



Republic of the Philippines
SUPREME COURT
Manila

THIRD DIVISION

**RHONDA AVE S. VIVARES and
SPS. MARGARITA and DAVID
SUZARA,**

Petitioners,

- versus -

**ST. THERESA'S COLLEGE,
MYLENE RHEZA T. ESCUDERO,
and JOHN DOES,**

Respondents.

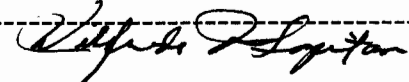
G.R. No. 202666

Present:

VELASCO, JR., J., Chairperson,
PERALTA,
VILLARAMA, JR.,
REYES, and
JARDELEZA, JJ.

Promulgated:

September 29, 2014

X----------X

DECISION

VELASCO, JR., J.:

The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives.

~ Alan Westin, *Privacy and Freedom* (1967)

The Case

Before Us is a Petition for Review on Certiorari under Rule 45 of the Rules of Court, in relation to Section 19 of A.M. No. 08-1-16-SC,¹ otherwise known as the "Rule on the Writ of Habeas Data." Petitioners herein assail the July 27, 2012 Decision² of the Regional Trial Court, Branch 14 in Cebu City (RTC) in SP. Proc. No. 19251-CEB, which dismissed their *habeas data* petition.

The Facts

Nenita Julia V. Daluz (Julia) and Julienne Vida Suzara (Julienne), both minors, were, during the period material, graduating high school students at St. Theresa's College (STC), Cebu City. Sometime in January

¹ Issued on January 22, 2008.

² Penned by Presiding Judge Raphael B. Yrastorza, Sr.

2012, while changing into their swimsuits for a beach party they were about to attend, Julia and Julianne, along with several others, took digital pictures of themselves clad only in their undergarments. These pictures were then uploaded by Angela Lindsay Tan (Angela) on her Facebook³ profile.

Back at the school, Mylene Rheza T. Escudero (Escudero), a computer teacher at STC's high school department, learned from her students that some seniors at STC posted pictures online, depicting themselves from the waist up, dressed only in brassieres. Escudero then asked her students if they knew who the girls in the photos are. In turn, they readily identified Julia, Julianne, and Chloe Lourdes Taboada (Chloe), among others.

Using STC's computers, Escudero's students logged in to their respective personal Facebook accounts and showed her photos of the identified students, which include: (a) Julia and Julianne drinking hard liquor and smoking cigarettes inside a bar; and (b) Julia and Julianne along the streets of Cebu wearing articles of clothing that show virtually the entirety of their black brassieres. What is more, Escudero's students claimed that there were times when access to or the availability of the identified students' photos was not confined to the girls' Facebook friends,⁴ but were, in fact, viewable by any Facebook user.⁵

Upon discovery, Escudero reported the matter and, through one of her student's Facebook page, showed the photos to Kristine Rose Tigol (Tigol), STC's Discipline-in-Charge, for appropriate action. Thereafter, following an investigation, STC found the identified students to have deported themselves in a manner proscribed by the school's Student Handbook, to wit:

1. Possession of alcoholic drinks outside the school campus;
2. Engaging in immoral, indecent, obscene or lewd acts;
3. Smoking and drinking alcoholic beverages in public places;
4. Apparel that exposes the underwear;
5. Clothing that advocates unhealthy behaviour; depicts obscenity; contains sexually suggestive messages, language or symbols; and
6. Posing and uploading pictures on the Internet that entail ample body exposure.

On March 1, 2012, Julia, Julianne, Angela, and the other students in the pictures in question, reported, as required, to the office of Sr. Celeste Ma. Purisima Pe (Sr. Purisima), STC's high school principal and ICM⁶ Directress. They claimed that during the meeting, they were castigated and verbally abused by the STC officials present in the conference, including

³ Facebook is a "voluntary social network to which members subscribe and submit information. x x x. It has created a worldwide forum enabling friends to share information such as thoughts, links, and photographs, with one another." (*H v. W.*, Case No. 12/10142, January 30, 2013, In the South Gauteng High Court, Johannesburg, Republic of South Africa).

⁴ By using the "Friends Only" setting.

⁵ Using "Public" as their Privacy Setting.

⁶ ICM stands for the "Missionary Sisters of the Immaculate Heart of Mary."

Assistant Principal Mussolini S. Yap (Yap), Roswinda Jumiller, and Tigol. What is more, Sr. Purisima informed their parents the following day that, as part of their penalty, they are barred from joining the commencement exercises scheduled on March 30, 2012.

A week before graduation, or on March 23, 2012, Angela's mother, Dr. Armenia M. Tan (Tan), filed a Petition for Injunction and Damages before the RTC of Cebu City against STC, et al., docketed as Civil Case No. CEB-38594.⁷ In it, Tan prayed that defendants therein be enjoined from implementing the sanction that precluded Angela from joining the commencement exercises. On March 25, 2012, petitioner Rhonda Ave Vivares (Vivares), the mother of Julia, joined the fray as an intervenor.

On March 28, 2012, defendants in Civil Case No. CEB-38594 filed their memorandum, containing printed copies of the photographs in issue as annexes. That same day, the RTC issued a temporary restraining order (TRO) allowing the students to attend the graduation ceremony, to which STC filed a motion for reconsideration.

Despite the issuance of the TRO, STC, nevertheless, barred the sanctioned students from participating in the graduation rites, arguing that, on the date of the commencement exercises, its adverted motion for reconsideration on the issuance of the TRO remained unresolved.

Thereafter, petitioners filed before the RTC a Petition for the Issuance of a Writ of Habeas Data, docketed as SP. Proc. No. 19251-CEB⁸ on the basis of the following considerations:

1. The photos of their children in their undergarments (e.g., bra) were taken for posterity before they changed into their swimsuits on the occasion of a birthday beach party;
2. The privacy setting of their children's Facebook accounts was set at "Friends Only." They, thus, have a reasonable expectation of privacy which must be respected.
3. Respondents, being involved in the field of education, knew or ought to have known of laws that safeguard the right to privacy. Corollarily, respondents knew or ought to have known that the girls, whose privacy has been invaded, are the victims in this case, and not the offenders. Worse, after viewing the photos, the minors were called "immoral" and were punished outright;
4. The photos accessed belong to the girls and, thus, cannot be used and reproduced without their consent. Escudero, however, violated their rights by saving digital copies of the photos and

⁷ Entitled *Dr. Armenia M. Tan, for and in behalf of her minor child v. St. Theresa's College, High School Department, Sr. Celeste Ma. Purisima Pe, Mrs. Mussolini S. Yap, Ms. Marnie D. Racaza, Ms. Kristine Rose Ligot (sic), and Ms. Edita Josephine Yu.*

⁸ Entitled *Rhonda Ave S. Vivares, and Sps. Margarita and David Suzara v. St. Theresa's College, Mylene Rheza T. Escudero, and John Does.*

- by subsequently showing them to STC's officials. Thus, the Facebook accounts of petitioners' children were intruded upon;
5. The intrusion into the Facebook accounts, as well as the copying of information, data, and digital images happened at STC's Computer Laboratory; and
 6. All the data and digital images that were extracted were boldly broadcasted by respondents through their memorandum submitted to the RTC in connection with Civil Case No. CEB-38594.

To petitioners, the interplay of the foregoing constitutes an invasion of their children's privacy and, thus, prayed that: (a) a writ of *habeas data* be issued; (b) respondents be ordered to surrender and deposit with the court all soft and printed copies of the subject data before or at the preliminary hearing; and (c) after trial, judgment be rendered declaring all information, data, and digital images accessed, saved or stored, reproduced, spread and used, to have been illegally obtained in violation of the children's right to privacy.

Finding the petition sufficient in form and substance, the RTC, through an Order dated July 5, 2012, issued the writ of *habeas data*. Through the same Order, herein respondents were directed to file their verified written return, together with the supporting affidavits, within five (5) working days from service of the writ.

In time, respondents complied with the RTC's directive and filed their verified written return, laying down the following grounds for the denial of the petition, viz: (a) petitioners are not the proper parties to file the petition; (b) petitioners are engaging in forum shopping; (c) the instant case is not one where a writ of *habeas data* may issue; and (d) there can be no violation of their right to privacy as there is no reasonable expectation of privacy on Facebook.

Ruling of the Regional Trial Court

On July 27, 2012, the RTC rendered a Decision dismissing the petition for *habeas data*. The dispositive portion of the Decision pertinently states:

WHEREFORE, in view of the foregoing premises, the Petition is hereby **DISMISSED**.

The parties and media must observe the aforestated confidentiality.

x x x x

SO ORDERED.⁹

⁹ *Rollo*, p. 39.

To the trial court, petitioners failed to prove the existence of an actual or threatened violation of the minors' right to privacy, one of the preconditions for the issuance of the writ of habeas data. Moreover, the court *a quo* held that the photos, having been uploaded on Facebook without restrictions as to who may view them, lost their privacy in some way. Besides, the RTC noted, STC gathered the photographs through legal means and for a legal purpose, that is, the implementation of the school's policies and rules on discipline.

Not satisfied with the outcome, petitioners now come before this Court pursuant to Section 19 of the Rule on Habeas Data.¹⁰

The Issues

The main issue to be threshed out in this case is whether or not a writ of *habeas data* should be issued given the factual milieu. Crucial in resolving the controversy, however, is the pivotal point of whether or not there was indeed an actual or threatened violation of the right to privacy in the life, liberty, or security of the minors involved in this case.

Our Ruling

We find no merit in the petition.

Procedural issues concerning the availability of the Writ of Habeas Data

The writ of *habeas data* is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party.¹¹ It is an independent and summary remedy designed to protect the image, privacy, honor, information, and freedom of information of an individual, and to provide a forum to enforce one's right to the truth and to informational privacy. It seeks to protect a person's right to control information regarding oneself, particularly in instances in which such information is being collected through unlawful means in order to achieve unlawful ends.¹²

In developing the writ of *habeas data*, the Court aimed to protect an individual's right to informational privacy, among others. A comparative law scholar has, in fact, defined *habeas data* as "a procedure designed to

¹⁰ A.M. No. 08-1-16-SC, February 2, 2008 [Sec. 19. *Appeal*. – Any party may appeal from the judgment or final order to the Supreme Court under Rule 45. The appeal may raise questions of fact or law or both.].

¹¹ *Id.*, Sec. 1.

¹² *Gamboa v. Chan*, G.R. No. 193636, July 24, 2012, 677 SCRA 385.

safeguard individual freedom from abuse in the information age.”¹³ The writ, however, will not issue on the basis merely of an alleged unauthorized access to information about a person. Availment of the writ requires the existence of a nexus between the right to privacy on the one hand, and the right to life, liberty or security on the other.¹⁴ Thus, the existence of a person’s right to informational privacy and a showing, at least by substantial evidence, of an actual or threatened violation of the right to privacy in life, liberty or security of the victim are indispensable before the privilege of the writ may be extended.¹⁵

Without an actionable entitlement in the first place to the right to informational privacy, a *habeas data* petition will not prosper. Viewed from the perspective of the case at bar, this requisite begs this question: given the nature of an online social network (OSN)—(1) that it facilitates and promotes real-time interaction among millions, if not billions, of users, sans the spatial barriers,¹⁶ bridging the gap created by physical space; and (2) that any information uploaded in OSNs leaves an indelible trace in the provider’s databases, which are outside the control of the end-users—**is there a right to informational privacy in OSN activities of its users?** Before addressing this point, We must first resolve the procedural issues in this case.

a. The writ of habeas data is not only confined to cases of extralegal killings and enforced disappearances

Contrary to respondents’ submission, the Writ of *Habeas Data* was not enacted **solely** for the purpose of complementing the Writ of *Amparo* in cases of extralegal killings and enforced disappearances.

Section 2 of the Rule on the Writ of Habeas Data provides:

Sec. 2. *Who May File.* – Any aggrieved party may file a petition for the writ of *habeas data*. However, **in cases of extralegal killings and enforced disappearances**, the petition may be filed by:

- (a) Any member of the immediate family of the aggrieved party, namely: the spouse, children and parents; or
- (b) Any ascendant, descendant or collateral relative of the aggrieved party within the fourth civil degree of consanguinity or affinity, in default of those mentioned in the preceding paragraph. (emphasis supplied)

¹³ See Andres Guadamuz, *Habeas Data and the European Data Protection Directive*, in THE JOURNAL OF INFORMATION, LAW AND TECHNOLOGY (JILT) (2001), cited in former Chief Justice Reynato S. Puno’s speech, *The Common Right to Privacy* (2008).

¹⁴ *Gamboa v. Chan*, *supra* note 12.

¹⁵ See *Roxas v. Macapagal-Arroyo*, G.R. No. 189155, September 7, 2010, 630 SCRA 211.

¹⁶ In *Recasting Privacy Torts in a Spaceless World* by Patricia Sanchez Abril, the term used to refer to the physical space which poses a number of problems in privacy torts that occur in Cyberspace - *a spaceless world*, is “spatial linchpins.” (Harvard Journal of Law & Technology, Vol. 21, Number 1 Fall 2007); See also Kizza, Joseph Migga, *Ethical and Social Issues in the Information Age*, Third Edition, Springer-Verlag London Limited 2007, p. 303 – “The totality of cyberspace is in reality a borderless self-regulating and decentralized mosaic of communities with a variety of cultural, political, and religious agendas.”

Had the framers of the Rule intended to narrow the operation of the writ only to cases of extralegal killings or enforced disappearances, the above underscored portion of Section 2, reflecting a variance of *habeas data* situations, would not have been made.

Habeas data, to stress, was designed “to safeguard individual freedom from abuse in the information age.”¹⁷ As such, it is erroneous to limit its applicability to extralegal killings and enforced disappearances only. In fact, the annotations to the Rule prepared by the Committee on the Revision of the Rules of Court, after explaining that the Writ of *Habeas Data* complements the Writ of *Amparo*, pointed out that:

The writ of *habeas data*, however, can be availed of as an independent remedy to enforce one’s right to privacy, more specifically the right to informational privacy. The remedies against the violation of such right can include the updating, rectification, suppression or destruction of the database or information or files in possession or in control of respondents.¹⁸ (emphasis Ours)

Clearly then, the privilege of the Writ of *Habeas Data* may also be availed of in cases outside of extralegal killings and enforced disappearances.

b. Meaning of “engaged” in the gathering, collecting or storing of data or information

Respondents’ contention that the *habeas data* writ may not issue against STC, it not being an entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party, while valid to a point, is, nonetheless, erroneous.

To be sure, nothing in the Rule would suggest that the *habeas data* protection shall be available only against abuses of a person or entity *engaged in the business* of gathering, storing, and collecting of data. As provided under Section 1 of the Rule:

Section 1. *Habeas Data*. – The writ of *habeas data* is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, **or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party.** (emphasis Ours)

¹⁷ From Former Chief Justice Reynato Puno’s speech, “The Writ of Habeas Data,” delivered on 19 November 2007, at the UNESCO Policy Forum and Organizational Meeting of the Information for all Program (IFAP), Philippine National Committee, citing Enrique Falcon, *Habeas Data: Concepto y Procedimiento* 23 (1996).

¹⁸ Committee on the Revision of the Rules of Court, A.M. No. 08-1-16-SC, *Rule on the Writ of Habeas Data* (2008).

The provision, when taken in its proper context, as a whole, irresistibly conveys the idea that *habeas data* is a protection against unlawful acts or omissions of public officials and of private individuals or entities engaged in gathering, collecting, or storing data about the aggrieved party and his or her correspondences, or about his or her family. Such individual or entity need not be in the business of collecting or storing data.

To “engage” in something is different from undertaking a business endeavour. To “engage” means “to do or take part in something.”¹⁹ It does not necessarily mean that the activity must be done in pursuit of a business. What matters is that the person or entity must be gathering, collecting or storing said data or information about the aggrieved party or his or her family. Whether such undertaking carries the element of regularity, as when one pursues a business, and is in the nature of a personal endeavour, for any other reason or even for no reason at all, is immaterial and such will not prevent the writ from getting to said person or entity.

To agree with respondents’ above argument, would mean unduly limiting the reach of the writ to a very small group, i.e., private persons and entities whose business is data gathering and storage, and in the process decreasing the effectiveness of the writ as an instrument designed to protect a right which is easily violated in view of rapid advancements in the information and communications technology—a right which a great majority of the users of technology themselves are not capable of protecting.

Having resolved the procedural aspect of the case, We now proceed to the core of the controversy.

The right to informational privacy on Facebook

a. The Right to Informational Privacy

The concept of *privacy* has, through time, greatly evolved, with technological advancements having an influential part therein. This evolution was briefly recounted in former Chief Justice Reynato S. Puno’s speech, *The Common Right to Privacy*,²⁰ where he explained the three strands of the right to privacy, viz: (1) locational or situational privacy;²¹ (2) informational privacy; and (3) decisional privacy.²² Of the three, what is relevant to the case at bar is the **right to informational privacy**—usually defined as the right of individuals to **control information about themselves**.²³

¹⁹ <http://www.merriam-webster.com/dictionary/engage>. Last accessed February 13, 2013.

²⁰ Delivered before the Forum on The Writ of Habeas Data and Human Rights, sponsored by the National Union of Peoples’ Lawyers on March 12, 2008 at the Innotech Seminar Hall, Commonwealth Ave., Quezon City. (<http://sc.judiciary.gov.ph/speech/03-12-08-speech.pdf>. Last Accessed, January 24, 2013).

²¹ Refers to the privacy that is felt in physical space, such as that which may be violated by trespass and unwarranted search and seizure. *Id.*

²² Usually defined as the right of individuals to make certain kinds of fundamental choices with respect to their personal and reproductive autonomy. *Id.*

²³ *Id.*

With the availability of numerous avenues for information gathering and data sharing nowadays, not to mention each system's inherent vulnerability to attacks and intrusions, there is more reason that every individual's right to control said flow of information should be protected and that each individual should have at least a reasonable expectation of privacy in cyberspace. Several commentators regarding privacy and social networking sites, however, all agree that given the millions of OSN users, "[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."²⁴

It is due to this notion that the Court saw the pressing need to provide for judicial remedies that would allow a summary hearing of the unlawful use of data or information and to remedy possible violations of the right to privacy.²⁵ In the same vein, the South African High Court, in its Decision in the landmark case, *H v. W*,²⁶ promulgated on January 30, 2013, recognized that "[t]he law has to take into account the changing realities not only technologically but also socially or else it will lose credibility in the eyes of the people. x x x It is imperative that the courts respond appropriately to changing times, acting cautiously and with wisdom." Consistent with this, the Court, by developing what may be viewed as the Philippine model of the writ of *habeas data*, in effect, recognized that, generally speaking, **having an expectation of informational privacy is not necessarily incompatible with engaging in cyberspace activities**, including those that occur in OSNs.

The question now though is up to what extent is the right to privacy protected in OSNs? Bear in mind that informational privacy involves personal information. At the same time, the very purpose of OSNs is socializing—sharing a myriad of information,²⁷ some of which would have otherwise remained personal.

²⁴ *Romano v. Steelcase, Inc. and Educational & Institutional Services Inc.*, Supreme Court of New York, Suffolk County, 30 Misc. 3d 426; 907 N.Y.S.2d 650; 2010 N.Y. Misc. Lexis 4538; 2010 NY Slip Op 20388, September 21, 2010, Decided. See also Kizza, Joseph Migga, *Ethical and Social Issues in the Information Age*, Third Edition, Springer-Verlag London Limited 2007, p. 109, "However, these days in the information age, the value of privacy has been eroded. We can no longer guarantee our privacy. It has left many wondering whether there is such a thing as privacy any more. x x x No one has guaranteed privacy any more unless such an individual is no longer part of the society." Page 304 reads, "According to recent studies, personal privacy is becoming the number-one social and ethical issue of concern for the information age. *Advances in technology have brought with them gadgetry that have diminished individual private spaces through electronic surveillance and monitoring, transmission, scanning, tapping, and fast and more efficient means of collecting, categorizing, and sorting data.*"

²⁵ Puno, *The Common Right to Privacy*, supra note 20.

²⁶ Supra note 3. Penned by Judge N. P. Willis.

²⁷ Including but not limited to the following: name, residence, email address, telephone or cellular phone number, personal pictures, relationship status, date of birth, current location, relatives, hobbies and interests, employment, profession, educational background, preferences, thoughts, messages, conversations, internet memes, videos (ranging from personal videos to scene extracts from movies, television shows, news, *et cetera*), photos, religious messages, political views, updates, commentaries and reactions to current events, support and prayer petitions, as well as products and services.

b. Facebook's Privacy Tools: a response to the clamor for privacy in OSN activities

Briefly, the purpose of an OSN is precisely to give users the ability to interact and to stay connected to other members of the same or different social media platform through the sharing of statuses, photos, videos, among others, depending on the services provided by the site. It is akin to having a room filled with millions of personal bulletin boards or "walls," the contents of which are under the control of each and every user. In his or her bulletin board, a user/owner can post anything—from text, to pictures, to music and videos—access to which would depend on whether he or she allows one, some or all of the other users to see his or her posts. Since gaining popularity, the OSN phenomenon has paved the way to the creation of various social networking sites, including the one involved in the case at bar, www.facebook.com (Facebook), which, according to its developers, people use "to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."²⁸

Facebook connections are established through the process of "friending" another user. By sending a "friend request," the user invites another to connect their accounts so that they can view any and all "Public" and "Friends Only" posts of the other. Once the request is accepted, the link is established and both users are permitted to view the other user's "Public" or "Friends Only" posts, among others. "Friending," therefore, allows the user to form or maintain one-to-one relationships with other users, whereby the user gives his or her "Facebook friend" access to his or her profile and shares certain information to the latter.²⁹

To address concerns about privacy,³⁰ but without defeating its purpose, Facebook was armed with different privacy tools designed to regulate the accessibility of a user's profile³¹ as well as information uploaded by the user. In *H v. W*,³² 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 fool-proof."³³

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:

²⁸ <http://newsroom.fb.com/Key-Facts>. Last accessed January 24, 2013.

²⁹ *H v. W*, supra note 3.

³⁰ *Id.*

³¹ A user's profile contains basic information about the account owner, i.e. Profile Picture, Full name, Birthdate, Address, Place of Work, Profession, a list of the user's "Facebook Friends," among others. It is akin to an Identification Card.

³² Supra note 3.

³³ *Id.*

- (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.

The foregoing are privacy tools, available to Facebook users, designed to set up barriers to broaden or limit the visibility of his or her specific profile content, statuses, and photos, among others, from another user's point of view. In other words, Facebook extends its users an avenue to make the availability of their Facebook activities reflect their choice as to "when and to what extent to disclose facts about [themselves] – and to put others in the position of receiving such confidences."³⁴ Ideally, the selected setting will be based on one's desire to interact with others, coupled with the opposing need to withhold certain information as well as to regulate the spreading of his or her personal information. Needless to say, as the privacy setting becomes more limiting, fewer Facebook users can view that user's particular post.

STC did not violate petitioners' daughters' right to privacy

Without these privacy settings, respondents' contention that there is no reasonable expectation of privacy in Facebook would, in context, be correct. However, such is not the case. **It is through the availability of said privacy tools that many OSN users are said to have a subjective expectation that only those to whom they grant access to their profile will view the information they post or upload thereto.**³⁵

This, however, does not mean that any Facebook user automatically has a protected expectation of privacy in all of his or her Facebook activities.

Before one can have an expectation of privacy in his or her OSN activity, **it is first necessary that said user, in this case the children of petitioners, manifest the intention to keep certain posts private, through the employment of measures to prevent access thereto or to limit its visibility.**³⁶ And this intention can materialize in cyberspace through the

³⁴ Westin, Alan, *Privacy and Freedom*, cited in Valerie Steeves' work, *Reclaiming the Social Value of Privacy*.

³⁵ Newell, Bryce Clayton, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, Richmond Journal of Law and Technology Vol. XVII, Issue 4, 2011, citing Avner Levin and Patricia Sanchez Abril, *Two Notions of Privacy Online*, 11 V AND.J. ENT. & TECH. L. 1001, 1012 (2009) (<http://jolt.richmond.edu/v17i4/article12.pdf>. Last accessed January 31, 2013)

³⁶ It has been suggested that: focus on the individual's control over information allows him to decide for himself what measure of privacy to grant certain topics. It can also relieve the burden of determining responsibility for certain perceived privacy breaches. For example, it is clear that the online socializer who posts embarrassing pictures of himself publicly and without heightened privacy settings is a victim of his own reckless behavior. By publicizing embarrassing information, he voluntarily relinquished control—and a legally recognizable privacy right—over it. (Avner Levin and Patricia Sanchez Abril, *Two Notions of Privacy Online*, 11 V AND.J. ENT. & TECH. L. 1001, 1012 [2009])

utilization of the OSN's privacy tools. In other words, **utilization of these privacy tools is the manifestation, in cyber world, of the user's invocation of his or her right to informational privacy.**³⁷

Therefore, a Facebook user who opts to make use of a privacy tool to grant or deny access to his or her post or profile detail should not be denied the informational privacy right which necessarily accompanies said choice.³⁸ Otherwise, using these privacy tools would be a feckless exercise, such that if, for instance, a user uploads a photo or any personal information to his or her Facebook page and sets its privacy level at "Only Me" or a custom list so that only the user or a chosen few can view it, said photo would still be deemed public by the courts as if the user never chose to limit the photo's visibility and accessibility. Such position, if adopted, will not only strip these privacy tools of their function but it would also disregard the very intention of the user to keep said photo or information within the confines of his or her private space.

We must now determine the extent that the images in question were visible to other Facebook users and whether the disclosure was confidential in nature. In other words, did the minors limit the disclosure of the photos such that the images were kept within their zones of privacy? This determination is necessary in resolving the issue of whether the minors carved out a zone of privacy when the photos were uploaded to Facebook so that the images will be protected against unauthorized access and disclosure.

Petitioners, in support of their thesis about their children's privacy right being violated, insist that Escudero intruded upon their children's Facebook accounts, downloaded copies of the pictures and showed said photos to Tigol. To them, this was a breach of the minors' privacy since their Facebook accounts, allegedly, were under "very private" or "Only Friends" setting safeguarded with a password.³⁹ Ultimately, they posit that their children's disclosure was only limited since their profiles were not open to public viewing. Therefore, according to them, people who are not their Facebook friends, including respondents, are barred from accessing said post without their knowledge and consent. As petitioner's children testified, it was Angela who uploaded the subject photos which were only viewable by **the five of them**,⁴⁰ although who these five are do not appear on the records.

Escudero, on the other hand, stated in her affidavit⁴¹ that "my students showed me some pictures of girls clad in brassieres. This student [sic] of

³⁷ In the same vein that "a person has a reasonable expectation of privacy in e-mail messages stored in computers that he alone could retrieve through use of his own assigned password. An objective expectation of privacy exists with regard to e-mail messages that a person transmits electronically to other subscribers of the same Internet service who have individually assigned passwords." (*United States v. Maxwell*, 42 M.J. 568 (A.F.C.C.A. 1995), 45 M.J. 406 [C.A.A.F. 1996])

³⁸ *Romano v. Steelcase, Inc.*, Supreme Court of New York, Suffolk County, 30 Misc. 3d 426; 907 N.Y.S. 2d 650; 2010 N.Y. Misc. LEXIS 4538; 2010 NY Slip Op 20388, September 21, 2010.

³⁹ *Rollo*, p. 54.

⁴⁰ TSN, July 19, 2012, pp. 32-34; 37.

⁴¹ *Rollo*, p. 134

mine informed me that these are senior high school [students] of STC, who are their friends in [F]acebook. x x x They then said [that] there are still many other photos posted on the Facebook accounts of these girls. At the computer lab, these students then logged into their Facebook account [sic], and accessed from there the various photographs x x x. They even told me that there had been times when these photos were ‘public’ i.e., not confined to their friends in Facebook.”

In this regard, We cannot give much weight to the minors’ testimonies for one key reason: failure to question the students’ act of showing the photos to Tigol disproves their allegation that the photos were viewable only by the five of them. Without any evidence to corroborate their statement that the images were visible only to the five of them, and without their challenging Escudero’s claim that the other students were able to view the photos, their statements are, at best, self-serving, thus deserving scant consideration.⁴²

It is well to note that not one of petitioners disputed Escudero’s sworn account that her students, who are the minors’ Facebook “friends,” showed her the photos using their own Facebook accounts. This only goes to show that no special means to be able to view the allegedly private posts were ever resorted to by Escudero’s students,⁴³ and that it is reasonable to assume, therefore, that the photos were, in reality, viewable either by (1) their Facebook friends, or (2) by the public at large.

Considering that the default setting for Facebook posts is “Public,” it can be surmised that the photographs in question were viewable to everyone on Facebook, absent any proof that petitioners’ children positively limited the disclosure of the photograph. If such were the case, they cannot invoke the protection attached to the right to informational privacy. The ensuing pronouncement in *US v. Gines-Perez*⁴⁴ is most instructive:

[A] person who places a photograph on the Internet precisely intends to forsake and renounce all privacy rights to such imagery, particularly under circumstances such as here, where the Defendant did not employ protective measures or devices that would have controlled access to the Web page or the photograph itself.⁴⁵

Also, *United States v. Maxwell*⁴⁶ held that “[t]he more open the method of transmission is, the less privacy one can reasonably expect. Messages sent to the public at large in the chat room or e-mail that is

⁴² *People v. Dolorido*, G.R. No. 191721, January 12, 2011, 639 SCRA 496.

⁴³ Since the students merely viewed the photographs using their own accounts which are linked to the profiles of the minors, they being Facebook friends.

⁴⁴ 214 F. Supp. 2d at 225.

⁴⁵ Furthermore, “[a] person who places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party. Simply expressed, if privacy is sought, then public communication mediums such as the Internet are not adequate forums **without protective measures.**” *Id.*

⁴⁶ 45 M.J. 406 [C.A.A.F. 199]

forwarded from correspondent to correspondent loses any semblance of privacy.”

That the photos are viewable by “friends only” does not necessarily bolster the petitioners’ contention. In this regard, the cyber community is agreed that the digital images under this setting still remain to be outside the confines of the zones of privacy in view of the following:

- (1) Facebook “allows the world to be more open and connected by giving its users the tools to interact and share in any conceivable way;”⁴⁷
- (2) A good number of Facebook users “befriend” other users who are total strangers;⁴⁸
- (3) The sheer number of “Friends” one user has, usually by the hundreds; and
- (4) A user’s Facebook friend can “share”⁴⁹ the former’s post, or “tag”⁵⁰ others who are not Facebook friends with the former, despite its being visible only to his or her own Facebook friends.

It is well to emphasize at this point that setting a post’s or profile detail’s privacy to “Friends” is no assurance that it can no longer be viewed by another user who is not Facebook friends with the source of the content. The user’s own Facebook friend can share said content or tag his or her own Facebook friend thereto, regardless of whether the user tagged by the latter is Facebook friends or not with the former. Also, when the post is shared or when a person is tagged, the respective Facebook friends of the person who shared the post or who was tagged can view the post, the privacy setting of which was set at “Friends.”

To illustrate, suppose A has 100 Facebook friends and B has 200. A and B are not Facebook friends. If C, A’s Facebook friend, tags B in A’s post, which is set at “Friends,” the initial audience of 100 (A’s own Facebook friends) is dramatically increased to 300 (A’s 100 friends plus B’s 200 friends or the public, depending upon B’s privacy setting). As a result, the audience who can view the post is effectively expanded—and to a very large extent.

This, along with its other features and uses, is confirmation of Facebook’s proclivity towards user interaction and socialization rather than

⁴⁷ McCarthy, Watson and Weldon-Siviy, *Own Your Space: A Guide to Facebook Security*.

⁴⁸ McCarthy, Caroline, *Facebook users pretty willing to add strangers as ‘friends’* (2007) http://news.cnet.com/8301-13577_3-9759401-36.html; https://threatpost.com/en_us/blogs/facebook-you-should-only-friend-people-you-know-no-seriously-were-not-kidding-081911; <http://blog.kaspersky.com/dont-be-facebook-friends-with-strangers/>. Last accessed February 1, 2013.

⁴⁹ Sharing allows a user to post content from another page or user, to his or her own page or to another user’s page.

⁵⁰ A tag is a special kind of link. When you tag someone, you create a link to their timeline. The post you tag the person in may also be added to that person’s timeline. For example, you can tag a photo to show who’s in the photo or post a status update and say who you’re with. If you tag a friend in your status update, anyone who sees that update can click on your friend’s name and go to their timeline. Your status update may also show up on that friend’s timeline. (From Facebook’s Help Center, <http://www.facebook.com/>. Last accessed April 23, 2013)

seclusion or privacy, as it encourages broadcasting of individual user posts. In fact, it has been said that OSNs have facilitated their users' self-tribute, thereby resulting into the "democratization of fame."⁵¹ Thus, it is suggested, that a profile, or even a post, with visibility set at "Friends Only" cannot easily, more so automatically, be said to be "very private," contrary to petitioners' argument.

As applied, even assuming that the photos in issue are visible only to the sanctioned students' Facebook friends, respondent STC can hardly be taken to task for the perceived privacy invasion since it was the minors' Facebook friends who showed the pictures to Tigol. Respondents were mere recipients of what were posted. They did not resort to any unlawful means of gathering the information as it was voluntarily given to them by persons who had legitimate access to the said posts. Clearly, the fault, if any, lies with the friends of the minors. Curiously enough, however, neither the minors nor their parents imputed any violation of privacy against the students who showed the images to Escudero.

Furthermore, petitioners failed to prove their contention that respondents reproduced and broadcasted the photographs. In fact, what petitioners attributed to respondents as an act of offensive disclosure was no more than the actuality that respondents appended said photographs in their memorandum submitted to the trial court in connection with Civil Case No. CEB-38594.⁵² These are not tantamount to a violation of the minor's informational privacy rights, contrary to petitioners' assertion.

In sum, there can be no quibbling that the images in question, or to be more precise, the photos of minor students scantily clad, are personal in nature, likely to affect, if indiscriminately circulated, the reputation of the minors enrolled in a conservative institution. However, the records are bereft of any evidence, other than bare assertions that they utilized Facebook's privacy settings to make the photos visible only to them or to a select few. Without proof that they placed the photographs subject of this case within the ambit of their protected zone of privacy, they cannot now insist that they have an expectation of privacy with respect to the photographs in question.

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.

⁵¹ From Patricia Sanchez Abril's *Recasting Privacy Torts in a Spaceless World*, supra note 16, citing Lakshmi Chaudhry, *Mirror Mirror on the Web*, The Nation, January 29, 2007.

⁵² *Rollo*, pp. 41-42.

On Cyber Responsibility

It has been said that **“the best filter is the one between your children’s ears.”**⁵³ This means that self-regulation on the part of OSN users and internet consumers in general is the best means of avoiding privacy rights violations.⁵⁴ As a cyberspace community member, one has to be proactive in protecting his or her own privacy.⁵⁵ It is in this regard that many OSN users, especially minors, fail. Responsible social networking or observance of the “netiquettes”⁵⁶ on the part of teenagers has been the concern of many due to the widespread notion that teenagers can sometimes go too far since they generally lack the people skills or general wisdom to conduct themselves sensibly in a public forum.⁵⁷

Respondent STC is clearly aware of this and incorporating lessons on good cyber citizenship in its curriculum to educate its students on proper online conduct may be most timely. Too, it is not only STC but a number of schools and organizations have already deemed it important to include digital literacy and good cyber citizenship in their respective programs and curricula in view of the risks that the children are exposed to every time they participate in online activities.⁵⁸ Furthermore, considering the complexity of the cyber world and its pervasiveness, as well as the dangers that these children are wittingly or unwittingly exposed to in view of their unsupervised activities in cyberspace, the participation of the parents in disciplining and educating their children about being a good digital citizen is encouraged by these institutions and organizations. In fact, it is believed that “to limit such risks, there’s no substitute for parental involvement and supervision.”⁵⁹

As such, STC cannot be faulted for being steadfast in its duty of teaching its students to be responsible in their dealings and activities in cyberspace, particularly in OSNs, when it enforced the disciplinary actions specified in the Student Handbook, absent a showing that, in the process, it violated the students’ rights.

OSN users should be aware of the risks that they expose themselves to whenever they engage in cyberspace activities. Accordingly, they should be

⁵³ Parry Aftab of WiredSafety.org.

⁵⁴ Kizza, Joseph Migga, *Ethical and Social Issues in the Information Age*, Third Edition, Springer-Verlag London Limited 2007, p. 117

⁵⁵ Id. at 306.

⁵⁶ Netiquette is the social code of network communication; it is the social and moral code of the internet based on the human condition and the Golden Rule of Netiquette; it is a philosophy of effective internet communication that utilizes common conventions and norms as a guide for rules and standards. <http://www.networketiquette.net/>. Last accessed, February 18, 2013.

⁵⁷ *Technology Trend: Responsible Social Networking for Teens*, <http://www1.cyfernet.org/tech/06-08-TeenUseSM.html>. Last Accessed, February 18, 2013.

⁵⁸ Kizza, Joseph Migga, *supra* note 54, at 341: “Perhaps one of the most successful forms of deterrence has been self-regulation. A number of organizations have formed to advocate parents and teachers to find a way to regulate objectionable material from reaching our children. Also, families and individuals, sometimes based on their morals and sometimes based on their religion, have made self-regulation a cornerstone of their efforts to stop the growing rate of online crimes.”

⁵⁹ *Children’s Safety on the Internet*, Privacy Rights Clearing House, available at <https://www.privacyrights.org/fs/fs21a-childrensafety.htm#1>. Last Accessed, February 18, 2013.

cautious enough to control their privacy and to exercise sound discretion regarding how much information about themselves they are willing to give up. Internet consumers ought to be aware that, by entering or uploading any kind of data or information online, they are automatically and inevitably making it permanently available online, the perpetuation of which is outside the ambit of their control. Furthermore, and more importantly, information, otherwise private, voluntarily surrendered by them can be opened, read, or copied by third parties who may or may not be allowed access to such.

It is, thus, incumbent upon internet users to exercise due diligence in their online dealings and activities and must not be negligent in protecting their rights. Equity serves the vigilant. Demanding relief from the courts, as here, requires that claimants themselves take utmost care in safeguarding a right which they allege to have been violated. These are indispensable. We cannot afford protection to persons if they themselves did nothing to place the matter within the confines of their private zone. OSN users must be mindful enough to learn the use of privacy tools, to use them if they desire to keep the information private, and to keep track of changes in the available privacy settings, such as those of Facebook, especially because Facebook is notorious for changing these settings and the site's layout often.

In finding that respondent STC and its officials did not violate the minors' privacy rights, We find no cogent reason to disturb the findings and case disposition of the court *a quo*.

In light of the foregoing, the Court need not belabor the other assigned errors.

WHEREFORE, premises considered, the petition is hereby **DENIED**. The Decision dated July 27, 2012 of the Regional Trial Court, Branch 14 in Cebu City in SP. Proc. No. 19251-CEB is hereby **AFFIRMED**.


No pronouncement as to costs.

SO ORDERED.





PRESBITERO J. VELASCO, JR.
Associate Justice

WE CONCUR:


DIOSDADO M. PERALTA
Associate Justice

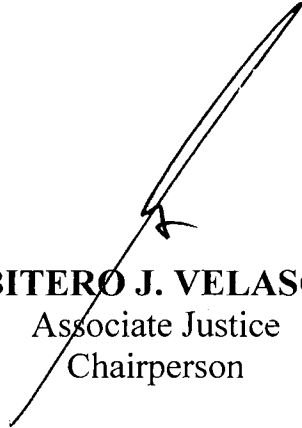

MARTIN S. VILLARAMA, JR.
Associate Justice


BIENVENIDO L. REYES
Associate Justice


FRANCIS H. JARDELEZA
Associate Justice

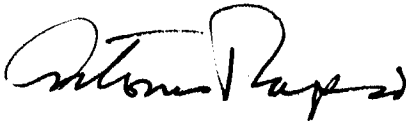
ATTESTATION

I attest that the conclusions in the above Decision had been reached in consultation before the case was assigned to the writer of the opinion of the Court’s Division.


PRESBITERO J. VELASCO, JR.
Associate Justice
Chairperson

CERTIFICATION

Pursuant to Section 13, Article VIII of the Constitution and the Division Chairperson’s Attestation, I certify that the conclusions in the above Decision had been reached in consultation before the case was assigned to the writer of the opinion of the Court’s Division.


ANTONIO T. CARPIO
Acting Chief Justice