TOO MUCH INFORMATION: RE-EXAMINING THE *VIVARES V. ST. THERESA'S COLLEGE* STANDARD OF REASONABLE EXPECTATION OF PRIVACY IN SOCIAL MEDIA*

*Enrico Miguel dela Rama Dizon***

ABSTRACT

The right to privacy found under Article III, Section 3 of our Constitution is perhaps the most malleable of our constitutional rights. As technological developments challenge traditional societal conceptions of privacy, the right to privacy has evolved from a physical, temporal right primarily tied to property rights, to becoming an independent right encompassing both persons *and* property. In recent years, it seems that privacy is once again being challenged by the rise of social media, which presents a whole new lacuna of privacy considerations primarily due to the novel, *sui generis* nature of the internet. Our jurisprudence has yet to sufficiently address these issues, with only one case, *Vivares v. St. Theresa's College*, tackling the issue of informational privacy in social media. While it is the leading case on the subject, it has formulated an insufficient and problematic standard for determining whether an internet user has exhibited a reasonable expectation of privacy online. Through an exploration of the implications of the *Vivares* ruling, this paper hopes to demonstrate how drastically our societal conceptions of privacy have changed as a result of social media, and thus argue for a re-formulation of the *Vivares* doctrine which better accounts for the unique nuances of social media.

---

* *Cite as* Enrico Miguel dela Rama Dizon, *Too Much Information: Re-Examining the Vivares v. St. Theresa's College Standard of Reasonable Expectation of Privacy on Social Media*, 96 PHIL. L.J. 318, [page cited] (2023).

** J.D., University of the Philippines College of Law (2022); B.A. in Broadcast Communication, University of the Philippines College of Mass Communication (2017). The author would like to thank his Supervised Legal Research adviser, Professor Raul C. Pangalangan, for his invaluable comments, insights, and encouragement, without which this paper would not have reached its final form.

INTRODUCTION

It is no secret that social media has had a considerable impact on our culture and on society. Since its advent in the late 2000s to early 2010s, social media has become a ubiquitous part of everyday life, to the point that it is seen as necessary for one to have a social media account in order to have a public presence and remain connected to their peers and loved ones. Social media has also been used extensively in school and work contexts,[1] with private Facebook groups for students and employees increasingly becoming the norm, and applications like Viber and WhatsApp being used as means of communication between employers and employees.

One of the most important issues raised by the advent of social media, however, is its impact on the informational privacy of individuals. Informational privacy is an aspect of the right to privacy that regulates the right of a user to prevent unwanted disclosures of their personal information.[2] While this principle is generally well-established, it faces several challenges when it comes to the online realm. The novel, *sui generis* nature of the internet has resulted in a blurring of the public and private sphere, a confusion that has only deepened with the increasing ubiquity of social media. In the past few years, the issue of social media privacy has only become more relevant. The increasing number of data breaches affecting social media sites, for example, has resulted in the likes of Facebook being probed by government agencies in the United States.[3]

Currently, there is a dearth of jurisprudence specifically regulating informational privacy in relation to social media. The most prominent jurisprudential pronouncement on the topic was laid down by the Supreme Court in the case of *Vivares v. St. Theresa's College*.[4] In this case, the Court recognized for the first time in Philippine jurisprudence that a reasonable expectation of privacy existed in the online realm. However, this reasonable expectation of privacy depended on a user's choice of privacy settings on social media sites. Posts that were left for the general public to see did not enjoy a reasonable expectation of privacy, while posts which were set to

---

[1] Yogesh Dwivedi, Gerald Kelly, Marjin Janssen, Nripendra Rana, Emma Slade & Marc Clement, *Social Media: The Good, The Bad, and the Ugly,* 20 INFO. SYS. FRONTIERS 419 (2008), *at* https://link.springer.com/article/10.1007/s10796-018-9848-5.

[2] *See* Whalen v. Roe, 429 U.S. 589 (1977).

[3] Natasha Lomas, *A Brief History of Facebook's Privacy Hostility Ahead of Zuckerberg's Testimony*, Apr. 10, 2018, *at* https://techcrunch.com/2018/04/10/a-brief-history-of-facebooks-privacy-hostility-ahead-of-zuckerbergs-testimony/.

[4] [Hereinafter "*Vivares*"], G.R. No. 202666, 737 SCRA 92, Sept. 29, 2014.

"Custom" or "Only Me" settings did.[5] Posts that were set to "Friends Only," meanwhile, did not automatically enjoy a reasonable expectation of privacy, absent proof that the user took steps to positively limit the viewership of their posts.[6]

This ruling is currently the controlling doctrine when it comes to social media privacy, but it also lays down a problematic standard insofar as its formulation of privacy on social media is concerned. In refusing to accord a reasonable expectation of privacy to users who opted to use the "Friends Only" setting, the Court laid down a flawed and potentially dangerous doctrine that fails to account for the nuances of social media and displays a lack of understanding of the medium being regulated, thereby undermining, rather than strengthening, the right to privacy on social media.

This paper aims to examine the *Vivares* ruling in its entirety, analyzing the import of the decision and drawing by inference the potential consequences it may have on social media users. The first half of Chapter II focuses on the right to privacy in general, its evolution, and its current state as interpreted by Philippine jurisprudence; while the second half thereof delves into the *Vivares* ruling by discussing the fact and dissecting the Court's reasoning. Chapter III points out the weaknesses and logical fallacies attendant to the ruling, which will then be fleshed out in greater detail in the succeeding chapters. Chapter IV situates the impact of social media within the broader evolution of privacy, utilizing Marshall McLuhan's "medium is the message" framework in order to illustrate the nature of privacy on social media. Chapter V delves into specific issues arising from the *Vivares* ruling, in order to emphasize the shortcomings of the doctrine. Finally, Chapter VI attempts to reformulate *Vivares* in light of the issues covered by the discussion, in order to reach a more just and workable standard that takes the complexities of online privacy into account.

I. GENERAL CONSIDERATIONS

A. The Right to Privacy

The right to privacy is defined as "the right to be free from unwarranted exploitation of one's person or from intrusion into one's private activities in such a way as to cause humiliation to a person's ordinary

[5] *Id.* at 123.
[6] *Id.* at 122.

sensibilities."[7] The essence of the right is essentially the "right to be let alone" and is "premised on the assertion that the right to life necessarily includes the right to live life as one chooses."[8]

While most of the provisions in our Bill of Rights originate from its American counterpart, the right to privacy was not accorded explicit constitutional imprimatur in American law for the first century and a half of the United States' (U.S.) existence.[9] Privacy, as an independent constitutional right, only received judicial recognition in the seminal 1965 case of *Griswold v. Connecticut*,[10] where the US Supreme Court recognized privacy as a guarantee emanating from the Bill of Rights' other specific guarantees, necessary to accord the latter life and substance.[11] From there, the right to privacy truly came into its own as the court used privacy considerations to expand civil liberties.[12] The breadth of protections emanating from the right to privacy demonstrates its all-encompassing importance.

As it stands today, the understanding is that there are three strands of the right to privacy, namely: (1) *decisional privacy*, or the right of one to make decisions for himself without unlawful interference by the State;[13] (2) *locational privacy*, or the privacy that is felt in physical space, such as that which may be violated by trespass or unwarranted searches and seizure;[14] and (3)

---

[7] Social Justice Society v. Dangerous Drugs Board, G.R. No. 157870, 570 SCRA 410, 431, Nov. 3, 2008.

[8] Jenny Jean Domino & Arvin Kristopher Razon, *Open Book: An Analysis of the Celebrity's Right to Privacy*, 87 PHIL. L.J. 900, 901–02 (2013).

[9] One key basis of the modern-day right was a Harvard Law Review article published by Samuel Warren and Louis Brandeis, who sought to formulate a right to privacy in order to combat the then-emerging "paparazzi culture" which existing legal remedies could not sufficiently address. This article would go on to inform the eventual historical evolution of privacy, culminating in the *Griswold* decision as cited above. *See* Paulo Romeo J. Yusi, *Tearing Down the Great Wall: Rethinking the State Action Doctrine with Respect to the Right to Privacy*, 93 PHIL. L.J. 885, 889–90 (2020).

[10] 381 U.S. 479 (1965).

[11] *Id.* at 484.

[12] The *Griswold* ruling formed the basis of later federal Supreme Court decisions which, among other things, protected the right of unmarried couples to possess contraception on the same basis as married couples, the liberty to undergo an abortion without excessive government interference, the right to contraception for juveniles at least 16 years of age, the unconstitutionality of anti-sodomy laws, and the right of same-sex couples to marry. *See* Eisenstadt v. Baird, 405 U.S. 438 (1972); Carey v. Population Services Int'l, 431 U.S. 678 (1977); Lawrence v. Texas, 539 U.S. 558 (2003); Obergefell v. Hodges, 576 U.S. 644 (2015).

[13] Morfe v. Mutuc [hereinafter "*Morfe*"], G.R. No. 20387, 22 SCRA 424, Jan. 31, 1968.

[14] *Vivares*, 737 SCRA 92, 111 n.21.

informational privacy, which is the right of an individual not to have private information about himself disclosed.[15]

Of these three, it is informational privacy which is of particular interest for the purposes of this paper, as we are currently living through a time where personal information is becoming more subject to disclosure thanks to the internet. Informational privacy can be further divided into (1) *unwarranted access to private information*, and (2) *unauthorized disclosures of private facts*.[16]

In the Philippines, the right has been enshrined in our legal system since the adoption of the 1935 Constitution, well before the U.S. recognized it. Notably, the current constitutional provision specifically protects the privacy of communication and correspondence, to wit:

> Section 3. 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. Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.[17]

Section 3 is thus understood as a subset of the exclusionary rule, along with the guarantee against unlawful searches and seizures.[18]

It should be noted, however, that this constitutional provision does not encompass the entire breadth and scope of privacy as a legal concept. Our Supreme Court has long adopted its American counterpart's expansive interpretation of privacy as an independent right apart from being an exclusionary rule.[19] In fact, the right to privacy is protected through a broad,

---

[15] Whalen v. Roe, 429 U.S. 589 (1977).

[16] Domino & Razon, *supra* note 8, at 903, *citing* William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

[17] CONST. art. III, § 3.

[18] *See* CONST. art. III, § 2.

[19] In *Morfe v. Mutuc*, the Court recognized the right to privacy as deserving of protection in and of itself, independently of considerations of liberty. Said the Court, "The concept of liberty would be emasculated if it does not likewise compel respect for his personality as a unique individual whose claim to privacy and interference demands respect. As Laski so very aptly stated: 'Man is one among many, obstinately refusing reduction to unity. His separateness, his isolation, are indefeasible; indeed, they are so fundamental that they are the basis on which his civic obligations are built. He cannot abandon the consequences of his isolation, which are, broadly speaking, that his experience is private, and the will built out of that experience personal to himself. If he surrenders his will to others,

interconnected swathe of laws, such as the tort provision under Article 26 of the Civil Code,[20] certain provisions of the Revised Penal Code such as those criminalizing libel[21] and classifying dwelling as an aggravating circumstance,[22] the Intellectual Property Code,[23] and the Data Privacy Act of 2012, and reliefs under special proceedings, such as a proceeding for a writ of habeas data.[24]

Not all of these laws are bound by the same principles as Section 3, Article III. The availability of these remedies, and even issues relating to the evidentiary aspects of privacy violations, depend on the legal provision being invoked.[25] This means that the various nuances and distinctions regarding privacy as a legal concept must be kept in mind in appreciating the analysis offered by this article.

That said, the focus of this paper is on the instance when the right to privacy arises in the first place. This is a matter common to most, if not all, of these laws. Logically, for the right to privacy to apply, there must be an expectation of privacy in the first place. It is within these contexts, these so-called "zones of privacy" where government intrusion becomes impermissible unless excused by law and in accordance with customary legal process.[26] The existence of a privacy right is thus determined by a two-pronged test: (1) whether a person has exhibited an actual expectation of

---

he surrenders his personality. If his will is set by the will of others, he ceases to be master of himself. I cannot believe that a man no longer master of himself is in any real sense free.'" *Morfe*, 22 SCRA 424, 442–43.

[20] CIVIL CODE, art. 26.

[21] REV. PEN. CODE, art. 353.

[22] Art. 14(3).

[23] INTELLECTUAL PROP. CODE, § 216–17.

[24] For a more expansive discussion on the various aspects of privacy as a legal concept, especially as a civil tort, *see* John Paul S. Vicencio, *Dissecting the Evolution of Philippine Privacy Torts: Introducing a Three-Pronged Framework for Claiming Damages under the Data Privacy Act of 2012*, 63 ATENEO L.J. 1209 (2019).

[25] Cadajas v. People, G.R. No. 247348, Nov. 16, 2021. In *Cadajas v. People,* the Court, deciding the issue of whether photos taken from the petitioner's Messenger account, noted among other things that when the privacy issue at play deals with laws other than the Bill of Rights, the privacy violation shall be governed by those laws, and the admissibility of the evidence therein shall be determined by the general rules of admissibility under the Rules on Evidence. Moreover, said the Court, "However, where private individuals are involved, for which their relationship is governed by the New Civil Code, the admissibility of an evidence cannot be determined by the provisions of the Bill of Rights."

[26] Ople v. Torres, G.R. No. 127685, 239 SCRA 141, 155–56, July 23, 1998, *citing Morfe*, 22 SCRA 424, 444–45.

privacy; and (2) whether such expectation is one that society is prepared to recognize as reasonable.[27]

Thus, the existence of privacy rights depends heavily on the surrounding circumstances, as there are situations where people voluntarily relinquish their privacy. Privacy considerations are often weighed against other competing rights, and often give way when issues of freedom of speech,[28] freedom of information,[29] or public safety and order[30] require their relinquishment.

This has made privacy one of the more malleable rights under the Bill of Rights, as the very definition of "privacy" hinges heavily on prevailing societal norms. Such norms are hence shaped by changes and developments in societal contexts spurred on by technological advances.

B. Historical Evolution of the Right to Privacy

Examining the historical development of the right to privacy, one can readily sense a recurring theme—that technological developments play a significant role in shifting our collective paradigms regarding privacy. In fact, as this paper hopes to illustrate, technological developments may arguably be the *primary catalyst* in spurring the evolution of privacy as a constitutionally protected right.

Once, privacy was seen as a physical, temporal right primarily tied to property. The existence of a privacy right was conceived in spatial terms or in terms of physical location.[31] Hence, for years, the prevailing notion was that the exclusionary rule operated only in the context of actual physical invasions of a person's privacy. This was the doctrine laid down by the controversial American case of *Olmstead v. United States*,[32] where a divided US Supreme Court held that wiretaps conducted by police officers on private telephone conversations, obtained without a judicial warrant, were not

---

[27] Pollo v. Constantino-David [hereinafter "*Pollo*"], G.R. No 181881, 659 SCRA 189, 206, Oct. 18, 2011, *citing* Katz v. United States, 389 U.S. 437 (1967).

[28] Ayer Productions v. Capulong, G.R. No. 82380, 160 SCRA 861, Apr. 29, 1988.

[29] Kilusang Mayo Uno v. Director General, G.R. No. 167798, 487 SCRA 623, Apr. 19, 2006.

[30] Alejano v. Cabuay, G.R. No. 160792, 468 SCRA 188, Aug. 25, 2005

[31] Yusi, *supra* note 9, 885, 889–90.

[32] [Hereinafter "*Olmstead*"], 277 U.S. 438 (1928).

prohibited by the Fourth or Fifth Amendments of the US Constitution, as wiretapping did not involve a physical intrusion.[33]

However, the emergence of new technologies forced a re-evaluation of these notions. Justice Irene Cortes, writing about the evolution of privacy in the context of the 1960s and 1970s, wrote extensively about her generation's paradigm shift regarding privacy by observing the ways in which radio, television, and even early computer technology provided more opportunities for ordinary people to gain wider and instantaneous publicity, making it more difficult to contain the flow of information about oneself.[34]

Jurisprudence evolved to reflect these changing notions. The *Olmstead* ruling was overturned in the landmark case of *Katz v. United States*,[35] where the Court departed from *Olmstead*'s physical and temporal interpretation of privacy and held that the unreasonable searches and seizures clause extend to non-physical intrusions of space.

In *Katz*, the FBI had wiretapped the telephone conversations of the petitioner Katz, who had been using a public phone booth in order to communicate with his bookmakers. [36] The lower courts applied the *Olmstead* rule in upholding the petitioner's conviction, on the premise that no privacy violation had occurred because the phone booth had not been physically penetrated by the officers. [37] The US Supreme Court reversed the decision, reframing the issue beyond the physical and characterizing the phone booth as a "constitutionally protected area" where he had the "right to privacy" not because of the place itself, but because Katz himself did not wish to publicly expose the information he had disclosed in his private phone call. Because Katz had exhibited a reasonable expectation of privacy, the government's intrusion into his zone of privacy became unlawful. [38]

Katz helped enshrine our modern understanding of privacy as an expectation not tied to physical location but that which is manifested through one's acts and the surrounding context. Privacy is conceived as a series of "zones," which surround a person like concentric circles, with privacy

---

[33] *Id.* at 466.

[34] Irene Cortes, *The Constitutional Foundation of the Right to Privacy*, 7 EMERGING TRENDS IN LAW, 42 (1983).

[35] [Hereinafter "*Katz*"], 389 U.S. 347 (1967).

[36] *Id.* at 348.

[37] *Id.* at 348.

[38] *Id.* at 351–52.

expectation lessening the further one goes from the center. Westin illustrates the concept as follows:

> This core self is pictured as an inner circle surrounded by a series of larger concentric circles. The inner circle shelters the individual's 'intimate secrets' — those hopes, fears and prayers that are beyond sharing with anyone unless the individual comes under such stress that he must put out these ultimate secrets to secure emotional relief. Under normal circumstances no one is admitted to this sanctuary of the personality. The next circle outward contains 'ultimate' secrets, those that can be willingly shared with close relations, confessors, or strangers who pass by and cannot injure. The next circle is open to members of the individual's friendship group. The series continues until it reaches the outer circles of casual conversation and physical expression that are known to all observers.[39]

This traditional understanding, however, seems to be breaking down with the rise of the internet and social media in particular.

The internet was traditionally seen as a virtual realm distinct and separate from the physical realm. A user may "exist" on this virtual realm, and his or her actions may occur in the virtual realm without them necessarily or automatically bleeding over into the physical realm.[40] The "hard barrier" between these two realms has broken down with the growing ubiquity of the internet, however, so much so that cyberspace is no longer a mere virtual parallel to real life, but an inextricable component thereof. The increasing blending of the physical and virtual realms, however, has forced the world to redefine privacy,[41] especially in the online sphere, which has otherwise been perceived as a public space.

This is especially true of social media, whose rise has accelerated the pervasiveness of the internet. Over 60% of the world's population (or around 4.80 billion people) use social media, with daily use averaging around 2 hours and 24 minutes.[42] The Philippines has one of the highest rates of

---

[39] A.F. WESTIN, PRIVACY AND FREEDOM 34 (1967).

[40] *See* Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE 16, 21 (1999).

[41] Mircea Turculet, *Ethical Issues Concerning Online Social Networks*, 149 PROCEDIA – SOCIAL & BEHAVIORAL SCIENCES 967, 969 (2014), *at* https://www.sciencedirect.com/science/article/pii/S1877042814050307.

[42] Dave Chaffey, *Global social media statistics research summary 2023,* May 11, 2023, *available at* https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/.

social media use globally, even earning the unofficial title of "Social Media Capital of the World."[43] In 2021, Filipinos spent an average of 4 hours and 15 minutes each day on social media, nearly double the global average.[44]

These numbers take on significance because the very architecture of social media blurs the distinction between publicity and privacy. Most sites require at least a baseline amount of personal information for one to be able to make an account, such as date of birth, email address, gender, and, of course, one's name. Beyond that, social media sites generally encourage "sharing" information about oneself,[45] through features that allow users to share tidbits of their lives, whether in the form of photos, status updates about one's location, job status, education, or even views and opinions on various everyday issues. Users create a public or semi-public profile within a limited system—i.e., the community of friends "generated" by the profile.

As Mircea Turculet points out, this lends social networks a somewhat oxymoronic character, as one's participation in the virtual world is facilitated mainly by the exchange of information, most of which have a private character.[46] The rise of social media has led to an upsurge of personal information being disclosed online, whether knowingly or not. The fact of social media's ubiquity has translated to millions of people revealing their personal information online at an unprecedented rate.[47]

As will be illustrated in greater detail later on, this is largely due to the way social media sites are structured; the sense of comfort and intimacy they offer to their users; and the level of control they allow the user regarding

---

[43] Statista Research Department, *Number of social media users in the Philippines from 2017 to 2020, with forecasts until 2026* (2021), *available at* https://www.statista.com/statistics/489180/number-of-social-network-users-in-philippines/.

[44] Kyle Chua, *PH remains top in social media, internet usage worldwide,* RAPPLER, Jan. 28, 2021, *at* https://www.rappler.com/technology/internet-culture/hootsuite-we-are-social-2021-philippines-top-social-media-internet-usage.

[45] Peter Suciu, *There Isn't Enough Privacy on Social Media and That is A Real Problem*, FORBES, June 26, 2020, *at* https://www.forbes.com/sites/petersuciu/2020/06/26/there-isnt-enough-privacy-on-social-media-and-that-is-a-real-problem/?sh=9122f7844f11.

[46] Turculet, *supra* note 41, at 969.

[47] Catherine Dwyer, Katia Passerini & Starr Roxanne Hiltz, *Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace*, AMCIS 2007 PROCEEDINGS 339, 340 (2007), *available at* https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007.

the privacy of their posts, even if the post can, in fact, be viewed by a large number of users.[48]

II. EXAMINING *VIVARES*

A. The *Vivares v. St. Theresa's College* Ruling

Vivares v. St. Theresa's College is the first Supreme Court case dealing with the issue of privacy on social media. It came about at a time when data privacy issues were at the forefront of the Philippine news cycle, given the passage of the controversial Republic Act No. 10175 (R.A. No. 10175) or the Cybercrime Prevention Act of 2012.[49]

Vivares involved a group of high school students from St. Theresa's College Cebu who posted photographs of themselves on Facebook, depicting them dressed only in brassieres from the waist up.[50] Other photos also showed them walking down the streets of Cebu in revealing clothing, and smoking and drinking in a bar.[51] These photos landed the girls in trouble when they were reported by fellow classmates. The school found that they had violated the Student Handbook, which prohibited possession of alcohol outside school premises, smoking and drinking in public places, and engaging in "immoral, indecent, obscene and lewd acts."[52] As a result, the school administrators banned the students from participating in their upcoming commencement exercises.[53]

The students protested, their parents intervened, and they successfully obtained an injunction with damages against St. Theresa's College. However, despite the injunction, the school continued to bar them from attending the graduation ceremony.[54] This led to the petitioners filing a petition for a writ of habeas data, arguing that the students' right to privacy

---

[48] *See infra* Part IV.A.

[49] In 2012, the controversial Rep Act No 10175 triggered widespread controversy, even to the point of people lodging protests, due to numerous provisions which were noted for their potential adverse impact on online freedom of expression. *See Cybercrime Law Suspended by Philippines Court*, BBC NEWS, Oct. 9, 2012, *available at* https://www.bbc.com/news/world-asia-19881346.

[50] *Vivares*, 737 SCRA 92, 100–01.

[51] *Id.* at 101.

[52] *Id.*

[53] *Id.* at 102.

[54] *Id.* at 103.

had been violated. In particular, they argued that the students had exhibited a reasonable expectation of privacy on their Facebook accounts, as they had set their privacy settings to "Friends Only."[55] Thus, the photos should not have been disseminated and reproduced without their consent. The petition was dismissed by the Regional Trial Court (RTC), so the petitioners elevated it all the way to the Supreme Court.

The Supreme Court dismissed the petition. While the Court ruled that the writ of habeas data was the proper remedy to defend one's right to informational privacy, it ruled that the petitioners had no reasonable expectation of privacy which would justify granting said remedy.[56] Crucially, while the Court did acknowledge that a reasonable expectation of privacy existed in cyberspace, it tempered its stance, quoting commentators who opined that "[i]n this [Social Networking] environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking."[57] Therefore, the main task of the Court became delineating the extent of the right to privacy on social media.

The Court looked at the privacy settings of Facebook and the controls with which a Facebook user could limit the viewership of their posts, based on the interface of the site as it existed in 2014:

> To address concerns about privacy, but without defeating its purpose, Facebook was armed with different privacy tools designed to regulate the accessibility of a user's profile as well as information uploaded by the user. In *H v. W*, the South Gauteng High Court recognized this ability of the users to "customize their privacy settings," but did so with this caveat: "Facebook states in its policies that, although it makes every effort to protect a user's information, these privacy settings are not foolproof."
>
> For instance, a Facebook user can regulate the visibility and accessibility of digital images (photos), posted on his or her personal bulletin or "wall," except for the user's profile picture and ID, by selecting his or her desired privacy setting:

---

[55] *Id.*

[56] *Id.* at 122–23.

[57] Dwyer et al., *supra* note 47, *citing* Romano v. Steelcase, Inc. and Educational & Institutional Services Inc., 30 Misc. 3d 426, 907 N.Y.S.2d 650, 2010 N.Y. Misc. Lexis 4538, 2010 NY Slip Op 20388, Sept. 21, 2010, and JOSEPH MIGGA KIZZA, ETHICAL AND SOCIAL ISSUES IN THE INFORMATION AGE 109 (2007).

> (a) Public - the default setting; every Facebook user can view the photo;
>
> (b) Friends of Friends - only the user's Facebook friends and their friends can view the photo;
>
> (b) Friends - only the user's Facebook friends can view the photo;
>
> (c) Custom - the photo is made visible only to particular friends and/or networks of the Facebook user; and
>
> (d) Only Me - the digital image can be viewed only by the user.[58]

In order to give effect to the privacy settings on Facebook and not render them a "feckless exercise," the Court calibrated its formulation of reasonable expectation of privacy based on the user's manifest intent to keep their posts private. This manifest intent could be inferred through the user's choice of privacy setting. [59] If a user's posts were set to "public," then a user could claim no reasonable expectation of privacy, since by making one's posts viewable to the public, one forsakes all privacy rights pertaining to the content posted. [60] If a post is set to "Only Me" or a custom set of viewers, then a reasonable expectation of privacy may exist because the user intended to limit the viewership of these posts to a select few people. [61] A user may also manifest the intent to keep posts private by taking special means to limit their viewership.

But the most crucial and most controversial point of contention was the privacy setting "Friends Only" used by the students and on which they anchored their defense. In rejecting this argument, the Court stated that the "Friends Only" setting did not automatically clothe petitioners' posts with a reasonable expectation of privacy because under such setting, the photos were not absolutely hidden from those outside one's friends list. If a user tagged their friend in a photo, that photo would also become visible to the friends of the friend tagged. [62]

If the "Friends Only" setting was chosen, therefore, the user should have taken steps to further limit the viewership of the posts. Moreover, even if there had been a breach, the school itself was not the entity responsible

---

[58] *Vivares*, 737 SCRA 92, 114–15.
[59] *Id.* at 116.
[60] *Id.* at 119.
[61] *Id.* at 117.
[62] *Id.* at 120–21.

for it, as it was simply responding to photos sent to it by Facebook friends of the students in question. The Court also stated that the result may have been different if the petitioners' posts had been limited to "Only Me" or a custom list, as then, "the intention to limit access to the particular post, instead of being broadcasted to the public at large or all the user's friends *en masse*, becomes more manifest and palpable."[63]

The primary import of the Court's ruling is that while there is a right to privacy in cyberspace which should be given effect, the reasonableness of the expectation should be evaluated according to the circumstances. The chief factor seems to be the user's manifest intent to keep the posts private, as demonstrated through the steps they took to restrict the viewership of such posts. This point will be revisited and re-examined later in this paper.[64]

B. Scope of the *Vivares* Ruling

It is crucial to note that the *Vivares* ruling does not impose a blanket rule applicable in all circumstances where privacy rights are affected. *Vivares* arose from an application for a writ of habeas data. Under the Rule on the Writ of Habeas Data, said remedy is available to:

> [A]ny person whose right to privacy in life, liberty, or security is violated or threatened by an unlawful act or omission of a public official or employee, or a private individual or entity engaged in the gathering, collecting, or storing of data or information regarding the person, family, home, and correspondence of the aggrieved party.[65]

Thus, the case itself pertains specifically to privacy as protected by the Rule on the Writ of Habeas Data, rather than the specific right to privacy of communication and correspondence and the exclusionary rule found in the Bill of Rights. In fact, nowhere in the case is Section 3, Article III of the Constitution cited or even mentioned. The distinction should be kept in mind, because, as stated, privacy is protected by numerous laws in our jurisdiction, most of which cannot be interchanged or conflated as each contains its own distinct rules and incidents.

This distinction notwithstanding, *Vivares* is still broadly applicable beyond the context of habeas data, for it deals with the existence of a

---

[63] *Id.*

[64] *See infra* Part. III.A.

[65] HABEAS DATA WRIT RULE, § 1.

reasonable expectation of privacy, which is a standard applicable to most, if not all, of the laws protecting privacy in our jurisdiction. It is relevant not only under the constitutional exclusionary rule,[66] but even to the tort action under Article 26 of the Civil Code,[67] and the Data Privacy Act (in terms of characterizing certain types of personal information).[68]

Thus, *Vivares*' pronouncements are ultimately inextricable from the right to privacy conceived of and protected by the Constitution, and the precedent it lays down regarding online privacy has a marked impact on how the right to privacy is perceived, interpreted, and implemented.

III. PROBLEMS WITH *VIVARES*

A. Logical Inconsistencies

Unfortunately, the Court's pronouncement in this case has problematic areas which must be revisited in the light of evolving standards of social media usage and changing attitudes regarding online privacy.

For one thing, there are portions of the Court's ruling which are logically contradictory. According to the Court, the test for determining the existence of a reasonable privacy expectation on social media is whether the user had *manifested an intent* to limit the viewership of their posts.[69] However, the Court itself did not apply this standard when the setting of "Friends Only" was chosen.

The moment the discussion arrived at the petitioner's choice of "Friends Only" as a privacy setting, the Court's analysis shifted from examining the user's intent in choosing a privacy setting, to the *consequences* of said choice. The petitioners' *very* argument hinged on the fact that choosing "Friends Only" was a manifestation of their intent to limit their posts' viewership. However, the Court focused on the fact that selecting such privacy setting does not prevent one's posts from being viewed by people outside the friend network.[70] Rather than focusing on the user's objective,

---

[66] *Pollo*, 659 SCRA 189.

[67] Spouses Hing v. Choachuy, 699 SCRA 667, June 26, 2013.

[68] Phil. Stock Exch., Inc. v. Sec'y of Finance, G.R. No. 213860, July 5, 2022, at 20. This pinpoint citation refers to the copy of this Resolution uploaded to the Supreme Court Website.

[69] *Vivares*, 737 SCRA 92, 116.

[70] *Id.* at 121.

the decision turned on whether the posts were *in fact* viewable by those outside the user's specified network. In short, the focus was on the *consequence*, rather than the *intent*.

Indeed, many of the Court's concerns regarding the theoretical consequences of "Friends Only" as a privacy setting were largely based on theoretical suppositions. The Court embarked on a long tangent on the hypothetical possibilities whereby the setting "Friends Only" could still be exposed to a wide viewership outside the intended network. For example, if a post set to "Friends Only" tagged certain users, then the friend networks of those users would be able to view the post. This is a fair observation in and of itself, but the way the Court used these hypothetical possibilities to make blanket pronouncements about "Friends Only" as a setting, rather than acknowledging the inherent unpredictability of social media privacy settings in general, is questionable.

Most importantly, it should be noted that the hypothetical scenarios envisioned by the Court *never arose* in the case itself. The respondents were not exposed to the incriminating photos via the tagging of their friends. In fact, nothing of the sort was specifically alleged by the school or the students who reported the offending posts.

Concededly, the *Vivares* ruling is not inflexible, and the language of the Court suggests that its application ultimately depends on the attendant circumstances.[71] However, the way the Court has since applied *Vivares* only strengthens the consequence-based test in determining a reasonable expectation of privacy online. The succeeding case of *Belo-Henares v. Guevarra*[72] involved a series of scathing Facebook posts levied by lawyer Roberto Guevarra against Dr. Maria Victoria "Vicki" Belo-Henares, a celebrity doctor. In defending his posts, Guevarra alleged that his right to privacy had been violated, again invoking his usage of "Friends Only" to limit his posts' viewership.[73] The Court rejected this argument, reiterating *Vivares*' pronouncement that "restricting the privacy of one's Facebook posts

---

[71] *Id.* at 123. This is especially apparent in certain pronouncements of the Court in the case, such as: "Had it been proved that the access to the pictures posted were limited to the original uploader, through the "Me Only" privacy setting, or that the user's contact list has been screened to limit access to a select few, through the "Custom" setting, the result may have been different, for in such instances, the intention to limit access to the particular post, instead of being broadcasted to the public at large or all the user's friends en masse, becomes more manifest and palpable."

[72] [Hereinafter "*Belo-Henares*"], A.C. No. 11394, 811 SCRA 392, Dec. 1, 2016.

[73] *Id.* at 403.

to 'Friends' does not guarantee absolute protection from the prying eyes of another user who does not belong to one's circle of friends."

B. Imprecise Formulation of Liability

Another difficulty with interpreting *Vivares* is that it offered no definite pronouncement on who would have been liable for a privacy violation if the students had actually manifested a reasonable expectation of privacy. Under Section 1 of the Rule on the Writ of Habeas Data, the writ may issue against "a private individual or entity *engaged in the gathering, collecting or storing of data or information.*"[74] The Court spends most of its discussion on the writ interpreting this phrase. According to the Court, the term "engaged" simply means "to do or take part in something"; it does not require that the entity be regularly engaged, such as in a business capacity, in the practice of data collection.[75] Thus, the school did not have to be regularly gathering data on its students for the writ to be validly issued against it.

However, Section 1 of the said Rule also requires an "*unlawful act or omission*" on the part of the data gathering entity.[76] In *Vivares*, the characterization of the school's conduct as unlawful was unclear. While the Court was quick to point out that St. Theresa's College did not resort to any unlawful means in gathering the data, the Court makes no pronouncement on whether the school would have been liable had it been the one to discover the offending photos without the intervention of the petitioners' classmates. Instead, the Court emphasized that St. Theresa's College only received the photos from the girls' classmates; therefore, it was not the school itself that committed the alleged violation of the girls' privacy. However, what if the posts had been set to "Friends Only" and a member of the school administration had inadvertently seen it through a chance encounter? Or if perhaps a teacher could have walked by the girls accessing the photos on their computers and caught a glimpse? Would the girls have exhibited a reasonable enough expectation of privacy in such a situation, given that the teachers normally could not have accessed the photos?

Moreover, it is less clear what would have happened if the students had taken steps to limit viewership of the posts beyond "Friends Only." The Court repeatedly emphasized that it was the students' classmates who had committed the supposed privacy violation, and not the school. However,

---

[74] HABEAS DATA WRIT RULE, § 1.
[75] *Vivares*, 737 SCRA at 109–10.
[76] *Id.*

what if Vivares and her companions had chosen a "custom" setting that blocked those outside their network from viewing the posts?

Instructive to this issue is the recent ruling in *Cadajas v. People*,[77] in which the Supreme Court had to deal with the admissibility of evidence taken from private photos shared on a Messenger chat. In this case, the petitioner Cadajas was accused of violating Section 4(c)(2) in relation to Sections 4(a), 3(b) and 3(c)(5) of R.A. No. 10175 punishing the inducement or coercion of any minor to participate in the creation of child pornography done through a computer system, due to Cadajas having persuaded a minor, AAA, to send him a picture of her breasts through Messenger.[78] AAA sought to have the photos admitted into evidence, but Cadajas invoked the exclusionary rule, arguing that they were taken in violation of his privacy.[79] The Court ruled against Cadajas, holding that he did not exhibit a reasonable expectation of privacy because in giving AAA access to his photos, Cadajas had limited his expectation of privacy relative to AAA. No violation of privacy had occurred as AAA was the one attempting to have the photos admitted into evidence in the first place.[80]

Applying *Cadajas* to the facts in *Vivares*, it would appear that the usage of a custom setting would result in a reasonable expectation of privacy only to those excluded from viewership under the custom setting. If the girls who transmitted the offending photos to the school are outside the custom group of viewers, their uncovering and transmission of the same to the school would constitute a privacy violation. However, this does not address the issue of those in the custom setting then spreading the photos to those outside the custom setting. If the photos are acquired in this manner, then under *Cadajas* they will not be considered as having been taken in violation of Vivares and her companions' privacy.

The combined effect of these rulings is to potentially create a restrictive online environment where users must watch their backs every time they post for fear that what they put out online may be used against them by their schools, employers, or any superior or authority that is liable to screen or monitor social media accounts. As this paper hopes to demonstrate, social media posts are often liable to be taken out of context due to the unique, often idiosyncratic climate of social media itself. This may result in

---

[77] G.R. No. 247348, Nov. 16, 2021.

[78] *Id.* at 2–3. This pinpoint citation refers to the copy of this decision uploaded to the Supreme Court Website.

[79] *Id.* at 6.

[80] *Id.* at 11.

disproportionate, sweeping, and even overbroad consequences on internet users, potentially leading to a sort of chilling effect, the full implications of which will be examined in greater detail in Part V.[81]

C. Failure to Appreciate the Reality of Privacy on Social Media

Aside from the issues explained above, the larger issue at play which this paper hopes to address is that in laying down its standard for reasonable expectation of privacy on social media, the Court exhibited a fundamental misunderstanding of the nature of privacy as it exists on social media. Shunting aside issues of logical inconsistency in its ruling, the Court seems to think that the user's intent is the final word on their manifestation of their reasonable expectation of privacy online.[82] In placing paramount importance on this manifestation of intent, the Court is clearly operating on traditional notions of privacy as an expectation made manifest by one's actions, the reasonability of which is evaluated based on the surrounding circumstances.

Unfortunately, the Court's analysis fails to account for nuances attendant in social media's very ecosystem, which complicates any examination of a social media user's intent in choosing a privacy setting.

It goes without saying that privacy on social media functions differently than the privacy one enjoys in his or her private domicile, or the privacy of information offered when one hides away sensitive data in a locked safe or hidden compartment. Beyond that, however, as will be argued later in this paper, the very architecture of platforms like Facebook often mislead users by lulling them into a false sense of privacy and security, when in reality, users who choose a specific privacy setting have little knowledge of the full implications of their choice.[83] Privacy settings have become increasingly more convoluted and users are often at the mercy of social media sites which increasingly profit off widespread mining of their data. The full implications of these shifting paradigms will be further explored in Part IV.[84]

These issues, combined with the Court's imprecise formulation and inconsistent application of the test they formulated in *Vivares*, raise a whole host of negative implications regarding the state of legal privacy protections

---

[81] *See infra* Part V.

[82] *Vivares*, 737 SCRA 92, 116

[83] *See infra* discussion in Part IV regarding B. Issues with Facebook Privacy Settings.

[84] *See infra* Part IV.

in the online sphere. Thus, the ruling must be re-examined in light of these new developments.

IV. SHIFTING PARADIGMS OF PRIVACY

In his landmark treatise *Understanding Media: The Extensions of Man*,[85] media theorist Marshall McLuhan noted how new media could reshape humanity's collective paradigms relative to the world around them. To McLuhan, the medium, whether it be film, television, or radio, was equally worthy of study as the messages broadcast therewith, since the architecture of the medium profoundly shapes how such content is consumed. "The medium *is* the message," McLuhan writes.[86]

Though McLuhan's work operates in the realm of communication and media studies, his approach may find relevance in the legal sphere, especially as it relates to the changes brought about by the internet, particularly social media. As early as 1999, Lawrence Lessig explored how the very architecture of cyberspace—its "code"—produced a profound normative shift upon any internet user who deigned to enter the virtual realm.[87] In cyberspace, "regulation came through code," and the rules therein are imposed, "not through sanctions, and not by the state, but by the very architecture of the particular space. A law is defined, not through a statute, but through the code that governs the space."[88]

This article argues along the same lines as both McLuhan and Lessig—social media produces a similar normative shift in the way privacy operates in that particular sphere, a shift rooted in how its architecture—its "code"—conditions users to behave. It is thus worth looking at this architecture and its effect on informational privacy online.

A. Nature of Privacy on Social Media

As previously discussed, participation in social media is facilitated mainly by the exchange of information, with most of it having a private character.[89] Social media sites such as Facebook, Twitter, and Instagram

---

[85] Marshall McLuhan, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN (1964).

[86] *Id.* at 10.

[87] Lessig, *supra* note 40, at 20.

[88] *Id.*

[89] Turculet, *supra* note 41, at 969.

encourage "sharing" information about oneself, arguably to a degree far beyond what most would opt for in real-life interactions,[90] given how many avenues for disclosure these sites provide. Upon registering an account, one must provide a baseline amount of personal information about oneself.[91] Afterwards, users are encouraged to share information about their lives, daily activities, beliefs, hobbies, interests, and political opinions.[92] This information can be viewed by the users' friend network. Users can, however, control the flow of information by choosing a privacy setting that will restrict viewership of their posts or profile depending on the chosen category.[93]

The relation between privacy and a person's social network is multifaceted. On certain occasions, users want information about themselves to be known only by a small circle of close friends, and not by strangers. In other instances, users are willing to reveal personal information to anonymous strangers, but not to those who know them better.[94] There are multiple levels of interaction on social media which can complicate any privacy analysis, as observed by Ralph Gross and Alessandro Acquisti:

> First, offline social networks are made of ties that can only be loosely categorized as weak or strong ties, but in reality are extremely diverse in terms of how close and intimate a subject perceives a relation to be. Online social networks, on the other side, often reduce these nuanced connections to simplistic binary relations: "Friend or not". Observing online social networks, Danah Boyd notes that "there is no way to determine what metric was used or what the role or weight of the relationship is. While some people are willing to indicate anyone as Friends, and others stick to a conservative definition, most users tend to list anyone who they know and do not actively dislike. This often means that people are indicated as Friends even though the user does not particularly know or trust the person.
>
> Second, while the number of strong ties that a person may maintain on a social networking site may not be significantly

---

[90] Suciu, *supra* note 45.

[91] This usually involves basic information such as name, date of birth, email address, mobile number.

[92] On Facebook, users' personal information, such as their date of birth, hobbies, educational background, are displayed on their users' "About" page.

[93] *See* Facebook account and privacy settings as of June 17, 2023 *at* https://www.facebook.com/settings/?tab=profile.

[94] Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks*, ACM Workshop on Privacy in the Electronic Society (WPES) 2005, *available at* https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

> increased by online networking technology, Donath and Boyd note that "the number of weak ties one can form and maintain may be able to increase substantially, because the type of communication that can be done more cheaply and easily with new technology is well suited for these ties.
>
> Third, while an offline social network may include up to a dozen of intimate or significant ties and 1000 to 1700 "acquaintances" or "interactions", an online social networks can list hundreds of direct "friends" and include hundreds of thousands of additional friends within just three degrees of separation from a subject.[95]

Though the foregoing passage would seem to support the *Vivares* ruling, it should instead be taken as a sign that the connections formed on social media do not fit neatly within the traditional "concentric circle" network of interpersonal relationships presented by Westin.[96] Social media encourages the type of behavior that enables users to divulge personal information and form connections by adding people they know, even those they are not necessarily close with in real life. This can skew a user's perception of their actual standing regarding the intimacy of their social network, and, by extension, the level of privacy attached thereto. In short, the intent of a user to keep their posts private may not necessarily correspond with their actions when using social media.

This false sense of intimacy can be amplified by social media algorithms, which curate the content of the users "news feed" according to their online behavior, to display content that they will most likely want to see. [97] Among other things, this curation considers who the user interacts with most often.[98] Naturally, because most users tend to frequently interact with people they perceive to be personally close to themselves, the latter's posts will most likely appear on their feeds.

These factors inform the way users behave on social media. A potent illustration of this disconnect regarding online privacy is the so-called "privacy paradox," which refers to the phenomenon of social media users who say they are concerned with privacy but do very little to restrict the reach

---

[95] *Id.*

[96] Westin, *supra* note 39, at 34.

[97] Brent Barnhard, *Everything you need to know about social media algorithms*, Mar. 26, 2021, *at* https://sproutsocial.com/insights/social-media-algorithms/.

[98] *Id.*

or viewership of the content they post online.[99] As a result, the privacy concerns of social media users rarely translate to protective action.[100] A recent meta-analysis of 166 studies including 75,269 participants from 34 countries found that while in general, individuals who are more concerned with and informed about privacy tend to use fewer online services and disclose less personal information, even social media users who express privacy-related concerns behave quite carelessly by engaging in uncensored or inappropriate self-disclosure, inadvertently publicizing their digital footprint, or allowing a wide range of external apps to access their data.[101]

Numerous factors have been suggested as contributive to the privacy paradox. For instance, there may be third-person bias involved as individuals go about using social media thinking that the threats to their privacy do not apply to them but only to other people. Another reason may be that people who are aware of the risks may feel that the benefits of disclosing personal information on social media freely outweigh those risks.[102] After all, most people use social networks to gratify fundamental psychological needs, such as the need to get along, construct and display their values and identity, and be entertained.[103]

The analysis used by the Court in *Vivares* does not account for these nuances. The Court seems to assume, somewhat mechanically, that a person who does not wish to make his posts too publicized would avail of social media privacy tools to restrict access. However, as illustrated, many social media users do not take such steps, but instead rely on a vague, blanket assumption of privacy generated in no small amount by the way social media conditions its users to behave.

B. Issues with Facebook Privacy Settings

Even when a user is prudent about choosing privacy settings, in practice, these privacy settings are not always presented transparently, and thus users are often misled as to how "private" their information actually is on the platform.

---

[99] Tomas Chamorro-Premuzic & Nathalie Nahai, *Why We're So Hypocritical About Online Privacy*, HARVARD BUS. REV. HOME, May 1, 2017, *available at* https://hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy.

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id.*

This is particularly true in the case of Facebook, which has found itself mired in data privacy scandals since its inception due to the lack of clarity regarding privacy settings. A glance at the history and evolution of Facebook's privacy settings tends to show an increasing trend towards leniency when it comes to a user's default privacy settings, and greater willingness to disclose private information submitted by its users. [104] This inclination is best exemplified by a quote from Facebook founder Mark Zuckerberg, who said, "[T]he age of privacy is over,"[105] as norms have evolved considerably since he first co-founded the site.

Back then, a user's private information was not available to anyone outside the groups one specified upon application. As Facebook expanded beyond its original network of college campuses, the controversy began to ensue. When Facebook introduced its trademark News Feed feature in 2006, users were outraged as their personal details were suddenly broadcasted through the Feed. [106] It angered users who did not consent to the publication of personal information and those who did not fully grasp the nature of this new feature.[107]

Facebook thus began introducing privacy settings to allow users to control the flow of information shared on the site. The settings took more or less their current form in 2009, when Facebook unveiled a new set of privacy settings and asked users to choose among them: "Everyone," "Friends of Friends," "Friends Only," "Other."[108] However, the default privacy setting was "Everyone," which many users passively accepted without being aware of the risks and what they consented to, allowing a massive amount of personal information to be disclosed unwittingly.[109]

---

[104] Bianca Bosker, *Visual Guide to Facebook's Privacy Changes Over Time*, July 7, 2010, HUFF. POST (U.S.), *at* https://www.huffpost.com/entry/facebook-privacy-changes_n_568345.

[105] *Id.*

[106] Natasha Lomas, *A Brief History of Facebook's Privacy Hostility Ahead of Zuckerberg's Testimony*, Apr. 10, 2018, *at* https://techcrunch.com/2018/04/10/a-brief-history-of-facebooks-privacy-hostility-ahead-of-zuckerbergs-testimony/.

[107] Natasha Lomas, *A Brief History of Facebook's Privacy Hostility Ahead of Zuckerberg's Testimony*, Apr. 10, 2018, *at* https://techcrunch.com/2018/04/10/a-brief-history-of-facebooks-privacy-hostility-ahead-of-zuckerbergs-testimony/.

[108] Burcu Sayin, Serap Şahin, Dimitrios Kogias & Charalampos Patrikakis, *Privacy Issues in Post Dissemination on Facebook*, 27 TURK. J. OF ELECTRIC ENG'G & COMP. SCIENCE 3417, 3418 (2019), *available at* https://journals.tubitak.gov.tr/cgi/viewcontent.cgi?article=1517&context=elektrik.

[109] *Id.*

Facebook revamped its privacy settings in 2010, but this was insufficient to prevent privacy leaks.[110] Another revamp occurred in 2011, but instead of solving the problem, it caused new problems as people could access the personal data and profiles of users who were not even their "Friends." It made almost all data publicly available through a combination of default settings. This finally prompted Facebook to develop its post-based privacy settings, which subsists to this day. This system was the one in effect during the pertinent events of *Vivares*, where privacy settings were modified to become "Friends," "Friends of Friends," "Public," and "Custom."[111]

Since then, Facebook's privacy track record has somewhat improved, but complaints still subsisted regarding the proliferation of third-party apps which funneled out information from users.[112] Moreover, a bigger and more direct issue was the confusing structure of Facebook's privacy settings. A study conducted from 2005 to 2015 surveyed the privacy settings as they evolved over the given period, and it was found that they became increasingly incomprehensible and confusing, with their usability, clearness, and transparency failing to improve. It left users with fewer options to control their personal information against third-party apps.[113]

Privacy considerations do not just stop with outside viewership. Any information uploaded onto social media will be visible to those running the site. All data provided is stored and recorded, being retained for potential use in data mining.[114] The data can then be transmitted to stakeholders and entities such as advertisers and marketers, who would benefit from using such data.[115] This phenomenon makes delineating privacy on social media difficult, because while users may have the impression that they have made their information sufficiently private using the site's privacy settings, those running the site will necessarily have access to users' data. Thus, the user will not know what their data is being used for, or to whom such data is being disseminated.

Once again, in the case of Facebook, there were numerous third-party apps proliferating in the platform in the early 2010s, such as quiz apps

---

[110] *Id.*

[111] Sayin et al., *supra* note 108.

[112] *Id.* at 3419.

[113] *Id.*

[114] Dwyer et al., *supra* note 47.

[115] Wil Harris, *Why Web 2.0 Will End Your Privacy,* June 3, 2006, *at* https://web.archive.org/web/20120923095940/http://www.bit-tech.net/columns/2006/06/03/web_2_privacy./.

where users were unknowingly funneling their personal information. Various public interest and tech groups accused Facebook of not being fully forthcoming with its information-sharing practices and misleading users to believe they could still maintain control over their personal information. Some US Senators even called on Facebook to rectify the situation.[116] These complaints eventually made their way to the US Federal Trade Commission, resulting in Facebook entering into a 2011 consent decree with the government whereby the case would be settled if Facebook agreed to get the consent of its users before sharing their data with third parties, among other things.[117]

Thus, it can be observed that even when a user tries to regulate the flow of their information on Facebook, they may have far less control than they envision. This makes applying the framework of *Vivares* problematic for a number of reasons. Since *Vivares* emphasizes the consequences of the users' choice regardless of intent, if a user's intent to limit their posts does not result in an actual limitation of their data, the user may lose the reasonable expectation of privacy necessary to trigger the constitutional protection. It thus leaves the users unprotected, among others, when it comes to Facebook's indiscriminate disclosures of user data to third parties.

The *Vivares* framework also runs into issues when it comes to the privacy settings of other social media sites. For example, sites like Twitter and Instagram contain only two layers of privacy settings—'public', and 'protected.' The former allows everyone who logs onto these platforms to view one's profile, while the latter restricts access only to the user's network of followers.[118] An unprotected account can be followed by anyone and they will automatically have access to the profile, but if a user protects their account, they can approve or disapprove follow requests, thus giving them control and discretion over their network.[119]

While Twitter has recently introduced its 'Circles' feature that allows users to post tweets restricted to a circle of "close friends," this still runs into the same issues that Facebook's custom setting faces—namely, that a user posts a tweet restricted to the close friends circle, and someone in the 'Circle' shares the tweet, they will be considered as not having breached the privacy of that user. This does not even get into the numerous bugs affecting the

---

[116] Lomas, *supra* note 106.

[117] *Id.*

[118] *Twitter privacy settings*, *at* https://twitter.com/settings/privacy_and_safety.

[119] *Id.*

functionality of the 'Circles' feature, which severely restricts how private these 'Circles' are and clips their viability as a true custom setting.[120]

Viewed in this light, the Court's ruling seems to create an unjust and inequitable scenario, based on reasoning that does not seem conversant with the reality of social media use. What makes it worse is this flawed reasoning resulted in a precedent that will have a far greater impact beyond the plight of the unlucky students therein, leaving users without useful legal protection for their privacy rights.

V. PROBLEM AREAS

In the preceding sections of this paper, the author argued that the Court's failure to appreciate the unique architecture and environment of social media and how it reshapes traditional notions of privacy may lead to unjust and inequitable results. In Part V, the author will examine the consequences of the Court's flawed ruling in *Vivares* in greater detail by discussing several potential problem areas in the application of the case law.

A. School Expulsions

Going back to the very issue that spawned the *Vivares* ruling in the first place, we must examine the vulnerable position students are placed in by the ruling, especially since they are often subject to the mercy of the school they attend.

In our jurisdiction, schools are given wide discretion as to how they conduct affairs vis-à-vis their students. Schools stand *in loco parentis* over their students, and this principle has traditionally granted them broad discretion as to how to discipline students, resulting in a diminished privacy expectation for students on school grounds.[121] In institutions of higher learning, the constitutional grant of academic freedom has been interpreted to give

---

[120] Amanda Silberling, *Twitter Circle Tweets are not that private anymore*, Apr. 10, 2023, *at* https://techcrunch.com/2023/04/10/twitter-circle-bug-not-private/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKF_Uhkll9b63Kk3QIFuENfQuJozRWImK-zphApiOvOJawezQPPYLw3W98IKqKxD1HmVOtc2H04vRv2YQSlRauJNKLtfVlZw1vaIvmqOa_0TPVpsG9HBgiteHpxqO5ogHyj-7ao3SL1f5IwK3xaHenGeYFsp3jNrhSFwsi7on6sn.

[121] Social Justice Society v. Dangerous Drugs Board, G.R. No. 157870, 742 SCRA 1, Nov. 3, 2008.

colleges and universities the discretion on who to admit.[122] Schools have every right to dismiss students who violate their norms of conduct or fail to meet the prescribed academic qualifications, subject to the requirements of procedural and substantive due process.[123] On the practical side, this makes disputing unwarranted school dismissals challenging, not only because of the valuable time a student must spend defending his or her case at the expense of actually receiving an education, but because the legal defenses available to a student are limited, short of invoking constitutional rights.

The general rule in our jurisprudence is that the authority of the school is co-extensive with its territorial jurisdiction, or its school grounds.[124] However, there are instances in which the school may extend its disciplinary authority outside school grounds, such as in cases where the misconduct of the student involves his status as a student or affects the good name or reputation of the school.[125] This, of course, is an inherently subjective criterion that is highly prone to abuse. The effect of the *Vivares* ruling is to extend this authority to the online realm and allow it to track its students' social media profiles in order to monitor compliance with its norms of conduct. This becomes a problem when one considers that such monitoring of students' social media profiles can very easily translate into a case for dismissal or expulsion.

One particularly notable incident occurred in 2021, when the University of Sto. Tomas (UST) dismissed a Grade 12 student, Datu Ampatuan, Jr., for attending a protest organized by the League of Filipino Students-UST to call for the protection of the democratic rights of all students. In addition, Ampatuan was also ousted from his post as head councilor of the UST Senior High School Student Council. The ground for said expulsion was the school's Code of Conduct, which only allowed students to join organizations "whose objectives uphold the mission and vision of the university" and "are duly recognized by the university."[126]

In the U.S., Kimberly Diei, a pharmacy graduate student at the University of Tennessee, was expelled after her Twitter and Instagram posts

---

[122] *See* Ateneo de Manila University v. Capulong, G.R. No. 99327, 222 SCRA 644, May 27, 1993.

[123] Non v. Dames, G.R. No. 89317, 185 SCRA 523, May 20, 1990.

[124] Angeles v. Sison, G.R. No. 45551, 112 SCRA 26, Feb. 16, 1982.

[125] *Id.*

[126] Jodee A. Agoncillo, *UST Students Protest Dismissal of Grade 12 Student*, PHIL. DAILY INQUIRER, Jan. 23, 2021, *at* https://newsinfo.inquirer.net/1387210/ust-students-protest-dismissal-of-grade-12-student#ixzz7Edvun54T.

were reported to the university's administration. Appearing under a pseudonym, she had posted racy and sexual pictures with provocative captions lifted from popular rap lyrics. Diei had posted such pictures in the spirit of "sex positivity," and she argued that they were well within the bounds of propriety. After an anonymous source reported them for a second time, a disciplinary panel declared Diei's posts "vulgar," "crude," and not in keeping with the mores of her chosen profession, hence her expulsion.[127]

There is also the incident of Yuri Wright, a then high school prep athlete who was, at one point, one of the most in-demand recruits for college football. Unfortunately, his career suffered a major setback when graphic, sexually explicit Tweets he had posted on his private Twitter account surfaced, prompting his conservative Catholic high school to expel him. Many of the colleges who lined up to recruit them had since rescinded or withdrawn their offers. Significantly, his Twitter account was set to private, but his tweets were viewable by a large audience, as he had accepted the follow requests of around 1,700 people.[128]

There are also incidents where students were expelled simply for reposting and sharing memes which were deemed to be objectionable by the school. [129] This occurred in 2019 with Hunter Richardson, a high school student from Lebanon, Ohio, who was expelled from Lebanon High School for posting a salacious meme on social media. [130] Notably, those close to Hunter claimed that students in Lebanon High had been merely suspended for comparatively harsher offenses such as drugs and fighting.[131]

The incident of Brandi Levy is particularly illuminating. Levy was a Pennsylvania high school student whose inflammatory Snapchat posts resulted in her expulsion from the junior varsity squad. She had posted an image of herself and a friend raising their middle fingers, along with captions containing curse words directed at their school and its various varsity sports and cheerleading teams. Some students complained about the message, and

---

[127] Amanda Hartocollis, *Students Punished for 'Vulgar' Social Media Posts Are Fighting Back*, N.Y. TIMES, Feb. 6, 2021, *at* https://www.nytimes.com/2021/02/05/us/colleges-social-media-discipline.html.

[128] *Tweets Get Student Expelled: A Cautionary Tale*, *at* https://www.educationworld.com/a_admin/tweets-get-student-expelled.shtml (last visited Feb. 22, 2023).

[129] *Ohio High School Student Expelled For Posting Explicit Meme to Social Media*, Nov. 27, 2019, *at* https://www.abcactionnews.com/news/national/ohio-high-school-student-expelled-for-posting-explicit-meme-to-social-media.

[130] *Id.*

[131] *Id.*

this led to Levy being removed from the junior varsity squad. Levy challenged the school's order, and her case made it all the way to the Supreme Court. In the resulting case of *Mahanoy Area School District v. B.L.*,[132] the Court held that the school violated Levy's freedom of expression. While the Court acknowledged that the school had power to regulate its students' *behavior* off-campus, it noted that the school's power to regulate *speech* off-campus is necessarily diminished because of the effect it had on the students' freedom of expression.[133] The Court also noted that giving the school unfettered discretion to punish speech off-campus essentially allows it to regulate the student's full 24-hour day,[134] which is plainly unconscionable. Thus, the Court warned against such a state of affairs:

> From the student speaker's perspective, regulations of off-campus speech, when coupled with regulations of on-campus speech, include all the speech a student utters during the full 24-hour day. That means courts must be more skeptical of a school's efforts to regulate off-campus speech, for doing so may mean the student cannot engage in that kind of speech at all. When it comes to political or religious speech that occurs outside school or a school program or activity, the school will have a heavy burden to justify intervention.[135]

The Court did not rule on the issue of privacy in this case and made no pronouncement as to whether the divulging of Levy's images was a violation of her privacy rights. However, the Court's ruling is still relevant as an implicit acknowledgment that some areas of one's life are off-limits to the regulatory authority of a school, even if disseminated in an online platform such as Snapchat. Note that it did not matter to the Court how many people were able to view the posts, nor did the Court seek to impose a blanket rule limiting the school's regulatory activity based on the "place" of posting—whether on or off-campus—or the character of the posts in question. Rather, it weighed each and every circumstance and based its ruling according to the outcome that would most effectively uphold Levy's freedom of expression.

In the U.S., incidents like Diei's, Wright's, and Levy's have sparked a debate as to whether schools should be given the right to police their students' off-campus behavior. Already, the constitutional rights of these students to both free speech and privacy have been raised as a point of

---

[132] 594 U.S. __ (2021).
[133] *Id.* at 8.
[134] *Id.*
[135] *Id.*

contention.[136] In the Philippines, while jurisprudence recognizes that students do not shed their constitutional rights at the school gate,[137] this right is still generally outweighed by the school's authority to discipline its students. Cases like *Vivares* strengthen the latter while undermining the former.

B. Employer Screening of Employees' Social Media Accounts

It is no secret at this point that employers screen the social media accounts of both job applicants and employees. The conduct of background checks on prospective employees is a standard measure on the part of human resource and hiring departments of most companies, and the fact that social media houses vital personal information of its users makes it a particularly useful tool in this regard.[138] Social media is often utilized in the course of conducting background checks on potential job applicants. Recent studies have shown that 70% of employers believe every company should screen candidates' social media profiles during the hiring process.[139]

The consequences of allowing an unfettered exercise of this prerogative can be disastrous, especially for employees, whose posts may often be misconstrued and taken out of context like the aforementioned examples about students. Previous studies have shown that over half of the applicants found on search engines and nearly two-thirds of the applicants found on social networking sites were not hired because of information found thereon.[140] Presumably, this only covers information that was not concealed by any sort of privacy setting. It is difficult to imagine that information available to friends only would be any different, especially as it pertains to those already employed, who are more likely to be Facebook friends with their employers.

---

[136] Hartocollis, *supra* note 127.

[137] Non v. Dames, G.R. No. 89317, 185 SCRA 523, May 20, 1990.

[138] *Social Media Background Checks: Everything You Need To Know*, *at* https://www.indeed.com/recruitment/c/info/social-media-background-checks.

[139] David Cotriss, *Keep It Clean: Social Media Screenings Gain in Popularity*, BUSINESS NEWS DAILY, *at* https://www.businessnewsdaily.com/2377-social-media-hiring.html (last modified May 12, 2023).

[140] Michael Jones, Adam Schuckman & Kelly Watson, *The Ethics of Pre-Employment Screening Through the Use of the Internet* (1996), *at* https://docplayer.net/3226905-The-ethics-of-pre-employment-screening-through-the-use-of-the-internet.html (last visited Feb. 22, 2023).

Even when applicants become employees, most employers remain concerned with their social media presence, with some employers rationalizing that monitoring their accounts is necessary in order to maintain the good name of the company.[141] While this seems like a reasonable concern, excessive monitoring of social media may still potentially "chill" an employee's freedom of expression due to the threat of dismissal or loss of professional standing. Employees who post pictures of themselves in bikinis or other outfits deemed "skimpy" could easily lose the respect of their peers, especially in highly regulated professions. [142] Similarly, employees who post pictures of themselves partying or drinking could potentially incur trouble if their workplace disapproves of such behavior.[143] Even when employees set their posts to private to prevent their employers from viewing their posts, this does not always offer adequate protection. In the U.S., employers have been known to demand access to their employees' social media sites by asking for their login credentials in order to more effectively monitor their social media presences.[144] The problem has grown so significant that several states have already passed laws banning such practices.[145]

Vivares did not rule upon a workplace issue between employers and employees, but the ruling can be applied analogously to such a situation. In the same way that it strengthened the ability of schools to regulate their students in the virtual space, *Vivares* may potentially strengthen the ability of employers to regulate their employees' online presences. Suppose a hypothetical situation involving a disgruntled employee who sees his workplace rival post something on Facebook that he knows their employer would object to, set to "Friends Only." This employee could easily report said post to their employer in order to sabotage the rival's standing in the workplace, or worse, have him dismissed. Such disgruntled employee would be acting within the bounds of the law as dictated by *Vivares*.

C. Social Media Posts as Evidence in Litigation

More generally connected to *Vivares*, but still just as pressing an issue, is the increasing reliance on social media posts as evidence in litigation. Social media is admissible in evidence as electronic documents under Republic Act No. 8792, or the E-Commerce Act of 2000,[146] as well as the

---

[141] *See* Cotriss, *supra* note 139.
[142] Theodore Claypoole, *Privacy and Social Media,* BUS. LAW TODAY, at 1 (2014).
[143] *Id.*
[144] Cotriss, *supra* note 139.
[145] Claypoole, *supra* note 142, at 3.
[146] Rep. Act No. 8792 (2000), § 7. Electronic Commerce Act of 2000.

Rules on Electronic Evidence.[147] Under both enactments, social media posts may be considered as electronic documents, which are functionally equivalent to written documents for evidentiary purposes. Arguably, deleted social media posts may also be considered as ephemeral communications as defined under Rule 2, Section 1(k) of the Rules on Electronic Evidence as referring to "telephone conversations, text messages, chatroom sessions, streaming audio, streaming video, and other electronic forms of communication the evidence of which is not recorded or retained."[148]

Evidence gathered from social media sites has increasingly been resorted to in other jurisdictions and can be proven pivotal in numerous cases.[149] They can serve as a veritable treasure trove of useful documentary and object evidence, especially when the kind of content posted thereon would not be as easily obtainable outside the vehicle of social media. Evidence can be gleaned not just from posts, but even from behavioral patterns exhibited through the users' activity, such as their "Friends" lists and their "Likes," both of which can be indicators of personal relationships and interests of a person.[150]

There is scant jurisprudence as to the admissibility or discoverability of social media posts in the Philippines. The recent ruling in *Cadajas* is one of the first major jurisprudential breakthroughs in this field, and as mentioned, it seems to have trudged down a similar minefield as *Vivares* in allowing private messages and photos transmitted through private chats to be admitted in evidence.

In the U.S., the evidentiary value of social media posts is an emerging issue, and the rulings of some state courts on the issue indicate an attitude to social media privacy not dissimilar to, and arguably less accommodating than, that of *Vivares*. State courts in Florida, for example, have cited the public nature of social networking sites ("SNS") such as Facebook, MySpace, and Twitter as one reason why they reject privacy considerations of litigants regarding social media.[151] Because an individual voluntarily discloses

---

[147] ELEC. EVID. RULE, rule 3, § 1.

[148] Francis Lim, *Are Social Media Posts Admissible In Evidence?*, May 1, 2014, PHIL. DAILY INQUIRER, *at* https://business.inquirer.net/169386/are-social-media-posts-admissible-in-evidence.

[149] Spencer Kuvin & Chelsea Silvia, *Social Media in the Sunshine: Discovery and Ethics of Social Media – Florida's Right to Privacy Should Change the Analysis*, 25 ST. THOMAS L. REV. 335 (2013).

[150] *Id.* at 338.

[151] *Id.* at 341.

information on SNS's in order to publicly display the same, it is well within the public realm and no privacy violation is committed when a litigant's social media posts are admitted in evidence.[152]

Nonetheless, there are dangers attendant to the unfettered admission of social media posts as evidence. The litigation process has a strong potential for unfairly invading a person's private affairs because social media posts can easily be taken out of context, and the threat that they may potentially be used in litigation could have a chilling effect on users, who will then likely limit what they post so that it cannot be used in evidence. Spencer Kuvin and Chelsea Silvia provide a useful illustration of this phenomenon:

> For instance, imagine you have just signed up what you think will be a great auto accident personal injury claim. Your client, Jane Doe, comes into your office in what appears to be great pain, limping, and holding her neck. Her MRIs come back with significant herniations, she is taking various pain medications, and she is recommended for surgery. During your initial intake, you fail to ask about Ms. Doe's social media accounts. During Ms. Doe's deposition with defense counsel, attorney Joe Black presents Ms. Doe with photographs printed from her Facebook profile showing Ms. Doe at Disney with her kids, riding roller coasters, and drinking around the world at Epcot. Ms. Doe is outraged and asks you, "How is he allowed to do this to me?" It appears that Ms. Doe has not only posted these photos just a few months after her car crash, but she also has failed to set any privacy settings on her photos so anyone with an internet connection could view and download these photos, including Joe Black. Welcome to the world of Internet discovery.[153]

On its face, such an intrusion cannot be sanctioned due to the guarantees of privacy of communication and freedom of expression. However, not everyone has come to the same conclusion, if the *Cadajas* ruling and the ambivalent stances taken by American state courts are any indication. As stated, for the purposes of admissibility in litigation, Facebook posts set to "Public" were not accorded any sort of privacy recognition that would render them inadmissible in evidence. The admissibility of posts set to "Friends Only" or "Custom," however, is a thornier issue. In our jurisdiction, as per *Vivares*, posts set to "Friends Only" may be considered admissible. This is reinforced by the *Belo-Henares* ruling[154] where the

---

[152] *Id.*

[153] *Id.* at 336.

[154] *Belo-Henares*, 811 SCRA 392.

respondent's Facebook posts were admitted into evidence because he had not limited the viewership of his posts beyond "Friends Only."

D. Effect of the Anti-Terrorism Act of 2020

The years since the *Vivares* ruling have seen the Philippine landscape change for the worst when it comes to free expression, whether in person or online. The passage of the controversial Anti-Terrorism Act of 2020 has raised fears surrounding its scope and impact. The law massively expands the power of the executive, with provisions giving the Anti-Terrorism Council established under the Act the power to designate individuals and groups as terrorists and detain them without charge for up to 24 days.[155] The law also allows for surveillance and wiretaps,[156] and punishments that include life imprisonment without parole.[157]

According to most critics of the law, its broad and expansive definitions, including that of the crime of "terrorism," could reasonably be interpreted to chill speech critical of the government.[158] While Section 4, which defines terrorism for the purposes of the Act, contains the clause "terrorism as defined in this section shall not include advocacy, protest, dissent, stoppage of work, industrial or mass action, and other similar exercises of civil and political rights," this is quickly followed by the clause "which are not intended to cause death or serious physical harm to a person, to endanger a person's life, or to create a serious risk to public safety." This last clause has been cited as one of the most dangerous provisions of the law, as it can be broadly interpreted.[159]

It is difficult to imagine this state of affairs improving upon the passage of the Act. Already, state officials have announced their intent to regulate social media pursuant to the provisions of the Act.[160] Given its

---

[155] Rep. Act No. 11479 (2020), § 29. Anti-Terrorism Act of 2020.

[156] § 16.

[157] § 4.

[158] Rebecca Ratcliffe, *Duterte's anti-terror law a dark new chapter for Philippines, experts warn*, THE GUARDIAN, July 9, 2020, *at* https://www.theguardian.com/world/2020/jul/09/dutertes-anti-terror-law-a-dark-new-chapter-for-philippines-experts-warn.

[159] JC Gotinga, *Beware of that Two-Faced Clause in the Anti-Terror Law*, RAPPLER, July 13, 2020, *at* https://www.rappler.com/newsbreak/in-depth/266384-beware-two-faced-clause-anti-terror-law.

[160] *Philippines: Government proposes social media regulation under anti-terror law*, INT'L FED. OF JOURNALISTS, Aug. 5, 2020, *at* https://www.ifj.org/media-

broad definition of terrorism, this leaves many groups vulnerable to being labelled as terrorists under the Act, even if they are not actually engaged in acts conventionally considered as terrorism. In 2021 alone, there have been notable incidents of "red tagging," defined as the "labelling, branding, naming and accusing individuals and/or organizations of being left-leaning, subversives, communists, or terrorists [used as] a strategy [...] by State agents, particularly law enforcement agencies and the military, against those perceived to be 'threats' or 'enemies of the State.'"[161]

For example, in July of 2020, several youth groups were red-tagged by the 303rd Infantry Brigade in a series of Facebook posts containing photos of said youth groups protesting during the 2021 State of the Nation Address by then President Rodrigo Duterte, with the caption labelling them as "terrorists" and "virus-carriers."[162] Earlier that same year, there was also the infamous case of Ana Patricia Non, the founder of the Maginhawa Community Pantry, a community relief initiative that fell under suspicion of secretly harboring communist elements due to the social media posts of the National Task Force – to End Local Communist Armed Conflict (NTF-ELCAC), as well as the public comments of its spokesperson, Lt. Gen Antonio Parlade, Jr.[163] The mere suspicion that Non was harboring communist elements led to her and her staff getting red-tagged.[164]

The fears surrounding the law have been somewhat allayed thanks to the recent Supreme Court decision which struck down Section 4 as unconstitutional for being overbroad.[165] However, this does not entirely

---

centre/news/detail/category/press-releases/article/philippines-government-proposes-social-media-regulation-under-anti-terror-law.html.

[161] Nymia Pimentel Simbulan, *Red-Baiting: A Tool of Repression, Then and Now*, 3 OBSERVER 2, 12 (2011), *available at* https://ipon-philippines.org/wp-content/uploads/ObserverJournal/Observer_Vol.3_Nr.2_RedBaiting.pdf#page=12.

[162] Khaela C. Vijar, *Not light threats: Groups slam military for tagging Bacolod youth activists as 'terrorists'*, RAPPLER, Aug 7. 2020, *at* https://www.rappler.com/moveph/groups-slam-red-tagging-bacolod-youth-amid-anti-terror-law/.

[163] *Maginhawa community pantry halts operations; organizer cites red*-tagging, ABS-CBN NEWS, Apr. 20, 2021, *at* https://news.abs-cbn.com/news/04/20/21/maginhawa-community-pantry-redtagging-covid-19.

[164] Cathrine Gonzales, *DILG probes 'police profiling' of Maginhawa community pantry organizer*, INQUIRER.NET, Apr. 21, 2021, *at* https://newsinfo.inquirer.net/1421775/dilg-probes-police-profiling-of-maginhawa-community-pantry-organizer.

[165] Kristine Joy Patag, *SC ruling on Anti-Terrorism Law: 'Small, important win for 'defeated' human rights*, PHIL. STAR, Dec. 9, 2021, *at* https://www.philstar.com/headlines/2021/12/09/2146812/sc-ruling-anti-terrorism-law-small-important-win-defeated-human-rights. *See also* Calleja v. Exec. Sec'y, G.R. No. 252578, Dec. 7, 2021.

remove the potential chilling effect, especially since many of the law's provisions remain in effect. Moreover, even without the law, the Philippine government has prosecuted persons for inflammatory social media posts in the past. In 2020, Ronnel Mas, a schoolteacher, was arrested without a warrant for posting a joke on social media wherein he offered a reward to kill Duterte.[166] While Mas was eventually absolved of the charge and the information against him quashed, the fact that the incident escalated to the point of filing criminal charges is enough to potentially chill freedom of expression online.

As with the school example above, *Vivares* could be applied analogously to a situation wherein social media posts set to "Friends Only" can be used against individuals who upload posts that could potentially be flagged as dangerous, or even as "terrorist acts" under the Anti-Terrorism Act of 2020. Because individuals who limit their viewership to "Friends Only" have not exhibited a reasonable expectation of privacy, anyone who is friends with the individual on Facebook may lawfully flag or report the post to the proper authorities, and doing so would not be considered as a violation of privacy.

E. Synthesis of the Issues

As illustrated earlier, one of the effects of social media is that it exposes people to a wider network than they would ordinarily be comfortable with, thereby amplifying the reach and audience of a person's regular activities and interactions, while at the same time encouraging near-constant connection and interaction with the said network. The architecture of social media encourages the "sharing" of personal details about oneself at every turn, and because of social media's ubiquity, one cannot simply combat the issue by not posting, because detaching from it is almost akin to secluding oneself away and living as a hermit.

The unavoidable conclusion of the discussion, then, is that social media has transformed the world into a more public one, where openness, interaction, and "sharing" of information has become the norm. The obvious effect of this is that the "zones" wherein an individual can enjoy true privacy in the traditional sense are gradually being eroded. Privacy is no longer the default setting in our everyday interactions.

---

[166] Lian Buan, *DOJ okays warrantless arrest of teacher who posted about 'killing Duterte'*, RAPPLER, May 15, 2020, *at* https://www.rappler.com/nation/260961-doj-okays-warrantless-arrest-ronnel-mas-teacher-reward-kill-duterte.

This may have been acceptable back when the internet was a parallel, separate realm, but it should be cause for alarm now that the internet has bled into practically every facet of modern life. Some, like Zuckerberg himself, have even gone as to declare that "the age of privacy is over."[167] Even the Court in *Vivares* realized this: "[i]n this [Social Networking] environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking."[168]

To illustrate the competing privacy considerations at hand and demonstrate how a mechanical application of the traditional privacy paradigm can result in unjust and inequitable results, let us use the example of a mother who breastfeeds her child at home, versus a mother who breastfeeds her child in public.[169] In the former situation, there is a clear delineation of privacy expectation under the constitutional system: one who chooses to breastfeed at home has a greater expectation of privacy than one who does it in public, as the home is a private space free from prying eyes. If a lecherous ogler should sneak a peek at her while she is breastfeeding, she can say her privacy has been invaded, and the law would agree with her.

In the latter situation, however, she is now in a public space shared with strangers who can observe her. The mother necessarily has to expose her breast, normally considered a private part of the body, in order to accomplish her task. It does not take an astute observer to realize her expectation of privacy is diminished, because there is no barrier between the mother and the lecherous ogler who can easily glance at her if he wishes. She *chose* to breastfeed in a public space. But does this mean that she can no longer invoke her right to privacy against the lecherous ogler if he stares at her?

The *Vivares* Court would answer the question depending on the steps the mother took to cover herself up. If she put on some cloth in order to mask her breast, only then she has manifested an expectation of privacy. But if she did not, then she cannot reasonably expect a privacy right in her favor. In essence, it places the burden entirely on the breastfeeding mother, and *not on the lecherous ogler.*

---

[167] Bosker, *supra* note 104.

[168] *Vivares*, 737 SCRA 92, 112, *citing* Romano v. Steelcase, Inc., 30 Misc. 3d 426 (N.Y. Sup. Ct. 2010).

[169] I thank my Supervised Legal Research Faculty Adviser, Judge Raul C. Pangalangan, for this analogy. I am alone responsible for the language and argument above.

Of course, this is patently unjust. Why should the mother, who is minding her own business and performing a normal act performed by all mothers for the health and well-being of her child, be expected to meticulously cover herself up simply to preserve her dignity? Should the State not step in to protect her from those who would harass her? Does the State not have as much of an interest in regulating invasive conduct on the part of the ogler as it does the mother's conduct? To put it more bluntly: even if the mother sheds a part of her privacy to breastfeed her child in public, can it not be said that the ogler has the corresponding obligation to respect her privacy *by not looking?*

The answer to these questions, and indeed, to the discussion as a whole, ultimately depends on one's conception of privacy. Does privacy only exist because of the structures that allow a reasonable expectation of privacy to exist? Or should it exist regardless of whether those structures are present or not?

In a world where the right to privacy is not simply being reshaped, but arguably *eradicated*, the answer seems clear as day, at least if the goal is to preserve the right to privacy. It is thus time we take this reimagined approach to *Vivares*, to reshape its doctrine in a way that meaningfully addresses the issues raised by this paper.

VI. REIMAGINING *VIVARES*

Once again, it is conceded that the *Vivares* doctrine did not intend to impose a blanket rule governing *all* matters relating to privacy on social media. However, the way the *Vivares* doctrine has thus far been applied by the Court reveals a consistent pattern, one that, as demonstrated above, can be analogously applied to other situations. The ways in which the ruling could potentially cause more harm than good have been demonstrated earlier in the paper. It is true, as the Court says, that privacy on social media rests on a shaky foundation, with data breaches and uncertainty characterizing every step, but this should have been cause to accord *more* protection, not less, to provide social media users with a potent legal defense when their rights have been violated.

Thus, it is time to reframe *Vivares* and to evolve its framework in order to be more in touch with the realities of social media use in the modern age.

Vivares was correct in stating that the manifest intent of the user to keep information private should be one of the determining factors for a reasonable expectation of privacy. However, the consequences of their choice of privacy setting should be immaterial. As demonstrated, oftentimes it is outside the user's control who can view their posts, and Facebook's privacy settings have historically proven difficult for most users to understand. Most importantly, according privacy protections to information based on how easily they can be accessed by others despite a user's choice sets a dangerous precedent, and it is doubtful how applicable such a formulation would be even outside the online realm. If a person accidentally or habitually leaves his private documents lying around in his home, does that make the contents of documents any less private?

Therefore, determining social media privacy should not merely rely on the intent of the user or the consequences of his act. Rather, it is submitted that a reasonable expectation of privacy on social media should be based on a holistic, three-fold consideration of: (a) the user's intent to limit a post's viewership; (b) whether the person being shown the post had access to it; and (c) the means by which someone outside the user's network managed to view the post.

Vivares initially starts off with this type of multifaceted approach, but it ultimately errs because it lays a blanket presumption that the "Friends Only" setting does *not* grant a reasonable expectation of privacy, and according to it such status requires further means to limit a post's viewership. Instead, it should be read in the opposite direction—the default rule should be that there is a reasonable expectation of privacy accorded to "Friends Only," and whether a post retains this reasonable expectation should be evaluated under the circumstances.

To illustrate, let us say that A is Facebook friends with B, but is not Facebook friends with C. A sets his post to "Friends Only," and it is seen by B, and B shows it to C without the consent of A. If C should later use the post against A for whatever reason, then it should be inadmissible for having been transmitted outside of A's private network. However, if C merely stumbled upon the post inadvertently, without intending to see its contents and without undertaking any special means himself to view the post, then C should not be considered as having violated A's privacy.

Similarly, the fact that the post may become viewable if someone outside the network is tagged thereon should not affect the overall reasonable expectation of privacy accorded to the *entire* setting of "Friends

Only." It should only be material to the extent of determining which particular posts have been brought outside the user's zone of privacy. Posts that remain viewable only within the "friend" network should remain private, even if the user's other posts become visible to the networks of those tagged.

Of course, this does not provide an easy fix to all the issues that may arise. For example, what if C becomes A's Facebook friend after B shows him A's post? C will have access to A's post once they become friends, but will it still be considered a violation of privacy if the "defect" was retroactively "cured" by A and C becoming part of each other's networks? There is no easy resolution to these issues. Therefore, in modifying and applying these proposed standards, there must be a common denominator to guide the Court in its application.

Guidance may be found in the framework introduced by the oft-overlooked but constitutionally significant case of *Zulueta v. Court of Appeals*.[170] While this case is often viewed as an aberration due to its seemingly inadvertent failure to apply the State Action Doctrine,[171] and has even been declared *obiter* by the Supreme Court[172], this author continues to argue for its jurisprudential value and maintains that there are guiding principles that can be gleaned from the progressive construction of the Constitution found in this case, despite its lack of binding authority.

Zulueta involved a husband and a wife, Dr. Alfredo Martin and Cecilia Zulueta, who were in the throes of a legal separation petition. In order to obtain evidence against her husband, Cecilia ransacked the drawers of her husband to obtain his private documents and letters. [173] The Court declared the evidence inadmissible, but what is notable is the way in which it framed the issue of privacy. First off, it departed from the State Action Doctrine which states that the Bill of Rights only operates as a shield against government intrusions.[174] Instead, it held that the acts of Cecilia, a private person, violated Dr. Martin's privacy, thereby triggering the exclusionary rule in the Bill of Rights.[175] According to the Court, "*any* violation of the right to

---

[170] [Hereinafter "*Zulueta*"], G.R. No. 107383, 253 SCRA 699, Feb. 20, 1996.

[171] *See* Raphael Lorenzo A. Pangalangan, *Blurring of the Public/Private Distinction: Obsolescence of the State Action Doctrine*, 90 PHIL. L.J. 154, 120 (2016).

[172] *Cadajas*, G.R. No. 247348.

[173] *Zulueta*, 253 SCRA at 701.

[174] People v. Marti, G.R. No. 81561, 193 SCRA 57, Jan. 18, 1991.

[175] CONST. art. III, § 2.

privacy renders the evidence obtained inadmissible for any purpose in any proceeding."[176]

Secondly, *Zulueta* saw the Court upending and reframing traditional notions of privacy within the marital domicile by preserving the individual privacy of two spouses joined together by the marital bond. Said the Court:

> Indeed the documents and papers in question are inadmissible in evidence. The constitutional injunction declaring "the privacy of communication and correspondence [to be] inviolable" is no less applicable simply because it is the wife (who thinks herself aggrieved by her husband's infidelity) who is the party against whom the constitutional provision is to be enforced. The only exception to the prohibition in the Constitution is if there is a "lawful order [from a] court or when public safety or order requires otherwise, as prescribed by law." Any violation of this provision renders the evidence obtained inadmissible "for any purpose in any proceeding."[177]

The primary factor that determined the existence of a privacy right in *Zulueta* was the *justness* of the act.[178] The Court did not merely limit itself to a mechanical examination of whether a privacy right existed in a specific context based on previous laws or jurisprudence. Instead, it examined the *substance* of the issue, and framed the issue based on whether the ransacking was justified according to the circumstances.[179]

This flexible, malleable approach should also govern when it comes to social media. Because of the complexities attending social media culture, it is difficult to ascribe to any one framework in resolving every privacy violation thereon. Therefore, courts must be guided by the common denominator of ensuring the most just outcome according to the circumstances, regardless of any hornbook rule on who views the posts or whether a user sufficiently manifested their intent to keep posts private. This may mean extending the notion of zones of privacy to areas which would not conventionally be considered private spaces, but, as we have seen, the Court has already done this numerous times. It can do so again.

---

[176] *Zulueta*, 253 SCRA 704.
[177] *Id.* at 703.
[178] Pangalangan, *supra* note 171, at 120.
[179] *Id.* at 121.

CONCLUSION

By this point, it is clear that the *Vivares* doctrine must be reconsidered in order to account for the nuances and changing trends in social media and online privacy. There are simply too many differences between the "real" physical world and the online world for concepts like "reasonable expectation of privacy" to be simply transmuted from one realm to another wholesale. Privacy on social media is a multi-faceted and complex matter that does not neatly line up with the jurisprudential contours of present-day Philippine privacy law. In laying down its standard for reasonable expectation of privacy, the *Vivares* court overlooked numerous factors that characterize social media privacy, and rather than protect the privacy of the individuals in question, it ended up strengthening the ability of schools, and potentially other regulatory bodies, to admit posts which should have otherwise been outside their purview.

Privacy is an inherently subjective right. It is bound to change with the times, according to societal notions of what constitutes a reasonable expectation of privacy, as well as advancements in science and technology. Social media is merely the most recent in a long line of technological breakthroughs which have shaped and molded the right to privacy. Though it may seem like a novel issue, in truth, this is not the first time the Court has had to recalibrate its approach on how it treats an individual's privacy rights.

Katz shows that the right to privacy can and must evolve in order to respond to advancements in technology and the impact they have on our societal notions of formerly well-entrenched concepts. In future rulings, the Court should adopt this forward-thinking mindset and reformulate the *Vivares* standard accordingly by recognizing the nuances that characterize social media privacy and broadening the scope of reasonable expectation of privacy online.

- o0o -