes that directly affect human rights. The concern is that algorithms are often "black boxed." Black boxing occurs when there are no external auditing or regulations for algorithms and the data it processes.[19] When algorithms are used to support a decision, such as a risk assessment or what ad to show on a person's screen, they may introduce or accentuate existing human rights challenges and pose new issues for accountability. Consequently, there is a need for transparency in the algorithmic process.

---

[12] THE BIG HACK, *supra* note 2.
[13] Paige Occeñola, *Exclusive: PH was Cambridge Analytica's 'petri dish' -Whistle-Blower Christopher Wylie,* RAPPLER, (Sept. 10, 2019, 2:57 PM), https://www.rappler.com/technology/social-media/239606-cambridge-analytica-philippines-online-propaganda-christopher-wylie/.
[14] THE BIG HACK, *supra* note 2.
[15] Vian Bakir, *Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting*, 5 FRONT. COMMUN. 1, 5 (2020).
[16] *Id.* at 6.
[17] Ujue Agudo & Helena Matute, *The influence of algorithms on political and dating decisions.* 16 PLOS ONE. 1, 11 (2021).
[18] *Id.*
[19] DATA AND SOCIETY, *supra* note 5, at 3.

This is made difficult by the very nature of an algorithm. An algorithm's learning process does not replicate human logic, which makes it difficult to comprehend and explain. Machine-learning models can also 'learn' in real-time, which means that comparable input data might produce different outputs over time.[20] As a result, these systems can be unpredictable, making it difficult to thoroughly examine and assess the impact of their use on human rights, and hence to effectively challenge judgments based on algorithms. While it is argued that human intervention alongside algorithms fills the gaps of what algorithms lack, human intervention may also provide additional bias and prejudice.[21] An algorithm designed to maximize profit in a platform where the main philosophy is human interaction presents a multitude of human rights concerns.

This paper examines how algorithmic systems impact human rights and the public and private regulations institutionalized to impose liability and control over intermediaries and algorithmic systems. While human rights do not apply to private persons, including the private entities involved in the design, building, and operating of algorithms, this paper examines the literature recommending international human rights law as an ideal framework for constructing subsequent algorithmic regulation. It must be noted that data-gathering or collection should go hand in hand with the discussion of algorithms. In the life cycle of algorithms, data gathering is a crucial part of training algorithms. Data is the bread and butter of algorithms; Without it, algorithms are meaningless equations and theories. Data impacts the design process of algorithms as the data fed to algorithms dictates the quality of the results. Hence, data collection and its contentious effects to human rights must be inseparable from algorithms.

RIGHT TO PRIVACY

An individual's right to privacy means a right against arbitrary or unlawful interference on an individual's privacy, family, home, and correspondence.[22] This is further refined by the UN Human Rights Committee to include the gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, should be regulated by law.[23] Every individual should be able to know what kind of information about them is being collected and for what purpose.[24] Additionally, he should be able to determine who has control over the information.[25] Algorithms need large amounts of data to

[20] Micheal Pizzi, Mila Romanoff & Tim Engelhardt, *AI for Humanitarian Action: Human Rights and Ethics*, 102 INTERNATIONAL REVIEW OF THE RED CROSS 145, 153 (2021).
[21] Raenette Gottardo, *Building Global Algorithmic Accountability Regimes: A Future-focused Human Rights Agenda Beyond Measurement,* 5 PEACE HUMAN RIGHTS GOVERNANCE 65, 68 (2021).
[22] International Covenant on Civil and Political Rights [ICCPR] art. 17, ¶ 1, *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171.; Universal Declaration of Human Rights, 9 G.A. Res. 217 (III) A, art. 12, U.N. Doc. A/RES/217 (III) (Dec. 10, 1948).
[23] U.N. Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy,)* ¶10, HRI/GEN/1/Rev.9 (Vol. I) (Apr. 8, 1988).
[24] *Id.*
[25] *Id.*

operate with utmost accuracy. The revelation of the Cambridge Analytica scandal revealed to the public that websites, such as Facebook and Google, have a surveillance-based business model that involves tracking personal internet history, profiling likes and interests, listening in to conversations, monitoring internet activity, etc.[26] This information is, in turn, sold to advertisers and companies to bombard the individual with targeted ads. Algorithms micro-profile individuals into subgroups and decide what ads to show based on the information collected.[27] The principal goal of algorithms is to predict the user's actions. Once it can predict the user's actions, it can conduct subliminal manipulation through specific ads and messages causing real-world behaviors and emotions to change. Change may be achieved depending on the client whether buying their product from an ad or swinging their votes in an election through a targeted message. This act of harvesting personal data violates the very essence of privacy and informational self-determination:[28] the control over one's personal information. An individual must be able to decide when and how his personal information is shared to others.

In *Davis v. Facebook, Inc.,*[29] it was found that the Facebook plugin tracks browsing histories of users, even after they have logged out from the site, and thereafter compiles them to a personalized profile to be sold to advertising companies. Such finding was considered to be a violation of several federal laws, specifically the anti-wiretapping laws and invasion of privacy. It was found that it is a valid ground to say that "Facebook's tracking and collection practices would cause harm or a material risk of harm to their interest in controlling their personal information."[30] Furthermore, it is also now valid to have a standing relying on Facebook's monetization of improperly collected user data constituting economic injury, namely, unjust enrichment, allowing plaintiffs to establish standing on several state law claims. This case reflects the changing attitude towards privacy litigation and algorithmic legislation moving forward.

Following the trend set by *Davis v. Facebook*, in June 2021, the same 9th Circuit Court Panel revived the 2018 class action *In re: Alphabet, Inc. Sec. Litig* which is a securities fraud class action against Alphabet Inc. for not disclosing a data privacy bug in the Google+ social network.[31] The court found that the plaintiffs had stated a potentially viable claim relating to the failure to inform investors of the issue.[32] In addressing public scrutiny from the Cambridge Analytica scandal, Justice Ikuta, who penned the decision, emphasized the need to be more stringent in punishing the lack of any new risk disclosures in light of the detection of cybersecurity issues. This reflects the international sentiment for stricter regulation.

[26] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, 18 (2019) https://www.amnesty.org/en/wp-content/uploads/2021/05/POL3014042019ENGLISH.pdf.
[27] Manheim & Kaplan, *supra* note 8.
[28] *Id.*
[29] Davis v. Facebook, Inc., 956 F.3d 589 (9th Cir., 2020) (U.S.).
[30] *Id.*
[31] In re Alphabet, Inc. Sec. Litig., No. 20-15638, slip op. at 9 (9th Cir., 2021) (U.S.)
[32] *Id.*

RIGHT TO FAIR TRIAL AND DUE PROCESS

Every human is entitled to equal protection of the laws, equal access to courts, and presumption of innocence.[33] The ICCPR provides:

> A hearing is not fair if, for instance, the defendant in criminal proceedings is faced with the expression of a hostile attitude from the public or support for one party in the courtroom that is tolerated by the court, thereby impinging on the right to defense, or is exposed to other manifestations of hostility with similar effects.[34]

Algorithms allow fake news to be broadcast to a multitude of people, and certain publicized cases become a hotspot for all sorts of news looking for attention and traffic.

The Dacera murder on New Year's Eve of 2021 spurred a number of social media content after she was found dead in a hotel after a night of partying with several male companions.[35] This was exacerbated by the fact that the police investigating themselves claimed that the case was solved under the assumption that her companions committed the crime.[36] The companions of Dacera received numerous flak from netizens,[37] who were outraged by the loss of Dacera purportedly under the hands of her trusted friends. Posts of sympathy and further conspiracy flooded Filipino feeds.

The right to fair trial and due process involves the media to avoid news coverage undermining the presumption of innocence.[38] However, this was not observed in the Dacera case as news stations and social media riding on publicity sensationalized the incident. There was coverage of the police chief consoling the victim's mother and assured her that they will bring the perpetrators of Dacera to justice.[39] In another interview with Dacera's mother, she was reported

[33] ICCPR, *supra* note 22, art. 14, ¶¶ 1-2.
[34] UN Human Rights Committee, *General Comment No. 32: Right to equality before courts and tribunals and to fair trial*, ¶25, CCPR/C/GC/32 (Aug. 23, 2007).
[35] Gus Bruno, *TIMELINE: The case of Christine Dacera, the flight attendant 'gang raped and murdered' at a NYE party,* 7 NEWS AUSTRALIA (Jan. 16, 2021, 7:06 A.M.), https://7news.com.au/news/court-justice/timeline-the-case-of-christine-dacera-the-flight-attendant-gang-raped-and-murdered-at-a-nye-party-c-1960725.
[36] Franco Luna, *With 9 Suspects Still At Large, Sinas Says Christine Dacera's Case Already 'Solved',* PHIL. STAR (Jan. 5, 2021, 11:18 A.M.), https://www.philstar.com/nation/2021/01/05/2068331/9-suspects-still-large-sinas-says-makati-rape-slay-case-already-solved.
[37] Robert Requintina, *Celebrities, netizens seek justice for death of Christine Dacera,* MANILA BULL., (Jan. 5, 2022, 12:27 A.M.), https://mb.com.ph/2021/01/05/celebrities-netizens-seek-justice-for-death-of-christine-dacera/.
[38] UN Human Rights Committee), *supra* note 33 at par¶ 30.
[39] CNN Philippines, *Sinas tells suspects in Dacera's alleged rape-slay: 'We will hunt you down'*, CNN PHIL. (Jan. 6, 2021, 8:03 A.M.), https://cnnphilippines.com/news/2021/1/6/Christine-Dacera-case-PNP-Sinas.html?fbclid=IwAR2gdR6CjGKqe2aIu9RM5RKyyTEjUnNhou7Niggdxr9cPmPE-E2ZlV_Ntgc.

accusing specific friends of Dacera as the perpetrators of the crime.[40] This assertion, coupled by the initial allegations that the companions were the perpetrators, did not bode well in social media. Clearly, the rights of the accused were violated by the sensationalism and the partiality of the police against them. Subequently, the court dismissed the case against the accused after evidence showed no foul-play which caused the death of Dacera. However, damage was already inflicted on the reputation and families of the accused.[41]

This is not a lone case as there have been several instances of "red-tagging" or the branding of an individual as subversive, left-leaning, communist, or terrorist, being committed in social media.[42] Identified personalities are then harassed or even persecuted when the algorithm makes it public enough.

The military or paramilitary use red-tagging as means to silence or cause human rights violations on vocal dissenters of the government.[43] Human rights groups and activists are often branded as the "legal front" of enemies of the State, which threatens the lives, liberty, and security of innocent individuals.[44] Red-tagging can take the form of speeches from government agents, presentations and pamphlets distributed to the public, and content in social media by government officials and members of the security sector.[45] When red-tagging officials have a platform in social media which is further amplified by algorithms, more individuals will have a distorted perception and attitude towards activists and human rights defenders.

DISCRIMINATION

An individual is protected against any advocacy that incites discrimination, hostility, or violence.[46] The principle of non-discrimination is coupled with the rights to equality and equal access to the law and its protection.[47] The system of profiling in social media seeks to divide people

[40] Dexter Cabalza, Krixia Subingsubing & Tina G. Santos, *Mother stil suspects foul play in Christine Dacera's* death, PHIL. DAILY INQ. (Jan. 13, 2021, 04:43 A.M.), https://newsinfo.inquirer.net/1382977/mother-still-suspects-foul-play-in-christine-daceras-death.
[41] Jairo Bolledo, *Dacera mom, others face libel and multiple complaints from suspects,* RAPPLER (Mar. 25, 2021, 08:10 P.M.), https://www.rappler.com/nation/dacera-mother-others-face-complaints-suspects-christine-death/.
[42] Pauline Macaraeg, *Gov't platforms being used to attack, red-tag media,* RAPPLER (May 12, 2020, 12:48 P.M.), https://www.rappler.com/newsbreak/investigative/260602-government-platforms-being-used-attack-red-tag-media/, Gabriel Pabico Lalu, *Some cops still red-tagging on social media despite PNP chief's warning,* PHIL. DAILY INQ. (Jun. 11, 2020, 4:20 A.M.), https://newsinfo.inquirer.net/1289609/did-gamboas-warning-about-cops-social-media-use-fall-on-deaf-ears.
[43] Commission on Human Rights, Report on the Situation of Human Rights Defenders in the Philippines, at 23, http://chr.gov.ph/wp-content/uploads/2020/07/CHRP-2020-Report-on-the-Situation-of- Human-Rights-Defenders.pdf.
[44] *Id.*
[45] *Id.* at 28.
[46] ICCPR, *supra* note 22, art. 20, ¶ 2.
[47] UN Human Rights Committee (HRC), *CCPR General Comment No. 18, par.1: Non-discrimination*, HRI/GEN/1/Rev.9 (Vol. I) (Nov. 10. 1989).

based on their interests and beliefs – beliefs that may or may not be discriminatory. Algorithms bring about similar content and similar people together. To prolong the user's interest and traffic in the site, Facebook has allowed discriminatory content to spread in their domain.[48] Discriminatory groups, such as white supremacy followers and terrorist groups, such as the Hamas members in *Force v. Facebook,*[49] as well as other extremist groups with harmful and prejudiced ideologies, use social media as a platform to converge, plan attacks, and spread hateful doctrine, malicious information, and harmful content.

In 2018, Facebook settled five class action lawsuits for discrimination filed by several civil rights organizations, labor groups, workers, and consumers when it allowed its ad platform to be used by advertisers for housing, employment, or credit (HEC advertisers) to discriminate based on race, national origin, ethnicity, age, sex, sexual orientation, disability, family status, or other characteristics.[50] Particularly, the ability of HEC advertisers to include or exclude Facebook users from receiving their ads based on their sex or age, or based on interests, behaviors, or demographic, the ability of HEC advertisers to set a narrow geographic area so that only Facebook users within that area would receive the ads, and Facebook's Lookalike Audience tool that allowed an advertiser to create audiences of Facebook users that had common characteristics with the advertiser's current customers or other groups.[51] One of the direct consequences is that targeted ads committed discrimination by showing one demographic certain housing offers, while another showed none or a different less attractive offer.[52] Facebook has already undertaken steps to inflict changes addressing the discrimination caused in pursuit of its settlement. While possibly harmless to an unsuspecting individual, no person should be subjected to any type of discrimination, despite the fact that they might be unaware of its ongoing occurrence. An unknowing victim should not be a reason to allow discrimination to continue.

Another example of algorithms being used as tools for discrimination comes from Amazon, where it was found that they used an algorithm to sift through thousands of job applicants to procure the best candidates. The said algorithm skewed heavily on male applicants; thereby severely discriminated against candidates of other genders.[53]

It must be reiterated that while algorithms are created to be objective, standard, and unbiased, they merely reflect the training data inputted. Hence, several types of bias can arise, such as technical bias, representation bias, emergent bias, etc.[54] Human resource recruitment algorithms can be inherently biased once an algorithm is trained on historical employment data, integrating

[48] Amnesty International, *supra* note 26, at p. 37.
[49] Force v. Facebook, Inc., 934 F.3d 53 (2nd Cir. 2019) (U.S.).
[50] Mobley et al. v. Facebook (N.D. Cal.), National Fair Housing Alliance et al. v. Facebook (S.D.N.Y.), Communications Workers of America et al. v. Facebook (EEOC), Spees et al. v. Facebook (EEOC), Riddick v. Facebook (N.D. Cal.)
[51] *Id.*
[52] *Id.*
[53] Alina Kochling & Marius Claus Wehner, *Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development*, 13 BUSINESS RESEARCH, 795-848 (2020), https://doi.org/10.1007/s40685-020-00134-w.
[54] *Id.*

implicit bias favoring previous bias of recruiters.[55] This is one of the many instances where algorithms become integrated into systems that influence decisions impacting human lives. This makes it necessary for companies to divulge to affected individuals whether an algorithm was used in decision-making process and the parameters set.

FREEDOM OF EXPRESSION

It is provided in the International Covenant on Civil and Political Rights (ICCPR) that the freedom of expression includes the right to seek, receive, and impart information of all kinds in all forms of media.[56] Search engines may violate this right by acting as the gatekeeper to websites. Only websites that are within its registry or ranked highly are those that can be featured or seen by a large audience. This causes bias towards certain news outlets or content creators resulting in polarization and diminution of social cohesion.[57] Grouping this bias upfront endangers media pluralism and diversity among opinions.[58] The intended effect is a delight for fake news and conspiracy theories which have both risen in the past decade. While not new to the world, the increased use of the internet and social media has made the creation and consumption of fake news rampant. Algorithms have given fake news and conspiracy theorists a platform to further their audience reach. As more people watch, search, comment, like, and interact with these types of content, algorithms propel them further up for more people to access and conferring a sense of legitimacy. It is found that fake news is 70% more likely to be retweeted than real news and facts that may take up more than six times longer to reach people.[59] Even when fake news or the conspiracy seems highly improbable, the user tends to feel that all signs lead to some hidden truth when the recommendations of subsequent videos or articles all have similar content.[60]

Algorithm can be used for good when it is used to determine and remove hate speech, discrimination, and track opinions that may incite or lead to the commission of a crime. However, filtering of speech to eliminate harmful content through algorithms faces a high risk of over-blocking and removing speech that is not only harmless but can also contribute positively to the public debate. This again removes plurality and diversity in opinion and replaces it with a cohesive and homogenous albeit suppressive and controlling form of media.

---

[55] *Id.*
[56] ICCPR, *supra* note 22, art. 19.
[57] Committee Of Experts On Internet Intermediaries, *Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications,* COUNCIL OF EUROPE 17, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.
[58] *Id.*
[59] Holly Latham, *Fake News and Its Implications for Human Rights,* HUMAN RIGHTS PULSE (Dec. 14, 2020), https://www.humanrightspulse.com/mastercontentblog/fake-news-and-its-implications-for-human-rights.
[60] Molly Mastantuono, *The Mathematics of Misinformation*, BENTLEY UNIVERSITY (Aug. 19, 2021), https://www.bentley.edu/news/mathematics-misinformation.

RIGHT TO FREE ELECTIONS

The Universal Declaration of Human Rights (UDHR) and the ICCPR highlight an individual's right to free, fair, regular elections without any undue influence or coercion of any kind.[61] Voters are also entitled to accurate and truthful information from electoral candidates. Their opinions and preferences should be able to develop independently from fraudulent machinations that may induce or manipulate a voter to have an inaccurate idea of certain candidates, whether positive or negative. The biggest example is the Cambridge Analytica scandal, where it was found that in the 2016 U.S. elections, the same was microtargeting certain individuals from around the U.S., particularly those from "swing states", to bombard with political and suggestive ads in favor of a particular candidate or party.[62]

In the Philippines, during the 2019 midterm elections, it was observed that massive disinformation campaigns in social media were being utilized. Underground operations of mobilizing coordinated click and troll armies to catch public attention and disseminate derogatory narratives.[63] Additionally, candidates from various sides and ideologies were found to employ emotionally manipulative and misinformative propaganda. There were also cases of hypernationalism and historical revisionism from various micro and non-influencers, including political parody accounts, pop culture accounts, and thirst-trap Instagram influencers.[64] Another example of micro media manipulation is the expansion of "alternative" news pages and content across social media platforms peddling themselves as a source of unbiased and unfiltered truth, while simultaneously disparaging mainstream news media outlets.[65] Hyper-partisan news channels continue to present themselves as legitimate news sites, while manufacturing more false legitimacy.[66] Meanwhile, local news pages toe the line between neutral and partisan by slipping political propaganda, such as track records and plans or promises.[67]

Algorithms make these types of content reachable to a broader audience. Without regard to the authenticity of the content, social media allows content that are seemingly reputable to proliferate to the detriment of the electoral process and the right of the individual to be accurately informed of candidates. This ultimately leads to the destruction of democracy and the

[61] ICCPR, *supra* note 22, art. 25, U.N. Human Rights Committee, *CCPR General Comment No. 25: Article 25*, ¶19, U.N. Doc. CCPR/C/21/Rev.1/Add.7 (July 12, 1996).
[62] THE BIG HACK, *supra* note 2.
[63] William Emmanuel Yu, *A Framework for Studying Coordinated Behavior Applied to the 2019 Philippine Elections*, ARCHIUM ATENEO, 8-10 (2021).
[64] Jose Mari Lanuza, Jonathan Corpus Ong, Ross Tapsell, *Evolutions of "Fake News" from the South: Tracking Disinformation Innovations and Interventions between the 2016 and 2019 Philippines Elections* 2-3 (Submission to Harvard University Disinformation in Comparative Perspective Workshop) (on file with the Harvard University), https://cyber.harvard.edu/sites/default/files/2019-11/Comparative%20Approaches%20to%20Disinformation%20-%20Jose%20Mari%20Hall%20Lanuza%20Slides.pdf,
[65] *Id.*
[66] *Id.*
[67] *Id.*

determination of truth because artificial intelligence does not know truth, merely unverified data collected from various sources. Artificial intelligence cannot distinguish between fact and fiction. Governments will crumble, and political parties in shambles when no form of fact-checking can be conducted. It becomes harder to support any ideology when it cannot be ascertained whether one is correct or not.

RIGHT TO HEALTH

The right to health is the most important right being impacted by the irresponsible use of algorithms in social media during this time of the COVID-19 pandemic. This is the first pandemic where majority of the global population is interconnected via the internet and social media. People became increasingly dependent on social media for information regardless of its legitimacy. The International Covenant on Economic, Social, and Cultural Rights (ICESCR) provides that every human is entitled to the enjoyment of the highest attainable health.[68] In times of an epidemic, signatory states are required to take measures to prevent, treat, and control epidemic diseases.[69] Signatories must provide accurate education and information concerning an epidemic, including methods of preventing and controlling them.[70] The right to accessibility of health facilities, goods, and services includes the right to seek, receive and impart information and ideas concerning health issues.[71] The COVID-19 pandemic is still amidst the Philippines after two years. In the early parts of the pandemic, there was a clamor for information about transmission, symptoms, variants, vaccines, and statistics. There were inconsistencies in the tracking of infected individuals wherein there would be regular "mass recoveries" reported by the government's health agency which were highly irregular.[72] It is exacerbated by the fact that crucial information about the pandemic is being politicized. The government's Department of Health and Inter-Agency Task Force (IATF) would issue proclamations and guidelines that were not up to the standard of the World Health Organization (WHO), such as the continued mandatory use of face shields, which were eventually ruled out by WHO as unnecessary, despite the persistence of the government of its use.[73] While the government has since then made the face shield use 'voluntary', controversy arose when news about the government overspending on pandemic funds to finance overpriced face shields came

[68] International Covenant on Economic, Social and Cultural Rights art. 12, opened for signature Dec. 19, 1966, 993 U.N.T.S. 3.
[69] Committee on Economic, Social and Cultural Rights, *General Comment No. 14: The right to the highest attainable standard of health (article 12 of the International Covenant on Economic, Social and Cultural Rights)*, ¶44(c), U.N. Doc. E/C.12/2000/4 (Aug. 11, 2000).
[70] *Id.* ¶ 44(d).
[71] *Id.* ¶12(b).
[72] Gabriel Pabico Lalu, *What Mass Recovery? Escudero Joins Calls for Duque's Firing,* PHIL. DAILY INQ. (Jul. 30, 2020, 11:09 P.M.), https://newsinfo.inquirer.net/1314658/mass-recovery-escudero-joins-calls-for-duques-firing.
[73] Dwight de Leon, *Isko Moreno Urges Gov't to Drop 'Face Shield' Policy*, RAPPLER (Jun. 2, 2021, 5:58 P.M.), https://www.rappler.com/nation/isko-moreno-message-philippine-government-drop-face-shield-policy/.

out.[74] Questions arise on whether the information spreading on the mandatory use of face shields was merely a ruse to cover up its exuberant costs.

Improper dissemination of information on the pandemic costs lives, jobs, and money. Misinformation about the safety and efficacy of the vaccines and the use of Ivermectin as an alternative are just a few examples of dangerously inaccurate information jeopardizing the lives of Filipinos.[75] In the U.S., theories and arguments attempting to debunk the COVID-19 pandemic have spread around in social media such as Facebook and TikTok.[76] This has led hundreds of civilians protesting their rights against vaccination and spreading hate against those who are pro-mask and pro-vaccine. Arguably, if proper information were broadcasted in social media, the status of the pandemic would most likely be better than what it currently is.

INTERMEDIARY REGULATION

With the rise of social media platforms, states have increasingly sought to regulate speakers indirectly by relying on a variety of measures to influence the content moderation practices of social media companies. In the Philippines, there are currently no intermediary regulation laws in the country; however, there are plans by senators and government agencies to impose regulations on specific aspects in social media.[77] In the U.S., there is a large pressure on the legislature to enact laws regulating the power and freedom granted to big tech companies or intermediaries to hold them accountable for spreading fake news, racist and discriminative content, and other harmful substances. However, legal experts are cross between the constitutional rights that might possibly be affected by it.[78]

A bill proposing regulation of companies like Facebook might not survive challenges concerning freedom of expression as it might alter how speech is promoted in the site. Previous

[74] Mara Cepeda, *LIST: Everything You Need to Know About the Pharmally Pandemic Deals Scandal*, RAPPLER (Dec. 17, 2021, 8:00 A.M), https://www.rappler.com/newsbreak/iq/list-everything-need-to-know-pharmally-covid-19-pandemic-deals-scandal/.

[75] Nini Cabaero, *Cabaero: Death Blow on Use of Ivermectin*, YAHOO NEWS (Aug. 30, 2021), https://ph.news.yahoo.com/cabaero-death-blow-ivermectin-100000910.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAN2B47J1HVII7cICbGwLeGnx2VQMjIOkcRamrZhI3-IM4CBwjQoeXOwTpFcjEAlUdo4qby5-2NtApNg_br-BAiE_ez1Y8XGeMGEMqmag-8v3T75pyQ68LgePrqdMpFr_qxSdfiRlO_X593ee7S0hZFtv4hmHzdbkwYtMeSqfUaVk.

[76] Jamie Grierson, Dan Milmo, & Hibaq Farah, *Revealed: Anti-vaccine TikTok Videos Being Viewed by Children As Young As Nine,* THE GUARDIAN (Oct. 8, 2022, 7:15 P.M.), https://www.theguardian.com/technology/2021/oct/08/revealed-anti-vaccine-tiktok-videos-viewed-children-as-young-as-nine-covid.

[77] Loreben Tuquero, *Drilon Eyes Law Requiring Social Media Platforms to Reveal Identities of 'Trolls',* RAPPLER (Dec. 9, 2021, 4:28 P.M.), https://www.rappler.com/nation/national-news/drilon-eyes-law-requiring-social-media-platforms-reveal-identities-trolls/.

[78] Julia Zorthian, *Washington Wants to Regulate Facebook's Algorithm. That Might Be Unconstitutional,* TIME (Oct. 13, 2021, 1:44 P.M), https://time.com/6106643/facebook-algorithm-regulation-legal-challenge/.

suits calling accountability against Facebook have failed because, as affirmed by the courts, restrictions from distribution of speech are restrictions of speech themselves.[79] Social media platforms rely on Sec. 230 (c)(2) of the United States Decency Act of 1996 to not be personally liable for the content posted on their platforms, which reads: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[80]

In other words, online intermediaries that host or republish content are shielded from a string of regulations that could, otherwise, hold them liable for what others say and do. Protected intermediaries include, not only traditional Internet Service Providers (ISPs), but also a variety of "interactive computer service providers,"[81] which includes any online service that distributes third-party content such as Facebook, TikTok, and Google. Despite the concerns of fake news and discrimination in social media, Sec. 230(c)(2) establishes a broad level of protection that has enabled internet innovation and free speech to thrive.

Other countries have their own version of Sec. 230(c)(2): Art. 14 and 15 of Directive 2000/31/EC and the updated Directive on Copyright in the Digital Single Market for the European Union, The e-Commerce Directive of 2000 for Italy, the Defamation Act in the United Kingdom, and several landmark cases from Australia, France, and New Zealand demonstrate some form of liability reduction in favor of intermediaries. Because of the concern on the lack of intermediary liability, there are continuing efforts to repeal or bypass these intermediary protection laws.

To regulate speech by means of formal legislation, States predominantly rely on two regulatory mechanisms for this purpose: *first,* content restriction laws, which define categories of content that are illegal in particular domestic and regional contexts and, *second,* intermediary liability laws, which establish the conditions under which intermediaries, including social media companies, may be held liable for unlawful content generated by their users.[82] As creators and operators of algorithms, intermediary liability laws are the most apt type of legislation to regulate companies like Facebook and Google.

Zeroing on intermediary liability laws, there are three common approaches to intermediary liability in democratic countries outside the United States: *first,* the awareness or "actual knowledge" approach, practiced in Australia, India, Japan, and the Philippines, *second,* the notice and takedown approach, applied in New Zealand and South Africa, and *lastly,* the "mere conduit"

[79] *Id.*
[80] Communications Decency Act, 47 U.S.C. § 230 (c)(2) (1996).
[81] *Id.* at § 230 (a)(5).
[82] Barrie Sander, *Democratic disruption in the age of social media: between marketized and structural conceptions of human rights law*. 32 THE EUROPEAN JOURNAL OF INTERNATIONAL LAW 151, 166 (2021).

approach in EU, South Africa, and India".[83] Furthermore, some countries have enacted legislation that deals with intermediary liability for certain types of harmful content for the removal of content, similar to Sec 230(c)(2) in the United States.[84] However, the conflict arises in tempering these legislations from a litany of circumstances depending on geography, usage, culture, and so on to avoid blanket bans that generally lack sufficient precision to be compatible with the legality test and necessity test found in Art. 19 (3) of the ICCPR.[85]

The problem with most legislations about intermediary liability is that it focuses on violation of freedom of expression and discrimination. It merely seeks the removal of harmful content created by individuals, but it does not regulate how algorithms are designed to allow such content to be disseminated. It merely touches on one implication of algorithmic involvement within the social media ecosystem. On the issue of privacy, Cambridge Analytica, Facebook, Google, etc. were able to tap into the personal information of people, monetize such data, and find subtle ways to manipulate users because there was no legislation regulating it. This is mostly attributed to the lack of knowledge lawmakers have on the subject matter. In fact, less than 20% of people in the tech industry fully understand how algorithms operate.[86] This is coupled with the fact that mining of information and incorporation of ads are so subtly integrated that the average individual would never notice anything irregular.

To date, the General Data Protection Regulation (GDPR) of the European Union (EU) is the most stringent privacy and security law in the world. Besides state parties to the EU, there are only 16 countries that have comparable legislation, to which neither the U.S. nor the Philippines belong.[87] However, it makes reservations in favor of Directive 2000/31/EC, which lessens liability from intermediaries. While it is not an intermediary nor algorithm-specific legislation, the GDPR imposes heavy obligations for data controllers and data processors. In fact, in the 2021 landmark decision of *Facebook Inc., v. Gegevensbeschermingsautoriteit*[88] of Belgium, the Court of Justice of the European Union (CJEU) affirmed that national supervisory authorities (NSA)in any EU country can enforce the General Data Protection Regulation (GDPR) against a company, provided that the GDPR confers them the authority to make a finding of GDPR infringement and that they exercise that power in accordance with the cooperation and consistency procedures under the GDPR.[89] The CJEU also clarified that acting by itself, NSAs can handle complaints lodged with it, concerning a cross-border processing of personal data or a possible infringement of that

[83] Ashley Johnson & Daniel Castro, *How other countries dealt with intermediary liability*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Feb. 22, 2021), https://itif.org/publications/2021/02/22/how-other-countries-have-dealt-intermediary-liability.
[84] *Id.*
[85] Sander, *supra* note 74, at 168.
[86] THE SOCIAL DILEMMA, *supra* note 1.
[87] Mike Woodward, *16 Countries with GDPR-like Data Privacy Laws*, SECURITY SCORECARD (Jul. 8, 2020), https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws.
[88] C-645/19, Facebook Inc., v. Gegevensbeschermingsautoriteit (Jun. 15, 2021).
[89] *Id.*

regulation, provided that the subject matter relates only to an establishment in its own Member State or substantially affects data subjects only in that Member State.[90] NSAs are also allowed to adopt provisional measures on its territory if it considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects.[91] The decision marks the conclusion of a six-year battle between Facebook and the Belgian privacy authorities, which ordered Facebook to stop using cookies and hidden monitoring techniques to track Belgians (even those without Facebook accounts) across the internet in 2015.

In recent years, the value of personal data has reached a global peak, while companies are earning trillions annually by selling such data. The user has increasingly become the product for companies to sell to advertisers. Hence, legal experts call that people should be able to control their own data like their own property.[92] Their consent must be obtained if data will be gathered, stored, and subsequently disposed. Adequate legislation should be instituted to ensure that no clandestine operation will be committed to mine an individual's data and to use it for compensation or whatsoever without the consent of the owner. There has yet to be a framework or a comprehensive law that seeks to regulate algorithms throughout their lifecycle and the different aspects affected by them which spans not only discrimination and free expression, but other matters such as privacy and residual effects, etc.

PUBLIC REGULATION OF ALGORITHMS

The regulatory and policy landscape for algorithms and AI is an emerging issue in different jurisdictions globally. It has only seen minor applications involving credit facilities, but it has yet to touch on social media platforms. There have been several bills filed in the U.S. Congress over the past years involving the word "algorithm" in its name. However, it seeks to primarily regulate speech and address problems within Sec. 230 of the Communications Decency Act.

As of 2019, there have been bills introduced in the U.S. Congress that center on the impact of algorithms, among which is "Algorithmic Accountability," which refers to "the assignment of responsibility for how an algorithm is created and its impact on society; if harm occurs, accountable systems include a mechanism for redress."[93] Algorithms are inventions of both humans and machine learning. Humans design algorithms, they decide the output of algorithms, and they are the ones interpreting and assessing the results. In the end, the final decisions on an

[90] *Id.*, EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. art. 56(2).
[91] *Id.* at art. 66.
[92] Chad Jones & Christopher Tonetti, *Consumers Should Own Their Data*, VOX EU CEPR (Jul. 28, 2020), https://voxeu.org/article/consumers-should-own-their-data.
[93] DATA AND SOCIETY, *supra* note 5, at 10.

algorithmic system released belong to the technology's designers and company. Hence, while algorithmic accountability regulates algorithms, it still places liability on the intermediaries as operators, making it a form of intermediary liability law.

Tackling the recommendation that countries develop a legislative basis to restrict companies from the uncontrolled use of personal data in social networks,[94] the Algorithmic Accountability Act[95] was introduced in April 2019 by Senator Cory Booker, Senator Ron Wyden, and Representative Yvette Clark. It directs the Federal Trade Commission (FTC) to develop regulations requiring large firms to conduct impact assessments for existing and to-be-released "high-risk automated decision systems."[96] High-risk automated decision systems are a broad concept and encompass a wide range of automated systems, including those that pose a "significant risk" to individual data privacy, security, as well as those that result in biased or unfair decision-making; those that make decisions that have a significant impact on users using data about "sensitive aspects," such as work performance and health; those that involve personal data like location, family, race, political and religious beliefs, gender identity and sexual orientation, and genetic information; or those that monitor a large public space.[97]

These impact evaluations would look at how an automated system is created and operated, as well as the training data, the threats it poses to privacy and security, and other aspects.[98] Companies would be expected to resolve the issues raised by these assessments in a reasonable manner, but they would not be required to reveal the results of these impact assessments.[99] Failure to comply, on the other hand, would be regarded as an unfair or misleading act under the Federal Trade Commission Act, making regulatory action justifiable.[100]

In May 2021, Senator Edward J. Markey and Congresswoman Doris Matsui introduced the Algorithmic Justice and Online Platform Transparency Act of 2021 to prohibit harmful algorithms, increase transparency into websites' content amplification and moderation practices, and commission a cross-government investigation into discriminatory algorithmic processes throughout the economy.[101] It seeks to cover what the 2019 bill lacked. Sections 4-7 of the bill provide the important provisions that the bill seek to enact: the prohibition of algorithmic process that discriminates,[102] the establishment of a safety and effectiveness standard for algorithms,[103] the

[94] Elena Boldyreva, *Cambridge Analytica: Ethics and Online Manipulation with Decision-Making Process,* THE EUROPEAN PROCEEDINGS OF SOCIAL & BEHAVIORAL SCIENCES 91-102. (2018).
[95] Algorithmic Accountability Act of 2019, H.R.2231, 116th Congress (U.S.) (2019).
[96] *Id.* at § 3(b)(1)(A)
[97] *Id.* at § 2(2)(7)
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] Algorithmic Justice and Online Platform Transparency Act of 2021, S.1896, 117th Congress (U.S.) (2021).
[102] *Id.* at § 6(a).
[103] *Id.* at § 6(d).

requirement of online platforms to inform users the algorithmic process employed and information collected,[104] the requirement of online platforms to maintain detailed records of their algorithmic process to be reviewed by the FTC,[105] the compliance with key privacy and data de-identification standards,[106] the requirement of online platforms to publish annual public reports of their content moderation process,[107] and the creation of an inter-agency task force comprised of several government entities to investigate the discriminatory algorithmic process.[108]

Nevertheless, both bills are criticized for not fully understanding the nature of algorithmic systems. First, it only targets automated high-risk decision-making, rather than all high-risk decision-making.[109] Second, it fails to consider the non-linear nature of software and process development and deployment.[110] Third, it limits the scope to certain companies within a revenue threshold.[111] Lastly, it does not require impact assessments to be public out of respect for the importance of protecting proprietary information.[112]

While the current attempts to impose liabilities to algorithm-operating intermediaries provide an element of accountability, their concentration on various components of the broader algorithmic process makes them deficient. Instead, due to the complexity of algorithmic decision-making, accountability proposals must be placed inside a larger framework that addresses the entire algorithmic life cycle, from conception and design to actual deployment and use of algorithms in decision-making.[113] It is necessary to devote more attention to the scope and implementation of states' obligations, as well as the expectations imposed on intermediaries in terms of prevention, oversight, accountability, and remedies.[114]

PRIVATE REGULATION OF ALGORITHMS

Intermediaries, in compliance with the law and public safety, have their own system of regulating content within their respective platforms such as removing it, sending warning notices, fact-checking, or algorithmically making it less accessible to people. They have the power to choose which accounts to suspend, block, or remove entirely. A necessary consequence of this is

[104] *Id.* at § 4(a)(1).
[105] *Id.* at § 4(a)(2)(C).
[106] *Id.* at § 4(a)(2)(B)(i).
[107] *Id.* at § 4(b)(2)(A).
[108] *Id.* at § 7.
[109] Joshua New, *How to Fix the Algorithmic Accountability Act*, CENTER FOR DATA INNOVATION (Sept. 23, 2019), https://datainnovation.org/2019/09/how-to-fix-the-algorithmic-accountability-act/.
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] Lorna McGregor, Daragh Murray, &Vivian Ng, *International Human Rights Law As A Framework For Algorithmic Accountability*. 68 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY, 309-343 (2019).
[114] *Id.*

that they can choose to remove valid expressions or be ignorant of others abusing their freedom of expression to an extent that encroaches on the rights of others.

For this purpose, companies have their own set of guidelines or rules. These rules are frequently changed by their own instance, by public response, or by court order. Some rules are made transparent to the users while some detailed rules are kept hidden. Because of human error in manually sifting through content causing public uproar, intermediaries have employed several measures to address this; hiring more moderators, institutionalizing algorithms that detect and remove harmful content, and constantly adjusting their guidelines.[115]

While there are no known intermediaries that have a transparent and independent body reviewing their algorithms, Facebook's unprecedented Oversight Board may soon apply it.[116] Comprising of various personalities, such as former political leaders, human rights activists, and journalists, the Oversight Board is created to be an independent tribunal for content moderation on Facebook and Instagram. It has the power to create precedent-setting rulings and offer recommendations to improve Facebook's Community Standards.[117] Its main sources for its rulings are Facebook's Community Standards, Facebook Values, United Nations Guiding Principles on Business and Human Rights (UNGPs), ICCPR, ICERD, CRC, among others. Legal experts view it as a necessary implication in order to establish the authority and legitimacy of the Oversight Board that its scope includes the power to conduct independent audits of Facebook's algorithms and automated content moderation platforms.[118]

INTERNATIONAL HUMAN RIGHTS LAW AS FRAMEWORK FOR REGULATING ALGORITHMS

A human rights-based approach to algorithmic accountability has been theorized by various legal experts.[119] *McGregor et al.,* provided a framework using International Human Rights Law (IHRL) for the design, development of algorithms.[120] They argued that IHRL is an effective framework to ensure that States and businesses can adequately protect and prevent violating human

[115] Susan Benesch, *But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies,* 38 YALE JOURNAL ON REGULATION BULLETIN 86, 88 (2020).
[116] Alex Hern, *Alan Rusbridger says Oversight Board will ask to see Facebook's algorithm,* THE GUARDIAN, (Mar. 2, 2021, 7:21P.M.), https://www.theguardian.com/technology/2021/mar/02/alan-rusbridger-says-oversight-board-will-ask-to-see-facebooks-algorithm; *Edward L. Pickup, The Oversight Board's Dormant Power to Review Facebook's Algorithms*, 39 THE YALE JOURNAL ON REGULATION BULLETIN 1, 4-10 (2021).
[117] Nick Clegg, *Welcoming the Oversight* Board, META (May 6, 2020), https://about.fb.com/news/2020/05/welcoming-the-oversight-board/.
[118] Michael Lwin, *Applying international human rights law for use by facebook*. 38 YALE JOURNAL ON REGULATION BULLETIN (2020).
[119] Nathalie Smuha, *Beyond a human rights-based approach to ai governance: promise, pitfalls, plea,* PHILOSOPHY & TECHNOLOGY (2020), https://doi.org/10.1007/s13347-020-00403-w.
[120] McGregor et al., *supra* note 93.

rights.[121] This is a framework that can accommodate other approaches to algorithmic accountability—including technical solutions—and which can grow and be built on as IHRL itself develops, particularly in the field of business and human rights.

McGregor et al.[122], as well as the study of *Pizzi et al.*,[123] provided reasons why an IHRL framework contributes to the algorithmic accountability discussion, to wit:

First, IHRL is universal. It offers a common system and a set of principles that can be applied in every country, ensuring AI fulfills the values in UDHR, ICCPR, and other international instruments.[124] It fills a gap in existing discourse by providing a means to define and assess harm.

Second, it imposes specific obligations on States and expectations on businesses to prevent and protect human rights and sets out the mechanisms and processes required to give effect to or operationalize these obligations and responsibilities.[125] It also has established accountability and advocacy mechanisms in place, such as the HRC and treaty bodies, complaint systems, and judicial systems that can conduct investigations and review the performance of States.[126]

Third, the IHRL framework can map on to the overall algorithmic life cycle. Thus, it provides a means for assessing the distinct responsibilities of different actors across each stage of the process. IHRL, therefore, establishes a framework capable of capturing the full algorithmic life cycle from conception to deployment.[127]

Fourth, IHRL uses an analytical lens with regard to the right holder and duty bearer in a given circumstance, which has easier and more realistic real-world applications. Instead of weighing on fairness between conflicting sides, IHRL calls on developers and operators of algorithms to focus on who will be impacted by the implementation of algorithms and whose fundamental rights are affected.[128]

Fifth, IHRL and human rights jurisprudence provide a basis for balancing rights in periods of conflict. This is applicable in instances where implementing an algorithm or technology comes with both risks and benefits, which may affect several rights simultaneously. IHRL provides a guide in tempering the balance between how and when fundamental rights can be restricted.[129]

---

[121] *Id.*
[122] *Id.*
[123] Pizzi et al., *supra* note 20.
[124] *Id.* at 162.
[125] McGregor et al., *supra* note 93.
[126] Pizzi et al, *supra* note 20, at 162.
[127] McGregor et al., note 93, at 327.
[128] Pizzi et al., *supra* note 20, at 162.
[129] *Id.* at 163.

Fifth, an IHRL framework can help determine if algorithmic decision-making should be forbidden, and whether such a limitation is permanent or only temporary in a certain decision-making setting. IHRL prohibits the use of an algorithm in decision-making if the goal or effect of its use would be to bypass IHRL, even if it is done inadvertently.[130]

Lastly, certain decisions made solely on the basis of an algorithm, without the possibility of human involvement, may be prohibited by IHRL. When a decision relying on algorithms infringes on an individual's rights, the underlying reasoning must be based on factors that are particular and applicable to that individual.[131] This stems from IHRL's primary principle of prohibiting interference of arbitrary rights, and is thus, applicable to any decisions that have the potential to infringe on specific rights. [132]

The increasing complexity of algorithms has led them to be unpredictable and difficult to control.[133] This has resulted in some arguing that humans or intermediaries should have less responsibility for algorithmic consequences that they could not have predicted. From an IHRL perspective, this does not diminish the responsibility of human operators as they made the decision to design and deploy the algorithms with an understanding that there will be outcomes beyond their control. Algorithms are not neutral, but are profoundly "value-laden" entities. Accordingly, they create moral consequences and ethical dilemmas, and affect the designation of roles and responsibilities within algorithmically-assisted decision-making processes, where 'humans in the loop,' as well as those outside of it, are also affected. [134] Intermediaries cannot evade their responsibilities in this regard for value-laden algorithms themselves or for design-based decisions that assign roles and responsibilities. Using an IHRL framework, designers are required to build human rights protections, so that in instances that algorithms act abnormally, there will be safeguards in place that convey accountability on operators. [135]

CONCLUSION

Human rights are not perfect. It is argued that the values embedded in human rights instruments may be too western, hence, too individualistic.[136] It is also posited that the nature of human rights being binding only against States makes it hard to enforce against private persons and other entities.[137] Others argue that the abstraction of human rights, leading it to have different

[130] McGregor et al., *supra* note 93, at 335.
[131] *Id.* at 337.
[132] U.N. Human Rights Committee, *General Comment No. 34, Article 19: Freedoms of Opinion and Expression,* ¶¶21-22, 24-30, 33-35, U.N. Doc CCPR/C/GC/34 (Sept. 12, 2011).
[133] *Supra* note 34.
[134] Raenette Gottardo, *Building Global Algorithmic Accountability Regimes: A Future-focused Human Rights Agenda Beyond Measurement,* 5 PEACE HUMAN RIGHTS GOVERNANCE 65, 82 (2021).
[135] Gottardo, *supra* note 98, at 8.
[136] *Id.* at 7-8.
[137] *Id.* at 9.

interpretations, can weaken its enforceability.[138] Despite these criticisms, human rights give a reasonable normative foundation for AI systems to follow. Human rights' position to support, guide, and fortify a governance framework for AI should be irrefutably recognized, rather than being diverted by the criticisms highlighted above and losing our path amidst ethical relativism.

While there is no need to recreate the wheel when developing an AI governance framework, it would also be a mistake to believe that the job is done. Consensus on the fact that AI governance must be based on human rights is just the beginning. It is a plan, but it is not a full-fledged AI governance system. Hence, this is an appeal for States and international bodies to agree on implementing an algorithmic accountability treaty with international human rights in mind. The same can be said to individual States to enact similar municipal legislation to match the specific circumstances of each State. Much research is still needed to fully understand the algorithmic process, its impacts now, and how it will impact our future. But by starting with human rights, we can be certain that the rights we currently possess will not be infringed.

ABOUT THE AUTHOR

Benjamin Niel E. Dabuet is a third-year student from Far Eastern University - Institute of Law. He is currently one of the staff editors for the 51st volume of the Review. His interests are intellectual property law and artificial intelligence.

[138] *Id.* at 11.

DATA PRIVACY IN ONLINE CLASSES: AN EXAMINATION OF THE DATA PRIVACY LAW AND ITS PROTECTION OF ONLINE LEARNING ENVIRONMENTS

Angelica Mae S. Andaya

Abstract: Following the shift to online classes in the new normal, data privacy in virtual learning environments has become a growing concern among educational institutions, students, and teachers alike. This work will examine the precepts of the current data privacy law and how they come into play in protecting data and information used for online classes, the persons providing and receiving the same, and their implications for modern education that, at present, is heavily relying on internet connection and computer screens to recreate the traditional in-person learning environment in a post-COVID-19 setting.

Among the countless, drastic changes brought about by the COVID-19 pandemic is the shift from onsite to online classes. Due to the government-mandated closure of schools in the Philippines,[1] students, teachers, and educational institutions have been constrained to recreate the traditional learning environment through internet connection and computers. With remote learning, particularly online classes being the new norm in a post-COVID-19 setting, several questions arise in relation to their effectiveness, sustainability, and security.

In the Philippines, online classes are regulated by the Department of Education (DepEd) for the K-12 basic education program, the Commission on Higher Education (CHED) for public and private Higher Education Institutions (HEIs), and the Legal Education Board (LEB) for legal education institutions. In particular, under LEB Memorandum Circular No. 67, online classes which are composed of synchronous and asynchronous learning methods, involve "real time interaction between the instructor and the students[,]" which is "facilitated by internet-based technology[,] such as video conferencing and similar methods."[2] Synchronous learning, which involves real time interaction between the instructor and students, is conducted through "video conferencing, teleconferencing, live chatting, live-streaming, and other similar methods."[3] In contrast, asynchronous learning, where the instructor and the students do not interact in real time,

[1] Inter-Agency Task Force for the Management of Emerging Infectious Diseases, *Guidelines on the Nationwide Implementation of Alert Level System for COVID-19 Response*, Official Gazette (Nov. 18, 2021).
[2] Legal Education Board, *Supplemental Guidelines on the Conduct of Remote Classes,* Legal Education Board Memorandum Circular No. 67, Series of 2020 (Oct. 14, 2020).
[3] *Id.,* §2(5).

includes "self-guided learning modules, recorded video and audio content, posted lecture notes, online discussion boards, and other similar methods."[4]

Both synchronous and asynchronous learning methods take place on several platforms, such as Canvas, Blackboard, Zoom, Google Meet, and Microsoft Teams, among others. Students and teachers interact and communicate through the said platforms to recreate the traditional learning environment of in-person classes. Consequently, everything that is needed for class – student information, learning materials, exam questionnaire, grades, school-related surveys, and even recorded video and audio lectures in some instances – is coursed through such platforms. Due to the shift to online learning, much of our files, data, and information are floated, submitted, and transacted through internet platforms, which – while secure and regulated on their own – still give rise to concerns of privacy in the virtual world. A question, thus, comes to mind: how much privacy and security are we guaranteed in an online learning environment?

DATA PRIVACY IN THE PHILIPPINE SETTING

In 2020, the National Privacy Commission (NPC) issued Data Privacy Council Education Sector Advisory No. 2020-1 to recommend guidelines for online learning. Among the advisory's areas of concern are the use of Learning Management System (LMS) and Online Productivity Platforms (OPP), use of social media, publication of information or files via other means or platforms, storage of personal data, use of webcams and recording videos of online discussions, online proctoring, and data security.[5] The advisory is patterned after Republic Act (R.A) No. 10173 or the Data Privacy Act (DPA) of 2012, the controlling law on data privacy. In fact, in its Division Memorandum No. 151 S. 2020, the DepEd – in accordance with the DPA – reiterated its inherent obligation "in securing and protecting the learners' and teachers' personal information in various virtual and online school systems,"[6] in light of the shift to the online learning environment. Educational institutions have also released their own issuances pursuant to the DPA, such as the University of the Philippines' (UP) Privacy Notice for Students, as well as the Philippine Science High School System (PSHS System).

Having established how online classes are contextualized within the DPA, it is relevant to examine how the said law lays out the groundwork for navigating data privacy concerns in a virtual learning environment. This work will explore the principles embedded in the DPA vis-à-vis their implications on the transmission and usage of data in meeting the demands of education in the new

[4] *Id.,* §2(1).
[5] National Privacy Commission, *Data Privacy and Online* Learning, Data Privacy Council Education Sector Advisory No. 2020-1 (2020).
[6] Department of Education City Schools Division of Dasmariñas, *Data Privacy on the Issuance of Learners' and Teachers' Personal Information in the New Normal,* DM No. 151, S. 2020 (Aug. 5, 2020).

normal. This work will also briefly examine the concept of privacy, its constitutional and legal precepts, and how the right to privacy is preserved and protected in the virtual world.

A. THE RIGHT TO PRIVACY IN JURISPRUDENCE

The right to privacy is enshrined in none other than the 1987 Constitution itself. Section 3 of Article III provides:

> 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.[7]

Such right was first recognized by our Supreme Court in the 1968 case of *Morfe v. Mutuc*, where the Court acknowledged that the protection of the dignity and integrity of the individual "has become increasingly important as the modern society developed."[8] The Court elucidated in *Morfe* that "the forces of a technological age — industrialization, urbanization, and 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 a totalitarian society."[9]

As early as 1968, the Court had already shed light on the possible intrusions on human privacy brought about by technological advancements. However, the ruling in *Morfe* was made in the context of privacy vis-à-vis unreasonable searches and seizures by the government, and not necessarily intrusions by private individuals. Thus, in latter cases, our jurisdiction has recognized different aspects of the right to privacy, namely, decisional and informational privacy. In *Disini v. Secretary of Justice*, where the Court upheld the constitutionality of R.A. No. 10175 or the Cybercrime Prevention Act of 2012 save for a few provisions, the Court discussed:

> Decisional privacy involves the right to independence in making certain important decisions, while informational privacy refers to the interest in avoiding disclosure of personal matters. It is the latter right—the right to informational privacy—that those who oppose government collection or recording of traffic data in real-time seek to protect. Informational privacy has two aspects: the right not to have private information disclosed, and the right to live freely without surveillance and

[7] PHIL. CONST. art. III, §3.
[8] Morfe v. Mutuc, 130 Phil. 415 (1968).
[9] *Id.*

> intrusion. In determining whether or not 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 his or her expectation of privacy must be one society is prepared to accept as objectively reasonable.[10]

Along with other provisions, the Court declared as unconstitutional Section 12 of the Cybercrime Prevention Act, which allows the real-time collection of traffic data upon reasonable grounds that cybercrime-related offenses are being committed. The Court held that despite the compelling interest of the State to prevent crimes in the cyberspace, Section 12 infringes on a person's right to privacy due to the probable usage of random bits of traffic data, which, if gathered and analyzed, may be used to create profiles of persons under surveillance to the extent of accessing information on their "close associations, religious views, political affiliations, even sexual preferences."[11] Because the power of law enforcement authorities over such data is "virtually limitless," which allowed them to engage in "fishing expeditions" using such data and information, the Court struck down Section 12 for violating a person's right to privacy.[12]

In another case, the Court invalidated Administrative Order (A.O.) No. 308, otherwise known as the "Adoption of a National Computerized Identification Reference System," for being violative of the constitutional right to privacy. The case of *Ople v. Torres*, through the *ponencia* of former Chief Justice Reynato Puno, recognized the "potential for misuse of the data to be gathered" under A.O. No. 308, which required a person to present his or her Population Reference Number (PRN) in transacting with a government agency for basic services and security.[13] A.O. No. 308 also sought to establish a biometrics system that would require the taking of the fingerprints, as well as other biological information of the person seeking to avail the services facilitated by the computerized identification system. The Court then further illuminated the perils of potential privacy breaches and intrusions under A.O. No. 308:

> Pursuant to said administrative order, an individual must present his PRN every time he deals with a government agency to avail of basic services and security. His transactions with the government agency will necessarily be recorded — whether it be in the computer or in the documentary file of the agency. The individual's file may include his transactions for loan availments, income tax returns, statement of assets and liabilities, reimbursements for medication, hospitalization, etc. The more frequent the use of the PRN, the better the chance of building a huge, formidable information base through the electronic linkage of the files. The data may be

[10] Disini v. Secretary of Justice, G.R. No. 203335, February 11, 2014.
[11] *Id.*
[12] *Id.*
[13] Ople v. Torres, 293 SCRA 141 (1998).

> 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.
>
> x x x
>
> Even that hospitable assumption will not save A.O. No. 308 from constitutional infirmity for again said order does not tell us in clear and categorical terms how these information gathered shall [b]e handled. It does not provide who shall control and access the data, under what circumstances and for what purpose. These factors are essential to safeguard the privacy and guaranty the integrity of the information. Well to note, the computer linkage gives other government agencies access to the information. Yet, there are no controls to guard against leakage of information. When the access code of the control programs of the particular computer system is broken, an intruder, without fear of sanction or penalty, can make use of the data for whatever purpose, or worse, manipulate the data stored within the system.[14]

Further, in the 2014 case of *Vivares v. STC,* the right to privacy in an online social network (OSN), such as Facebook, was examined in the context of how OSN users avail of the privacy settings provided by OSNs in limiting access to the content they upload on the internet.[15] In *Vivares,* the Court cited *U.S. v. Gines-Perez* and *United States v. Maxwell*, which recognized the renunciation of one's privacy rights upon uploading images or sending virtual messages or correspondence online.[16] The Court, thus set a reminder in *Vivares:*

> OSN users must be mindful enough to learn the use of privacy tools, to use them if they desire to keep the information private, and to keep track of changes in the available privacy settings, such as those of Facebook, especially because Facebook is notorious for changing these settings and the site's layout often.[17]

B. THE DATA PRIVACY ACT OF 2012

It is well to note that in the foregoing jurisprudence that while they discussed several privacy concerns, no reference was made to the present data privacy law. Certainly, the DPA was not yet in effect when the Court decided *Ople,* as the said law was only enacted in 2012. However, it was curious for the *Vivares* case, which was decided when the DPA was already in effect, not to cite the DPA in its decision. It should also be noted that as of this writing, the Court has yet to

[14] *Id.*
[15] Vivares vs. St. Theresa's College, G.R. No. 202666, September 29, 2014.
[16] *Id.*
[17] *Id.*

decide a case under the present data privacy law. Nevertheless, to further explore the topic of data privacy in the current situations brought about by online classes, a closer look on the DPA is, therefore, warranted. It is also at this juncture that we flesh out the significance of the aforementioned guidelines for online classes and their supposed compliance with the DPA, as well as their implications in a virtual learning environment.

To start, data privacy refers to the act of protecting the integrity, confidentiality, and availability of personal information that are collected, stored, and processed.[18] Under its declaration of policy, the DPA recognizes a person's right to privacy in communication and correspondence, as well as the State's protection of personal information within the government and the private sector.[19] In line with this mandate, the DPA created the NPC to administer and implement the provisions of the DPA, while ensuring the Philippines' compliance with international standards of data protection.[20] The NPC is also empowered to receive complaints, investigate, and adjudicate matters relating to personal information, issue cease and desist orders or temporary bans on the processing of personal information, and even recommend to the Department of Justice the prosecution and imposition of penalties for violations of the DPA, among others.[21]

Information under the DPA is classified into three, namely: (1) personal information; (2) sensitive personal information; and (3) privileged information. *Personal information* includes any information which, if put together with other information, would directly and certainly identify an individual.[22] On the other hand*, sensitive personal information* includes those pertaining to an individual's race, ethnic origin, marital status, age, color, religious, political, or philosophical affiliations, as well as a person's individual health, education, genetic or sexual life, or any offense which was committed or alleged to have been committed by such person.[23] Sensitive personal information also covers those issued by government agencies such as social security numbers, health records, tax returns, as well as those specifically established by an executive order or an act of Congress to be kept classified.[24] Lastly, *privileged information* refers to any and all forms of data which constitute privileged information under the Rules of Court and other pertinent laws.[25]

[18] Video Lecture: Data Privacy Act, Dean Marian Ivy Fajardo (Jul. 23, 2021).
[19] An Act Protecting Individual Personal Information In Information And Communications Systems In The Government And The Private Sector, Creating For This Purpose A National Privacy Commission, And For Other Purposes (Data Privacy Act of 2012), Republic Act No. 10173, §2 (2012).
[20] *Id.,* §7.
[21] *Id.*
[22] *Id.,* §3(g).
[23] *Id.,* §3(1).
[24] *Id.*
[25] *Id.,* §3(k).

Further, Section 4 of the DPA defines the scope of the law, which covers the processing of any natural or juridical person's personal information, including those personal information controllers located in the Philippines.[26] Processing refers to "any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data."[27]

Moreover, Section 4 also provides for exceptions under the DPA, which apply to the following:

> (a) information about any individual who was an officer or employee of a government institution in relation to his or her position or functions;
> (b) information about an individual who is or was performing service under contract for a government institution;
> (c) information relating to any discretionary benefit of a financial nature such as the granting of permits;
> (d) personal information processed for journalistic, artistic, literary or research purposes;
> (e) information necessary to carry out the mandate of government bodies and law enforcement agencies in relation to particular laws such as R.A. 1405 or the Secrecy of Bank Deposits Act, R.A. 6426 or the Foreign Currency Deposit Act, and R.A. 9510 or the Credit Information System Act;
> (f) information necessary to comply with R.A. 9160 or the Anti-Money Laundering Act and other applicable laws; and
> (g) personal information originally collected from residents of foreign jurisdictions in accordance to their laws and applicable data privacy laws for information processed in the Philippines.[28]

At the crux of the DPA are the general principles on the processing of personal information, namely: (1) transparency; (2) legitimate purpose; and (3) proportionality.[29] Under Section 11, the processing of personal information shall be "determined and declared as soon as reasonably practicable after collection and later processed in a way compatible with such declared, specified, and legitimate purposes only."[30] Section 11 provides that personal information shall be retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained, and kept in a form that permits the identification of data subjects for no longer than necessary for

[26] *Id.,* §4.
[27] *Id.,* §3(j).
[28] *Id.,* §4.
[29] *Id.,* §11.
[30] *Id.*

which the data were collected and processed.[31] The DPA, thus, set the criteria for lawful processing of personal information under Section 12:

> Section 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> (a) The data subject has given his or her consent;
>
> (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
>
> (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
>
> (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[32]

More importantly, Section 13 of the DPA prohibits the processing of sensitive personal information and privileged information except in the following cases:

> (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
>
> (b) The processing of the same is provided for by existing laws and regulations: *Provided, That* such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
>
> (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

[31] *Id.*
[32] *Id.,* §12.

> (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided, That* such processing is only confined and related to the bona fide members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing; (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
> (f) The processing concerns such personal information as 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.[33]

Aside from the general principles of data privacy, an essential facet of the DPA lies in the consent of the data subject, which shall be freely given and shall constitute "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."[34] Such consent shall be "evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so."[35] The DPA also stressed the principle of accountability which holds each personal information controller responsible for "personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation."[36]

Further strengthening the safeguards on the processing of personal information, the DPA also provides penalties for the conduct of the following acts: unauthorized processing of personal information and sensitive personal information,[37] accessing personal information and sensitive personal information due to negligence,[38] improper disposal of personal information and sensitive personal information,[39] processing of personal information and sensitive personal information for unauthorized purposes,[40] unauthorized access or intentional breach,[41] concealment of security

[33] *Id.,* §13.
[34] *Id.,* §3(b).
[35] *Id.*
[36] *Id.,* §21.
[37] *Id.,* §25.
[38] *Id.,* §26.
[39] *Id.,* §27.
[40] *Id.,* §28.
[41] *Id.,* §29.

breaches involving sensitive personal information,[42] and malicious and unauthorized disclosure of personal information.[43]

DATA PRIVACY IN ONLINE CLASSES

In fine, while the safeguards under the DPA are embedded in the guidelines for online learning, it is worthy to inquire about the particularity of the DPA regarding the data and information used and disseminated for purposes of online classes. Considering that DPA was enacted in 2012 – several years before the educational shift caused by a global pandemic—we now examine how the peculiar circumstances of online classes are situated within the context of the DPA. As the Supreme Court has yet to make a pronouncement regarding the application of the DPA to a particular legal controversy, it may be assumed that the present data privacy law is premised on a general application over data processed by personal information processors, and even private persons in some instances, without actually contemplating the situation in online classes.

Thus, apart from compliance to the general principles of transparency, legitimate purpose, and proportionality, there are limited, or yet-to-be-determined standards of protection afforded to data and information used for purposes of online classes. At present, the DPA does not explicitly mention how student information, learning materials, exam questionnaires, grades, school-related surveys, and recorded lectures are to be kept, stored, or processed in a virtual learning environment. Verily, online learning brought about by the pandemic has exposed gaps in our present data privacy law, where the rights of students as to their school-related data and information, as well as the safeguards and standards for the use and dissemination of academic materials, are yet to be particularly defined and delineated.

A. THE CURRENT STATE OF ONLINE LEARNING

In Lisa Ward's "Data Privacy in the Age of Online Learning" published by the Wall Street Journal, it was stressed that "infrastructure for protecting students' personal data wasn't that sound to begin with," citing Leah Plunkett, a Harvard Law School Meyer Research Lecturer.[44] Plunkett compared the current situation of online learning "to building something 'using duct tape on top of Legos.'"[45] Bo Chang, in her paper for Ball State University, emphasized that online privacy issues are indeed manifested in various activities such as peer reviewing, group collaborative work,

[42] *Id.,* §30.
[43] *Id.,* §31 and §32.
[44] Lisa Ward, *Data Privacy in the Age of Online Learning*, The Wall Street Journal, (Dec. 8, 2020, 3:02 PM), https://www.wsj.com/articles/data-privacy-in-the-age-of-online-learning-11607457738.
[45] *Id.*

and learners' evaluations.[46] Citing Booth, Chang noted that "in class or in online discussions, students reveal lots of personal and private information that might be questionable or even threatening to our boundaries and ethical responsibilities, which raises a question about how much students should share their personal information with the instructor."[47] Chang also acknowledged that while social media sites, such as Facebook and Twitter, provide flexible digital environments for online learners, they also impose challenges that blur the lines between the learners' skillfulness and comfort in using technology, as well as between their social and professional identities.[48]

In her work, Chang heavily stressed the importance of protecting the learners' privacy in an online learning environment, when "privacy issues are more complex and nuanced compared with the privacy issues in a physical learning environment."[49] Chang also emphasized the necessity of revisiting existing privacy policies or contracts which need to be "revised and tailored to a new group of the community or a new context."[50] Thus, Chang concluded that "to balance the needs for privacy and the benefits of sharing knowledge publicly, students can be informed about the ways they can conveniently modify and control their privacy identification information."[51]

The issuance of guidelines by the University of the Philippines – Visayas (UPV)[52] is illustrative. Culled from NPC bulletins and memoranda, the UPV crafted its own data privacy guidelines in conducting online classes.[53] UPV emphasized three principles: (1) privacy, reminding that students "might feel uncomfortable displaying their living space to their peers;" (2) equity, acknowledging that not all students may have the same capacity as regards internet connection and available devices to use for their classes; and (3) peculiarity, noting that some

---

[46] Bo Chang, *Privacy Issues in Online Learning Environment,* Online Learning (2021), https://files.eric.ed.gov/fulltext/ED611641.pdf.

[47] *Id* (citing Booth, *Boundaries and student self-disclosure in authentic, integrated learning activities and assignments*, New Directions for Teaching and Learning, (2012), https://doi.org/10.1002/tl.20023).

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id* (citing Biehl and Rieffel, *When privacy and utility are in harmony: Towards better design of presence technologies,* Personal and Ubiquitous Computing, (2013), https://doi.org/10.1007/s00779-012-0504-7).

[52] University of the Philippines Visayas, *Online Learning and Data Privacy*, (Mar. 11, 2021), https://www.upv.edu.ph/index.php/announcements/online-learning-and-data-privacy.

[53] *Id,* (citing the National Privacy Commission, *supra* at 5; National Privacy Commission, *NPC PHE Bulletin No. 16: Privacy Dos and Don't's for Online Learning in Public K-12 Classes,* (2021), *available at https://www.privacy.gov.ph/2020/10/npc-phe-bulletin-no-16-privacy-dos-and-donts-for-online-learning-in-public-k-12-classes/;* National Privacy Commission, *NPC PHE Bulletin No. 17: Update on the Data Privacy Best Practices in Online Learning,* (2021), *available at https://www.privacy.gov.ph/2021/02/npc-phe-bulletin-no-17-update-on-the-data-privacy-best-practices-in-online-learning/;* National Privacy Commission, *Privacy Commission's updated online learning guidelines advise schools to enforce social media policy,*(2021), *available at https://www.privacy.gov.ph/2021/02/privacy-commissions-updated-online-learning-guidelines-advise-schools-to-enforce-social-media-policy/;* National Privacy Commission, *Online Learning Guidelines Issued to Help Protect Student Privacy and Reduce Data Breaches in Schools*, (2020), *available at* https://www.privacy.gov.ph/2020/09/online-learning-guidelines-issued-to-help-protect-student-privacy-and-reduce-data-breaches-in-schools/).

students may feel "shy or anxious on camera, affecting their performance in class."[54] More importantly, the UPV advisory instructed that the announcement of personal data, such as grades and results of assignments shall be directed only to its intended recipients.[55] It also stressed that posting photos and videos on social media must have a legitimate purpose, and that if photos and videos are posted as part of the course requirements, "such data's lifespan usually coincides with that of the course."[56] Thus, once the course has concluded, it means the data's lifespan will have also elapsed.[57] It must then be removed or deleted unless there is "some other lawful basis for keeping it online."[58] It also discouraged submissions of course requirements via social media platforms, as well as the public posting of communications regarding test and assignment results, and reminders on unpaid school fees, among others.[59]

Citing the NPC, the UPV advisory also reminded that the use of cameras during online classes and examinations should be "reasonable and necessary" for the monitoring of students, and such use shall be optional whenever possible. It enumerated instances considered as legitimate use of recorded class discussions: a) review of lecture presentations and ensuing class discussions, and b) viewing by students (and/or their parents) who were not present during class, subject to appropriate school protocols.[60]

As for students, the advisory suggested the creation of strong passwords for online learning platforms, the use of customized virtual backgrounds to avoid accidental disclosure of personal information, and the default off mode of both cameras and microphones, especially when the student is not speaking or reciting. Also, it reminded students to refrain from connecting their devices for online classes in public Wi-Fi networks, sharing submissions for an unlimited time, and taking screenshots of the video feed of their teachers and other students, as well as sharing online class links and passwords to persons who should not be in the class.[61]

B. STUDENT PRIVACY LAWS MODEL: THE UNITED STATES OF AMERICA

After an examination of our current data privacy law, as well as the present situation in our new virtual learning environments, it is relevant to examine how other countries are faring in relation to addressing school-related data privacy concerns. It is well to note that in the United States of America, there are several legislations specifically covering student privacy on data and information used for academic purposes.

[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*

An example is the Family Educational Rights and Privacy Act (FERPA) of 1974, a federal law that protects the privacy of student education records. FERPA's application covers all schools receiving funds under an applicable program of the U.S. Department of Education.[62] Under the FERPA, parents are given certain rights in relation to their children's education records, which are transferred to students once they turn 18 years old, making them "eligible students," or attend school beyond the high school level. Parents and eligible students have the following rights under the FERPA:

1) Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
2) Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
3) Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions:
    a. School officials with legitimate educational interest;
    b. Other schools to which a student is transferring;
    c. Specified officials for audit or evaluation purposes;
    d. Appropriate parties in connection with financial aid to a student;
    e. Organizations conducting certain studies for or on behalf of the school; Accrediting organizations;
    f. To comply with a judicial order or lawfully issued subpoena;
    g. Appropriate officials in cases of health and safety emergencies; and
    h. State and local authorities, within a juvenile justice system, pursuant to specific State law.[63]

Additionally, the FERPA authorizes the disclosure of "directory" information, such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance even without consent, subject to notification to parents and eligible students, and the allowance of reasonable time for parents and eligible students to request that such directory

[62] U.S. Department of Education, *Family Educational Rights and Privacy Act (FERPA)*, (Aug. 25, 2021), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
[63] *Id.*

information not be disclosed.[64] The FERPA also mandates that parents and eligible students are advised annually of their rights under the said law[65].

On the other hand, the U.S. Congress has also enacted the Children's Online Privacy Protection Rule (COPPA), which regulates the activities of website and online services operators in collecting personal information of children below 13 years old. Enacted in 1998, the COPPA "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet."[66] Under the COPPA, a website operator is required to perform the following:

a) Provide notice on the Website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information;
b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children;
c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance;
d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[67]

It is worth mentioning that although the COPPA mandates a general application to personal information of children below 13 years old,[68] it also applies to schools acting as agents of parents when they use online services or websites for educational purposes.[69]

More specifically, the State of California passed its own student data privacy legislation called the Student Online Personal Information Protection Act (SOPIPA). Passed in 2014, SOPIPA mainly prohibits websites, online services, or mobile applications used primarily for K-12 school purposes from committing the following acts:

1) Commercializing the collection of covered student data – either by selling such data, using such data to create target advertisements to students or their families; or
2) Collecting such data for any other noneducational purpose.[70]

[64] *Id.*
[65] *Id.*
[66] Federal Trade Commission, *Children's Online Privacy Protection Rule*, 78 FR 4008, (Jan. 17, 2013), *available at* https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule.
[67] *Id.*
[68] *Id.*
[69] LearnPlatform, *Student Data Privacy Regulations Across the U.S.: A Look at How California, Illinois and New York Are Handling Privacy*, LearnPlatform, (Mar. 23, 2021), *available at* https://learnplatform.com/blog/edtech-management/student-data-privacy-regulations.
[70] *Id.*

The SOPIPA also "applies to any [education technology] company regardless of whether they have a contract in place with the school or district. It also removes the idea of consent, meaning parents and students cannot consent to a company's use of a student's personal information for commercial purposes."[71] The SOPIPA was eventually expanded to cover pre-school and pre-kindergarten students in 2016 through Assembly Bill 2799.[72]

In addition, the State of California has also passed Assembly Bill 1584, which authorizes California local educational agencies (LEAs) to enter into contracts with third-party storage providers for the "digital storage, management, and retrieval of pupil records or to provide digital educational software, or both," subject to the third party's description of the process of keeping the records secure, as well as the LEA and the third party's compliance with federal data privacy laws.[73]

In 2019, the Student Online Personal Protection Act (SOPPA) was enacted in the state of Illinois through House Bill 3606.[74] The SOPPA centers mainly on data breach involving student information, and prohibits the disclosure of student information by operators, unless such disclosure is made for certain purposes, one of which is section (E):

> (E) For a school, educational, or employment purpose requested by the student or the student's parent or legal guardian, provided that the information is not used or further disclosed for any other purpose.[75]

Having taken effect in July 2021, the SOPPA emphasized that student data shall be used only for beneficial purposes, such as "providing personalized learning" and "innovative technologies."[76] The SOPPA also mandates school districts to post a list of school operators processing student data, including written agreements to that effect.[77] It also requires school districts to notify students and parents regarding any breach of student data by said operators.[78]

Furthermore, the State of Illinois also has in place the Right to Privacy in School Setting Act which requires elementary and secondary schools to notify a student, as well as his or her parent or guardian, that the school is prohibited from requesting or requiring a student's password

---

[71] *Id.*
[72] A.B. No. 2799 (2016).
[73] *Id.*
[74] Learning Technology Center of Illinois, *Student Data Privacy Laws,* Learning Technology Center of Illinois, *available at* https://ltcillinois.org/dataprivacy.
[75] H.B. 3606, 101st General Assembly (2019).
[76] *Id*, §27, par. (a).
[77] *Id,* §27, par. (a)(2).
[78] Learning Technology Center of Illinois, *supra* at 74.

or account information to access his or her account on a social networking website.[79] It also states that a school may require the student to cooperate in investigations regarding violations of the school's disciplinary policy, which may be contained in specific information on the student's social media account.[80] On the other hand, Illinois' Protection of Pupil Rights Amendment (PPRA) provides for a restriction on the collection of information for surveys, analyses, or evaluations from students which involves specified protected topics, and requires notification to and consent of the parents if such information is collected for the said purpose.[81]

CONCLUSION

From the foregoing, it could be inferred that while our current data privacy law provides a decent framework for guidelines in online classes, the principles of transparency, legitimate purpose, and proportionality may be further refined to meet the demands of our current virtual learning environments. Certainly, despite guidelines and advisories provided by educational and government institutions, there is still a considerable possibility for data breach in online classes, especially if the rules are not implemented by schools and followed by teachers and students themselves to the letter. These guidelines and advisories could only go so far in the process of conducting online classes, as the probability of these rules being relaxed to the point of compromising data privacy is still of a significant concern.

Thus, the DPA could surely welcome additional safeguards that particularly refer to the security and preservation of data and information collected for educational purposes, similar to precedents laid down in the United States. Perhaps, the NPC could come up with more stringent rules, or our Congress could even supplement the DPA to further address the needs of education in the new normal. In fact, Privacy Commissioner Raymund Enriquez Liboro announced in the 55th Asia Pacific Privacy Authorities (APPA) Forum last February 2021 that a substitute bill to amend the DPA has already been lodged in the House of Representatives.[82] The provisions in the substitute bill focus on expanding the coverage of sensitive personal information, clarifying the extraterritorial application of the DPA, defining the digital age of consent to process personal information to more than 15 years old, including of performance of a contract as a new criterion for processing sensitive personal information, among others.[83]

---

[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] National Privacy Commission, *A Stronger Data Privacy Law Sought in Proposed Amendments,* (Nov. 11, 2021), *available at https://www.privacy.gov.ph/2021/06/a-stronger-data-privacy-law-sought-in-proposed-amendments/#:~:text=Efforts%20to%20amend%20the%20DPA,and%20to%20impose%20administrative%20penalties.*
[83] *Id.*

Notably, data privacy guidelines for online classes are not included in the proposed amendments. A suggestion would therefore be to include a specific provision that centers on the creation and implementation of data privacy guidelines by academic institutions for online classes. The provision may also include a coercive mandate for said academic institutions to craft their own data privacy policies for online classes, similar to the initiative of UPV. Certainly, the codification of NPC's data privacy guidelines for online classes into actual legislation would buttress the presence of the DPA within academic institutions, thereby allowing a more empowered and well-rounded implementation of the law. After all, the DPA could come into a fuller force and effect if academic institutions themselves are mandated by law to create their own online class policies. It would also be an advantage if such policies are specially crafted for the institutions' internal rules and circumstances, with the overarching principles of transparency, legitimate purpose, and proportionality.

Undeniably, a huge part of academic integrity lies in facilitating a safe and secure learning environment for students which allow them to freely engage in academic activities without fear of compromising their data and identities online. Because the virtual world involves a vast realm of knowledge and information susceptible to unscrupulous maneuverings with grave consequences, it is proper that sufficient measures are in place to protect all communications and transactions made for educational purposes. If we are to continue with online classes for the long haul, it is necessary that we have a strong set of rules and legislation that are specifically tailored for protecting our virtual learning environments, albeit being within our screens' reach.

ABOUT THE AUTHOR

Angelica Mae S. Andaya is a sophomore at the Far Eastern University - Institute of law. She currently serves as an Associate Editor of the Far Eastern Law Review where she also contributed as a Staff Editor for Vol. 50. She has also served as a News Writer, and on her senior year, a News Editor for The GUIDON, the official publication of Ateneo de Manila University from 2015-2019.

BIR CLICKS THE "BELL BUTTON"

Atty. Joshua Emmanuel L. Cariño

INTRODUCTION

The global pandemic caused by the Coronavirus Disease (COVID-19) has drastically altered the lives and livelihood of many people around the world. Though the pandemic has caused more harm than good, there are silver linings that indicate a sudden change in people's way of life brought to some who can be considered "winners" of the crisis.

Since physical interaction is perhaps the most restricted activity in the global pandemic, technology has become more important than ever. The world has gone virtual in practically all respects. Hence, social media has achieved greater heights in terms of usage and reach.

Social media has extended its scope beyond mere interaction between two or more users. It now has the capacity to reach out to numerous people resulting from both innovation and increased usage amongst many people. It has become the barometer of popular culture and can even influence political landscapes.

In recent years, social media has also transformed into a source of income for its users. It now has the ability to produce individuals who attain popularity, not only online, but also in society due to its very wide reach. Anyone who gains a lot of following in their accounts or postings can influence a significant amount of people online. Thus, these people have been christened as "influencers."

During the global pandemic where social media activity is significantly larger due to stay-at-home restrictions, the success of social media influencers is well-documented. Their improved ways of life are usually highlighted by their content featuring their milestones, such as purchasing new homes, vehicles, and many more. Most of these influencers' success stories are paraded all over different media platforms as a way of showcasing how social media can be used as a tool to better one's life amidst the crisis brought about by the pandemic.

One particular social media influencer couple has caught the attention of the public after suddenly disappearing in the online world, following the issuance of the Bureau of Internal Revenue (BIR) of a circular on income received by social media influencers.[1] Since then, different views emerged as to how the Bureau of Internal Revenue (hereinafter referred to as "BIR") has

[1] Ralf Rivas, *After JaMill YouTube channel closure, BIR says income can still be tracked*, RAPPLER, (Aug. 24, 2021 8:30pm), https://www.rappler.com/business/bir-response-income-can-still-be-tracked-after-influencers-channel-closure/ (last accessed Dec. 11, 2021).

become the bad cop anew on the success of social media influencers who are usually characterized as ordinary people who suddenly found a stable and lucrative means of livelihood.

Is the BIR a "killjoy" in the success of these influencers? This article will discuss the recently issued Revenue Memorandum Circular of the BIR on taxes of social media influencers and critique whether the issuance of the circular is proper and whether the issuance is just a way of imposing a burden on the lives of ordinary people.

THE BIR IS WATCHING

The BIR issued Revenue Memorandum Circular No. 97-2021 (hereinafter referred to as "Circular") on August 16, 2021. In this Circular, the tax bureau issued guidelines as to how social media influencers should fulfill their obligation to pay taxes. Weeks after, the BIR reported having issued several Letters of Authority to around two hundred fifty (250) social media influencers who are found to be top earners in the field.[2]

Several days after the issuance of the Circular, social media influencers, one particularly known as the *Jamill* couple reportedly took down their YouTube account. This sparked a buzz online as to the income generated by influencers and how some may have been remiss in their tax obligations. Weeks after, the said influencer couple reportedly have ironed things out with the BIR.[3]

A QUICK LOOK AT BASIC PRINCIPLES OF TAX LAWS

One of the primary sources of income for the government is the payment of taxes of its people. It is one of the essential powers of the State; the purpose of which is for the government to earn revenue to fulfill its functions. Income is one of the foremost kinds of taxes in the Philippines. Income, as contemplated by law, is the amount of money coming to a person or corporation within a specified time, whether as payment for services, interest, or profit from an investment.[4] For it to be taxable, there must be gain that is realized or received, and not excluded by law or treaty from being taxed. Hence, an individual or corporation that received an amount of money considered as a gain — such amount was not used to pay or compensate for any other obligation — may be liable for income taxes.

---

[2] Department of Finance, *BIR Probing Initial 250 SocMed Influencers to Check Tax Compliance,* https://www.dof.gov.ph/bir-probing-initial-250-socmed-influencers-to-check-tax-compliance/ (last accessed Dec. 13, 2021).

[3] Stephanie Bernardino, *JaMill Clears Issue with BIR, Selling of Properties,* MANILA BULLETIN (Sept. 20, 2021 9:29am), https://mb.com.ph/2021/09/20/jamill-clears-issue-with-bir-selling-of-properties/ (last accessed Dec. 13, 2021).

[4] IGNATIUS MICHAEL T. INGLES, TAX MADE LESS TAXING: A REVIEWER WITH CODALS AND CASES, 33 (3rd ed. 2021).

Section 23 of the National Internal Revenue Code of the Philippines (hereinafter referred to as "Tax Code") provides for the general principles of income taxation. Philippine citizens residing therein, and domestic corporations are taxed on all income from sources within and without the Philippines.[5] Nonresident Philippine citizens, foreign citizens, and corporations are all similarly taxed only for sources within the Philippines.[6] Rates and tax treatments may vary depending on the type or kind of income, but they are nonetheless taxed as long as they are considered as gain realized or received.

Aside from income, another kind of tax that social media influencers have to contend with is business taxes. There are two kinds of taxes for influencers stated by the Circular: percentage and value-added tax. Percentage taxes are taxes based on gross sales or receipts.[7] Value-added tax, on the other hand, is a tax imposed on consumption, levied on the sale or exchange of goods and services in the Philippines.[8]

REVENUE MEMORANDUM CIRCULAR 97-2021

The highlight of this writing is the recent BIR Revenue Memorandum Circular No. 97-2021 with the subject: *Taxation of Any Income Received by Social Media Influencers.* Under Section 2 of the Circular, the purpose of the issuance is to clarify the tax obligations of social media influencers, whether individuals or corporations.[9] The Circular also defined who social media influencers are, to wit:

> Section 3. Definition of Social Media Influencers
>
> The term "social media influencers" referred to in this Circular includes all taxpayers, individuals or corporations, receiving income, in cash or in kind, from any social media sites and platforms (YouTube, Facebook, Instagram, Twitter, TikTok, Reddit, Snapchat, etc.) in exchange for services performed as bloggers, video bloggers or "vloggers" or as an influencer, in general, and from any other activities performed on such social media sites and platforms.[10]

Under the definition, it is clear that any entity or individual on social media sites receiving income through or from said sites and platforms are deemed social media influencers. While the term "social media influencer" is usually associated with individuals who have gone viral over the

[5] An Act Amending the National Internal Revenue Code, As Amended, And for Other Purposes [NATIONAL INTERNAL REVENUE CODE], Republic Act No. 8424, as amended, §23 (1997).
[6] *Id.*
[7] INGLES, *supra* note 4, at 393.
[8] *Id.* at 323.
[9] Bureau of Internal Revenue, Taxation of Any Income Received by Social Media Influencers, Revenue Memorandum Circular No. 97-2021, §2 (Aug. 16, 2021) (*hereinafter* RMC 97-2021).
[10] *Id.* §3.

internet, it can be gleaned from the definition that any blog or video content creating endeavor on social media – as long as receiving income – falls within the definition. The question can now be raised as to the extent of the scope of the definition. The Circular did not define bloggers or video bloggers.

Section 4 of the Circular states that social media influencers are liable for payment of income tax and Percentage or Value-Added Tax unless they are exempted under the National Internal Revenue Code and other laws.[11]

The Circular enumerates several income sources for social media influencers. Due regard must be given to the tax bureau, as they have listed quite an exhaustive list of possible income sources of social media influencers based on the prevailing course of business happening in the very young industry of social media.

The Circular enumerates sources from which social media influencers derive their income, to wit:

i. YouTube Partner Program - this allows an influencer to make money from;
   a) Advertising revenue - the influencer gets ad revenue from display, overlay, and video ads.
   b) Channel membership - the influencer makes recurring monthly payments in exchange for special perks that he/she/it offers.
   c) Merch shelf - followers can browse and buy official branded merchandise from the influencer's watch pages.
   d) Super Chat and Super Stickers - followers pay to get their messages highlighted in chat streams.
   e) YouTube Premium Revenue - the influencer gets a part of a YouTube Premium subscriber's subscription fee when followers watch his/her/its contents.

ii. Sponsored social and blog posts - an influencer features a product or concept he/she/it is paid to promote.

iii. Display advertising - influencers also have the ability to earn money passively through display advertising. Here, the ad is similar to radio commercials because it interrupts the program.

iv. Becoming a brand representative/ambassador - the influencer would promote the products on his/her/its social media account in exchange for free products from the brand. Some brands may pay an additional fee for every piece of content or conversion the influencer creates or drives.

[11] *Id.* §4.

v. Affiliate marketing - In this type of arrangement, an affiliate marketer for the brand or the influencer would be provided with a unique link or code that will be used for tracking his/her conversions. For every conversion resulting from the said link or code, the influencer will earn a commission.
vi. Co-creating product lines - a brand would partner with an influencer to co-create products for their brand and the latter, in tum, gets paid based on a certain percentage of the profits.
vii. Promoting own products - the influencer may come up with his/her own line of products.
viii. Photo and video sales - influencers may create and sell frame-worthy pictures, high-quality videos, or the rights over them as well.
ix. Digital courses, subscriptions, e-books - influencers sell digital products.
x. Podcasts and webinars - these may include sponsored ads that generate money or the influencer may charge a small fee to access the content.[12]

The Circular further states that payments must be received by social media influencers in consideration for services rendered or to be rendered, regardless of the manner and form of payment. Thus, when an influencer receives products in exchange for a promotion, he/she/it must declare the fair market value of the said product as income.[13]

The Circular also provides for the business tax liabilities of social media influencers. They are liable for either percentage tax or value-added tax depending on whether they are self-employed or mixed-income individuals, and if they fall under the threshold amount provided under Section 116 of the Tax Code.[14] Self-employed individuals whose gross sales or gross receipts and other non-operating income that do not exceed the Value Added Tax (VAT) threshold of three million pesos (P3,000,000.00) have the option of availing the eight percent (8%) tax on gross sales or gross receipts and other non-operating income in excess of two hundred fifty thousand pesos (P250,000.00).[15] Otherwise, they shall pay under the graduated income tax rates under Section 24(A)(2)(a) of the Tax Code and the three percent (3%) percentage tax under Section 116 of the same code.[16] Should a self-employed influencer exceed the P3,000,000.00 VAT threshold, said influencer would have to follow the requirements set forth by Tax Code on persons required to register for Value-Added Tax under Section 236(G).

Social media influencers may also be considered mixed-income earners if they are earning both compensation income and income from business and/or profession. For this kind of

[12] *Id.*, §4.
[13] *Id.*
[14] *Id.*
[15] *Id.* §4.
[16] *Id.*

influencers, they are instructed by the Circular to be taxed according to the following: for their compensation income, they shall be taxed at graduated rates under Section 24(A)(2)(a) of the Tax Code; for the income earned from business and/or profession, such may be taxed under the same graduated rates or eight percent (8%) income tax based on gross sales/receipts as long as such does not exceed the VAT threshold of P3,000,000.00. However, if the total gross sales and/or gross receipts and other non-operating income exceed the VAT threshold, the graduated rates under Section 24(A)(2)(a) shall apply and they shall likewise be liable for VAT.[17]

Echoing Section 34 of the Tax Code, the Circular also provides for those allowable deductions that should be considered in computing the taxable income of social media influencers. Under the said section, ordinary and necessary expenses paid for and incurred for that are directly attributable to the conduct and development of their trade or business. Under Section 5 of the Circular, the BIR recommended common business expenses that social media influencers may encounter in their activity. These expenses, although not exclusive, may be deducted from the gross income. These common business expenses were enumerated, to wit:

1. Filming expenses (cameras, smartphones, microphone, and other filming equipment);
2. Computer equipment;
3. Subscription and software licensing fees;
4. Internet and communication expenses;
5. Home office expenses (ex. proportionate rent and utilities expenses);
6. Office supplies;
7. Business expenses (e.g. travel or transportation expenses related to YouTube business, payment to an independent contractor or company for video editing, costume designer, advertising and marketing costs (cost of contests and giveaway prizes, etc.);
8. Depreciation expense; and,
9. Bank charges and shipping fees.[18]

The Circular also stated, consistent with the provisions of the Tax Code, that the taxpayer-influencer may choose to elect the Optional Standard Deduction (OSD) not exceeding forty percent (40%) of gross sales/receipts or gross income for individuals and corporations, respectively.[19]

The Circular also provided a guide on reporting taxes specific to YouTube. As it states, income derived from payments from YouTube is treated as royalties and taxable under the United States Internal Revenue Code. Hence, the BIR advises affected influencers residing in the

[17] *Id.*
[18] RMC 97-2021.
[19] *Id.*

Philippines to submit their tax information to Google to be able to claim eligibility benefits under the Philippines-US Tax Treaty.[20]

PROVISIONS OF THE CIRCULAR – MERE REITERATIONS OF THE TAX CODE?

Many items stated under the Circular are simply reiterations of those provided for under the Tax Code. Among them is Section 6, which provides for the tax compliance requirements for these influencer-taxpayers.[21] Social media influencers are encouraged to register with the appropriate Revenue District Office (RDO) and/or update their registration information. The Circular also states that all unregistered taxpayers must secure their Tax Identification Number (TIN) from the appropriate RDO of the BIR. Those influencers already registered according to the requirements of the BIR are also reminded to ensure that their registration must reflect their existing line of business.[22]

Section 6 also states that influencer-taxpayers must keep their books of accounts duly registered with the BIR, and their tax returns filed accordingly on time.[23] The same section also reminds that a social media influencer shall withhold required creditable/expanded withholding tax, final tax on compensation of employees, and other withholding taxes, if applicable.[24] They are likewise obliged to remit the same to the Bureau at the time or times required and issue to the concerned payees the necessary Certificates of Tax Withheld.[25] The Circular also reminds the influencer-taxpayers of the liabilities of failing to file returns and pay taxes on time, and its correlation to an attempt to evade or defeat tax as provided for under Sections 254 and 255 of the Tax Code. Thus, to avoid criminal and civil liabilities under the Tax Code, the Circular has already advised social media influencers, to wit:

> The social media influencers are, therefore, advised to voluntary and truthfully declare their income and pay their corresponding taxes without waiting for a formal investigation to be conducted by the BIR to avoid being liable for tax evasion and for the civil penalty of fifty percent (50%) of the tax or of the deficiency tax.[26]

Aside from the special guide on income from YouTube discussed in the preceding part of this article, Section 7 of the Circular is also a mere reminder by the tax bureau of the benefits of tax treaties of which the Philippines is a part of in order to avoid double taxation. Hence, social media influencers are advised to ensure that they have proper documentation in case their income

[20] *Id.* §7
[21] *Id.* §6.
[22] *Id.* §6 (C).
[23] *Id.*
[24] *Id.*
[25] *Id.* §6 (D).
[26] *Id.* §6.

from foreign sources is already taxed. Sections 8 and 9 are also mere iterations of the benefits of a Tax Residency Certificate and the effect of taxes withheld in foreign countries.

INTERESTING POINTS TO CONSIDER ARISING FROM THE PROVISIONS OF THE CIRCULAR

As previously stated, the Circular did not define bloggers or video bloggers. A blogger or video blogger is any individual/entity or user on the internet that creates a blog or a vlog, respectively. Vlog, a shorter term for video blog, is defined as:

> A blog done with the help of videos, unlike a text blog where information is shared using just text and static images. Like a text blog, however, video blogs are visible to all and may be shared, commented on and rated. Video blogs are more descriptive and interactive compared to other types of blogs and are considered best for tutorial blogs.[27]

A blog, on the other hand, is defined as a regular feature appearing as part of an online publication that typically relates to a particular topic and consists of articles and personal commentary by one or more authors.[28]

From these definitions, blogs and video blogs are any content in word or video format, respectively. Under the Circular, any income in exchange for services performed as bloggers, video bloggers, or "vloggers", or as an influencer, in general, and from any other activities performed on such social media sites and platforms are taxable.[29]

Any form of content on social media which results in a form of gain on the part of the influencer can be considered taxable income, as provided for by the phrase "…and from any other activities performed on such social media sites and platforms" of Section 3 of the Circular. Hence, this form of gain from influencers may range from collaborations and product placements incorporated in an influencer's content or a share of the revenue from advertising spots provided by the social media platforms. Corollary, content creators, who can be individuals or corporations, are taxable entities. Entities ranging from individuals to media outlets, groups, associations, educational institutions, religious institutions, and a lot more are also taking advantage of the wide reach of social media to further their causes. Considering the foregoing, income from social media engagements and advertising gained by any kind of user or influencer will be considered as income.

[27] Techopedia, *What Does Video Blog (Vlog) Mean?*, https://www.techopedia.com/definition/5205/video-blog-vlog (last accessed Dec. 13, 2021).
[28] Merriam-Webster, *blog*, https://www.merriam-webster.com/dictionary/blog (last accessed Dec.13, 2021).
[29] RMC 97-2021, §3.

The question now arises on those entities that enjoy income tax privileges under the Constitution and relevant laws. Is income derived from social media engagement considered income by income tax entities as such that will be part of an entity's tax exemption?

As previously mentioned, a blog can be any content. A video blog is any video content. Hence, it also includes any video-related content. How about news, movies, or other forms of video content? Are the uploaders/creators also considered social media influencers?

Another interesting point that may raise an issue is the determination of Philippine-based content. The Circular has no particular definition of what the scope of Philippine-based content is. Neither does it have a determination of proper situs of social media content. Section 4 of the Circular states:

> For resident aliens, any income derived from Philippine-based contents shall generally be taxable. Thus, the burden of proof that the income was derived from sources without the Philippines lies upon the resident alien. Absent such proof, the income will be assumed to have been derived from sources within the Philippines.[30]

It is contended that the definition of Philippine-based content can be interpreted in several ways.

First, Philippine-based content can be interpreted as content that was created, produced, and published within the Philippines. Under this interpretation, any form of online content is considered Philippine-based as long as there exists a Philippine element in the content of a particular social media engagement. For instance, a video content setting is located, filmed, and produced in the Philippines.

Second, Philippine-based content can be interpreted as those which were uploaded and/or accessible in the Philippines. Social media platforms have the capacity to impose location-based accessibility restrictions. Video content may be made unavailable by YouTube, for instance, in a particular country. Hence, this second interpretation can simply classify content as to whether it is accessible in the Philippines for it to be considered taxable for income derived from it.

Third, Philippine-based content could be those whose topics or depictions involve the Philippines, its people, or any other discussion covering Philippine relations. Under this interpretation, content may be created elsewhere but its contents depict or contain topics or issues concerning the Philippines or Filipinos. An example of this would be a video blog of an Australian physician based in Australia that discusses health issues in the Philippines.

[30] *Id.* §4.

The Circular dictates a presumption that the income of resident aliens derived from social media engagement will be assumed to have been derived from the Philippines absent proof to the contrary. Questions on the situs of Philippine-based content would have relevance for the determination of income tax of aliens falling under the definition of social media influencers. This can be illustrated in instances where an alien shifts his/her resident or non-resident status under tax laws, yet still earns income from Philippine-based content. As in the previously suggested third interpretation of Philippine-based content, can it be argued that continuous income from display advertising and income from YouTube, as defined under the Circular, from video blogs that have Philippine-related content still be considered as Philippine-based content when the influencer is already a non-resident alien, and the content was created outside the Philippines? Perhaps the tax bureau would be able to address these questions and intricacies when the filing of income taxes from social media engagements grows through time.

CONCLUSION: THE CIRCULAR IS REALLY JUST A REMINDER

In sum, the Circular mostly reiterates the provisions of the National Internal Revenue Code on income and business taxes. Looking closely, it did not introduce anything new. Even the provision on income from YouTube is just a provision illustrative of other forms of income that are treated as royalties in another country. It is not surprising, to say the least, as the scope of the Tax Code as to what constitutes income is encompassing and would already include all such forms of income from all sources. The Circular merely informs people that income from novel sources such as those derived from social media engagements is no exception.

The Circular is a positive measure on the part of the BIR, as it shows that it is keeping in step with the technological advancements of our ever-changing times. This shows that the tax bureau is up to date with the emerging sources of income of people and is ready to impose its mandate.

ABOUT THE AUTHOR

Joshua Emmanuel "Emman" Cariño is a graduate of the FEU Institute of Law in 2020. Part of the "Covid" batch, he is preparing for the #BestBarEver2020_21 as of the time of this writing. Emman is the former Editor-in-Chief of the FELR in 2019-2020 (Vol. 49) and Layout Editor in 2018-2019 (Vol. 48).

THE FAR EASTERN
LAW REVIEW
VOLUME LI | 2021

IF LIKES CAN ELECT: AN EXAMINATION OF THE COMELEC SOCIAL MEDIA RULES

Arvin A. Maceda

Abstract: On November 17, 2021, the Commission on Elections (COMELEC) promulgated Resolution No. 10730[1] - a resolution providing the guidelines for the conduct of campaigns for the 2022 National and Local elections. The resolution included the old rules promulgated by the COMELEC since the passage of the Fair Elections Act (FEA), as well as the new regulations on social media campaigns and guidelines because of the COVID-19 pandemic.

Candidates and election observers have both praised and criticized these rules. Some argue that the COMELEC has no legislative framework for the social media guidelines, while others question its constitutionality. With candidates running for both national and local posts utilizing social media platforms because of its efficacy in the past elections, it is high time the COMELEC issued guidelines in furtherance of its to ensure the holding of a free, orderly, honest, peaceful, and credible elections through fair election practices.

Social media has evolved into one of the most effective platforms to disseminate information, regardless of whether the said information is true, factual, or honest. In contrast to traditional media such as newspapers, television, and radio, the creation and dissemination of information on social media is universally accessible. Everyone who has access to internet can visit social media platforms, post content with little to no regulation or restriction from any government entity, and disseminate the information virtually to anyone around the globe.

One of the occasions where its value is observed is during the elections. Globally, politicians have started to capitalize and utilize social media in their campaigns. For the past two elections in the Philippines, there has been a surge of political blogs, influencers, and content creators promoting and/or mud-slinging other candidates.[2] Most of these content creators claim to be independent and have no control over their content. Regardless of whether the claims are true, the benefit that the candidates yield from these creators is undeniable.

[1] Commission on Elections, Rules and Regulations Implementing Republic Act No. 9006, Otherwise Known As The "Fair Election Act", In Connection With The May 9, 2022 National And Local Elections, Republic Act No. 9006 (2021).
[2] Katrin Büchenbacher, *Philippines likely to face another 'social media election',* CHINA GLOB. TEL. NET., May 9. 2019, *available at* https://news.cgtn.com/news/3d3d414e7763444e34457a6333566d54/index.html (last accessed Jan. 20, 2022).

As the country embarked on another presidential election, the candidates doubled down on their social media presence, now that traditional methods of campaigning have been limited due to the COVID-19 pandemic.

The COMELEC promulgated Resolution No. 10730, which provides guidelines for the conduct of online campaigns, as well as the regulation of social media sites used for electoral campaigns. As early as 2019, the COMELEC has already eyed the promulgation of these guidelines to prevent the use and abuse of microblogging sites or the use of *fake news* in election campaigns.[3] However, due to the lack of a legislative framework to limit the content of social media posts, the COMELEC stated that these guidelines would only regulate social media as to its cost and not its content, hopefully reaching a compromise to regulate social media post with the current legal framework.[4]

MANDATE OF THE COMELEC IN REGULATING ELECTION-RELATED POSTS

The COMELEC is one of the Constitutional Commissions created by Article IX of the 1987 Philippine Constitution, and has the power to enforce, and administer all laws and regulations relative to the conduct of an election, plebiscite, initiative, referendum, and recall.[5] Along with other Constitutional Commissions, the COMELEC, as an administrative agency, has quasi-legislative powers. It also has a rule-making power that is untouchable by Congress absent a constitutional amendment or revision.[6]

Jurisprudence is replete with cases defining and strengthening the powers vested by the Constitution to the COMELEC as an independent commission tasked to oversee the conduct of elections. In *Abainza vs. COMELEC,* the Court ruled that the COMELEC is empowered by the Constitution to enforce and administer all laws and regulations relative to the conduct of an election.[7] In *Dibaratun vs. COMELEC*, the Court further states that the COMELEC is vested with plenary authority to decide all questions affecting elections except the question of the right to vote.[8] In *Garcia vs. COMELEC*, the Court explains that the COMELEC is empowered to investigate, and where appropriate, prosecute cases for violation of election laws—including acts or omissions

[3] Jauhn Etienne Villaruel, *Why Comelec is 'handicapped' in regulating social media campaigning,* ABS-CBN NEWS, Nov. 5, 2021 *available at* https://news.abs-cbn.com/news/11/05/21/why-comelec-cant-control-social-media-campaigning (last accessed Jan. 20, 2021).
[4] *Id.*
[5] PHIL. CONST. art. IX-C § 2 (1).
[6] Trade and Investment Development Corporation of the Philippines v. Civil Service Commission, 692 SCRA 384 (2013).
[7] Abainza v. COMELEC, 573 SCRA 332 (2008).
[8] Dibaratun v. COMELEC, 611 SCRA 367 (2010).

constituting election frauds, offenses, and malpractices.[9] The finding of probable cause in the prosecution of election offenses rests in the COMELEC's sound discretion.[10]

The authority and mandate of the COMELEC to regulate campaign and election propaganda is outlined in Batas Pambansa Blg. 881 or the Omnibus Election Code (OEC).[11] The OEC defines and delimits election and campaign periods,[12] sets limits to the election expenses to be incurred by every candidate, enumerates what constitutes lawful propaganda,[13] imposes guidelines for the regulation of election propaganda through mass media,[14] and requires political candidates to disclose to the COMELEC the expenses they have incurred during their campaign.[15] The OEC also provides the COMELEC with the authority to prosecute cases involving election-related offenses or offenses punishable under the OEC.[16]

The authority and scope of the COMELEC to regulate election propaganda was further expounded by Republic Act No. 9006 or the Fair Elections Act (FEA). It allowed the publication or broadcast of political advertisements for or against any candidate or political party, and further provided that such election propaganda, whether on television, radio, newspaper, or any other medium, shall be subject to the supervision of the COMELEC.[17] To promulgate such directive, the COMELEC must supervise the use and employment of press, radio, and television broadcasting facilities insofar as the placement of political advertisements is concerned, to give candidates equal opportunity under equal circumstances and to make known their qualifications and stand on public issues within the limits set forth in the OEC.[18]

NEW COMELEC RULES ON ELECTION CAMPAIGN

On November 17, 2021, the COMELEC promulgated Resolution No. 10730,[19] which provides the guidelines for the conduct of campaigns for the 2022 elections. The Resolution expanded the existing regulations on the press, radio, and television to social media. It introduced new regulations on: (1) the use of the internet, mobile, and social propaganda, (2) reporting requirements to be submitted by companies performing internet-related services, and (3) e-rallies.

[9] Garcia v. COMELEC, 611 SCRA 55 (2010).
[10] *Id.*
[11] Omnibus Election Code of the Philippines, [OMN. ELECTION CODE], Batas Pambansa Blg. 881 (1985).
[12] *Id.* § 3.
[13] *Id.* § 82.
[14] *Id.* § 86.
[15] *Id.*
[16] *Id.* § 65.
[17] An Act To Enhance the Holding ff Free, Orderly, Honest, Peaceful and Credible Elections Through Fair Election Practices [Fair Elections Act], Republic Act. No. 9006. § 3 (2001).
[18] *Id.* § 13.
[19] Commission on Elections, Rules and Regulations Implementing Republic Act No. 9006, Otherwise Known As The "Fair Election Act", In Connection With The May 9, 2022 National And Local Elections, Republic Act No. 9006 (2021).

Section 9(c) of the Resolution provides that the use of the internet, social media platforms, and social media for the purpose of election propaganda shall be allowed subject to the following guidelines:

1. Each registered political party/coalition and candidate shall register with the Education and Information Department of the COMELEC, the website name and web address of all platform–verified official accounts, websites, blogs and/or other social media pages of such political party or candidate within thirty (30) days from the last day of the period for the filing of the Certificates of Candidacy. Websites completing the verification process after the said period and other social media accounts established after the said period must be registered with the COMELEC-EID within five (5) days from its verification or registration.

2. Any other website, blog, or social media page not registered above but which, when taken as a whole, has for its primary purpose the endorsement of a candidate, whether or not directly maintained or administered by the candidate or their official campaign representatives, shall be considered additional official websites, blogs or social media pages of the said candidate, for all regulatory purposes.

3. Only verified accounts, websites, blogs, and/or social media pages may run electoral ads, and boost or promote electoral posts.

4. Microtargeting of electoral ads shall not be allowed provided that electoral ads can be targeted using only the following criteria: geographical location, except radius around a specific location; age; and gender; provided further that contextual targeting options may also be used in combination with the above-mentioned criteria.

5. Information contained in online campaign propaganda shall be truthful and not misleading, nor shall it tend to unjustifiably cast doubt on the integrity of the electoral process.

6. All electoral ads must show a disclosure that identifies who paid for the ad. All electoral posts must show a disclosure

> that identifies it as a paid electoral ad, and discloses who paid for the ads.[20]

Commentators of the Resolutions pointed out that the requirement of having a verified account before running electoral ads is unfair to some candidates, especially those who have low social media following.[21] Having a verified account varies across different platforms; for example YouTube, it requires at least 100,000 subscribers before it can be verified.[22] While on Instagram, there is no minimum number of followers needed to be verified. Instead, an Instagram user has to apply for the coveted verified badge.

An interesting provision introduced in these guidelines is found in Section 9(c)(2), which provides that even though an account is not maintained or administered by a candidate, when the said website, blog, or social media account has for its purpose the endorsement of a candidate, it shall be considered an additional official website for all regulatory processes.[23] A candidate need not consent or be informed that a website, blog, or social media platform is campaigning for him or her for it to be considered an additional official website for all regulatory processes.

The direct implication of this regulation is that the use of influencers and microbloggers may be considered part of the candidate's election spending, which is subject to maximum spending limits. In addition, being considered as an additional official website may also mean that the candidate may be held liable for any content the creator produces even though the said content was not directed or consented to by the candidate.

Section 11 of the Resolution expanded the existing reporting requirements from mass media companies to companies performing internet-related services. Under the new rules, the reportorial requirement has been expanded to include the following:

(1) Contractors and business firms who were engaged by the candidate in political advertisement contracts;[24]
(2) Social media associates, content creators, and influencers;[25]
(3) Agencies and other intermediaries;[26] and

[20] Rules and Regulations Implementing Republic Act No. 9006, Otherwise Known as the "Fair Election Act", In Connection with the May 9, 2022 National And Local Elections, § 9 (C).
[21] Melissa Luz Lopez, *Comelec defends 'verified' requirement for candidates' social media pages.* CNN PHIL., Dec. 13, 2021 *available at* https://www.cnnphilippines.com/news/2021/12/13/Comelec-defends-verified-requirement-socmed-pages.html (last accessed Jan 20, 2022).
[22] Youtube, Verification Badges on Channels (Apply for Channel Verification), *available at https://support.google.com/youtube/answer/3046484?hl=en (*last accessed Jan 20, 2022) [https://perma.cc/HU6X-GY9P].
[23] Rules and Regulations Implementing Republic Act No. 9006, Otherwise Known as the "Fair Election Act", In Connection with the May 9, 2022 National And Local Elections, § 9 (C)(2).
[24] *Id.* § 11.
[25] *Id.*
[26] *Id.*

(4) Internet companies which includes social media companies, transacting or doing business in the Philippines, whether or not incorporated under the Philippine laws, which a candidate or party utilize to directly reach out to voters and mobilize support through the use of ads, paid promoted hashtags/trends.[27]

The rules also provide that social media associates, including paid digital influencers and online content creators who use social media platforms to promote or defeat the election of any candidate, are considered individual contractors who are subject to reportorial requirements.[28] During the past elections, independent content creators have slowly created a platform and built their following. The amount spent by each candidate on any of these independent content creators is not disclosed to the COMELEC since the previous resolution does not consider these amounts as election expenses. But the new rule now provides that candidates must comply with disclosure and will now be subject to the amount spent for its campaign.

In the past elections, there has been increasing reliance and mobilization of paid digital influencers. The amount spent by any candidate on any of these digital influencers is not bound under the previous rules and therefore, candidates may opt not to report such expenses. Through this regulation, the amount spent and paid to content creators would be under the maximum amount spent per candidate.

The Resolution defined e-rally as a rally under Article X of the OEC, which is conducted for an online audience.[29]

According to the Resolution, the COMELEC shall provide a platform for free live streaming of e-rallies of national candidates, which shall be conducted every night, beginning February 8, 2022.[30] Airtime shall be allotted to Presidential, Vice-Presidential, and Senatorial candidates, as well as to Party-List Organization participating in the 2022 National and Local Elections. This new rule is an adaptation of the existing rules and regulations to quarantine guidelines due to the COVID-19 pandemic.

REGULATION OF SPEECH IN THE CONTEXT OF ELECTORAL CAMPAIGNS IN SOCIAL MEDIA

In terms of the authority of the COMELEC to regulate speech in the context of electoral campaigns, the decision of the Court in *Diocese of Bacolod vs. COMELEC* is instructive in deciding whether the COMELEC has the power to regulate election propaganda exercised by a non-candidate. The Court ruled:

[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] Rules and Regulations Implementing Republic Act No. 9006, Otherwise Known as the "Fair Election Act", In Connection with the May 9, 2022 National And Local Elections, §14 (C).

> While respondent COMELEC cited the Constitution, laws and jurisprudence to support their position that they had the power to regulate the tarpaulin, however, all these provisions pertain to candidates and political parties. xxx COMELEC does not have the authority to regulate the enjoyment of the preferred right to freedom of expression exercised by a non-candidate.
>
> Regulation of election paraphernalia will still be constitutionally valid if it reaches into speech of persons who are not candidates or who do not speak as members of a political party if they are not candidates, only if what is regulated is declarative speech that, taken as a whole, has for its principal object the endorsement of a candidate only.[31]

As a general rule when applied to social media posts, such posts are now considered election paraphernalia, the COMELEC's authority to regulate is only limited to candidates and political parties. A non-candidate posting on social media is still considered an exercise of one's right to freedom of expression. Pursuant to the ruling in *Diocese of Bacolod,* the COMELEC does not have the authority to regulate the enjoyment of the preferred right to freedom of expression exercised by a non-candidate.

However, the Resolution provides for instances where social media posts created by non-candidates would be considered election paraphernalia. *First*, when the non-candidate is engaged by the candidate as a social media associate and by virtue of his contractual relationship to the candidate or the political party, his posts on the official website or other blog, website or social media site would be considered as election posts. *Second*, when a non-candidate publishes and maintains an additional official website even without the consent of the candidate. The Resolution considers any other website, blog, or social media page from those registered by the candidate as an additional official website and if a non-candidate maintains such additional website, such websites shall be regulated under the Resolution promulgated by the COMELEC.

In both instances, actions may be considered as declarative speech wherein its principal object is the endorsement of the candidate only. In *Diocese of Bacolod,* the Court ruled that the regulation of such may be constitutionally valid:

> Regulation of election paraphernalia will still be constitutionally valid if it reaches into speech of persons who are not candidates or who do not speak as members of a political party if they are not candidates, only if what is regulated is declarative speech that, taken

[31] The Diocese of Bacolod v. COMELEC, 747 SCRA 1 (2015).

> as a whole, has for its principal object the endorsement of a candidate only.[32]

Furthermore, *Diocese of Bacolod* also provides the guidelines for a valid regulation of speech in election posts to be as follows:

> The regulation (a) should be provided by law, (b) reasonable, (c) narrowly tailored to meet the objective of enhancing the opportunity of all candidates to be heard and considering the primacy of the guarantee of free expression, and (d) demonstrably the least restrictive means to achieve that object. The regulation must only be with respect to the time, place, and manner of the rendition of the message. In no situation may the speech be prohibited or censored on the basis of its content.[33]

The Resolution resonates with majority of the guidelines set in the case of *Diocese of Bacolod,* except for the first criteria. Although the OEC and the FEA empower the COMELEC to issue rules and regulations to promulgate the law, it can be argued that there is still no law that regulates or empowers the COMELEC to promulgate rules and regulations on the use of social media in election campaigns. Although the COMELEC is hinging its authority on its plenary powers vested by the Constitution and by statutes to promulgate rules and regulations pertaining to elections in general.

CONCLUSION

The use of the internet and social media in election campaigns will remain in the next foreseeable future. There is no doubt in its effectiveness in disseminating information misinformation. The promulgation of COMELEC Resolution No. 10743 serves as a timely innovation in election regulation, as a response to the growing reliance on the internet and social media. It may not be the silver bullet that will eliminate fake news and misinformation, but it is a great leap toward ensuring a fair and honest election.

ABOUT THE AUTHOR

Arvin Maceda is a second-year student from the Far Eastern University – Institute of Law. He is currently one of the Staff Editors for the 50th volume of the Review. He also serves as the Vice Chairperson for FEU Centralized Bar Operations.

[32] *Id.*
[33] *Id.*

FAR EASTERN UNIVERSITY
INSTITUTE OF LAW
FEU Makati Campus
FEU Building, Sen. Gil Puyat Ave.
corner Zuellig Loop, Makati City
(02) 8836 2002 loc. 123
law@feu.edu.ph