Right to Privacy

K. Yngwie Enriquez

Right to Privacy

- The right to privacy is the right to be free from unwarranted publicity, or to live without unwarranted interference by the public in matters in which the public is not necessarily concerned.
- Simply put, the right to privacy is the **right to be left alone**. (*Ople v. Torres*, G.R. No. 127685, July 23, 1998)
- The right to be let alone is the beginning of all freedom – U.S. Supreme Court Justice William O. Douglas.
- Reflected in several laws mandating that a person's right to privacy be respected.

Anti-Wiretapping Act

- Section 1 of Republic Act No. 4200 or the Anti-Wiretapping Act provides:

  Section 1. It shall be unlawful for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word by using a device commonly known as a dictaphone or dictagraph or dictaphone or walkie-talkie or tape recorder, or however otherwise described:

  It shall also be unlawful for any person, be he a participant or not in the act or acts penalized in the next preceding sentence, to knowingly possess any tape record, wire record, disc record, or any other such record, or copies thereof, of any communication or spoken word secured either before or after the effective date of this Act in the manner prohibited by this law; or to replay the same for any other person or persons; or to communicate the contents thereof, either verbally or in writing, or to furnish transcriptions thereof, whether complete or partial, to any other person: Provided, That the use of such record or any copies thereof as evidence in any civil, criminal investigation or trial of offenses mentioned in section 3 hereof, shall not be covered by this prohibition.

New Civil Code of the Philippines

- ARTICLE 26. Every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief:

  (1) Prying into the privacy of another's residence;

  (2) Meddling with or disturbing the private life or family relations of another;

  (3) Intriguing to cause another to be alienated from his friends;

  (4) Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition.

Extent of Right to Privacy

- The protection to privacy under Article 26 of the New Civil Code should not be confined to his house or residence, as it may extend to places where he has the right to exclude the public or deny them access. The phrase “prying into the privacy of another’s residence” covers places, locations, or even situations which an individual considers as private. (*Spouses Hing v. Choachuy*, G.R. No. 179736, June 26, 2013)
- In this case, the respondents installed in their premises two video surveillance cameras facing the petitioners’ property for purposes of obtaining evidence to be used by the former in an injunction suit they were planning to file against the latter. The petitioners complained and asked that the cameras be taken down. The Supreme Court affirmed the petitioners’ right to privacy and ordered the removal of the cameras, declaring that the petitioners have a reasonable expectation of privacy in their property.

Reasonable Expectation of Privacy Test

- Courts have used the Reasonable Expectation of Privacy test in determining whether there are violations of the right to privacy.
- The reasonableness of a person's expectation of privacy depends on a two-part test:
  1. Whether, by his/her conduct, the individual has exhibited an expectation of privacy; and
  2. This expectation of privacy is one that society recognizes as reasonable.
- The reasonableness of a person's expectation of privacy must be determined on a case-to-case basis since it depends on a factual circumstances surrounding the case.
- For instance, a person in a public beach.

Pollo v. CSC Chairperson Constantino-David, G.R. No. 181881, October 18, 2011

- This case involves a search of office computer assigned to a government employee who was charged administratively and eventually dismissed from the service.
- Petitioner failed to prove that he had an actual (subjective) expectation of privacy either in his office or government-issued computer which contained his personal files. Petitioner did not allege that he had a separate enclosed office which he did not share with anyone, or that his office was always locked and not open to other employees or visitors. Neither did he allege that he used passwords or adopted any means to prevent other employees from accessing his computer files. Under this scenario, it can hardly be deduced that petitioner had such expectation of privacy that society would recognize as reasonable.
- Moreover, even assuming arguendo, in the absence of allegation or proof of the aforementioned factual circumstances, that petitioner had at least a subjective expectation of privacy in his computer as he claims, such is negated by the presence of policy regulating the use of office computers.

Pollo v. CSC Chairperson Constantino-David, G.R. No. 181881, October 18, 2011 (con't)

- Office Memorandum No. 10, S. 2002 "Computer Use Policy (CUP)" explicitly provides:
  - *Waiver of privacy rights. Users expressly waive any right to privacy in anything they create, store, send, or receive on the computer through the Internet or any other computer network. Users understand that the CSC may use human or automated means to monitor the use of its Computer Resources.*
  - *Non-exclusivity of Computer Resources. A computer resource is not a personal property or for the exclusive use of a User to whom a memorandum of receipt (MR) has been issued. It can be shared or operated by other users. However, he is accountable therefor and must insure its care and maintenance.*
- Hence, employees have a decreased expectation of privacy with respect to work devices, email accounts, and internet surfing activities. The same may be said for the contents therein, since there is an assumption that its use will be limited to work-related purposes.

NPC Privacy Policy Office Advisory Opinion No. 2018-090

- Facts: "We understand that you were put under preventive suspension and as a result, your office-issued phone and laptop were confiscated. You were advised by your employer to remain logged in using your personal iCloud account in the office-issued phone. You then found out that selected conversations in the phone's messaging applications were shared in a meeting. Also, that Human Resource (HR) personnel were able to access your messages by reinstalling the messaging application using your personal iCloud account.
- After this incident, you filed a case against your employer for constructive dismissal. Due to the severance of your contract and relationship with the company, you opted to log out of your iCloud account and removed access through the office-issued device. However, the HR has been requiring you to log back in in your personal iCloud and provide access to back up files even if you already resigned. Hence, the question of whether this may be considered a violation under the DPA."

NPC Privacy Policy Office Advisory Opinion No. 2018-090 (con't)

- By virtue of a legislation on data protection and privacy (i.e. the DPA), the assumption is that individuals now have an expectation of privacy. Data privacy is now more than a reasonable expectation – it is now enshrined in the DPA. The reasonable expectation of privacy test then should take into consideration the standards provided under the DPA.
- The fact that an employer has the ownership of the electronic means does not rule out the right of employees to privacy of their communications, related location data and correspondence. As such, employees have an expectation of privacy in their own personal iCloud accounts even if they are logged in using their office-issued mobile devices.
- More recent jurisprudence in other jurisdictions also recognizes employee privacy in the workplace. In *Stengart v. Loving Care Agency Inc.*, the New Jersey Supreme Court held that **an employee has a reasonable expectation of privacy in her personal, web-based email correspondence using a company-owned laptop.** The court recognized that though employers can enforce policies relating to computer use to protect the assets, reputation and productivity of a business, they nonetheless have no need or basis to read the specific contents of personal communications in order to enforce corporate policy.

NPC Privacy Policy Office Advisory Opinion No. 2018-090 (con't)

- In *Copland v. the United Kingdom*, the European Court of Human Rights (ECtHR) held that **monitoring of calls and email as well as personal internet usage in the workplace without the person's knowledge, amounted to an interference with her right to respect for her private life and correspondence.** In another case decided by the ECtHR, it was held that an **employer's policy on monitoring communications in the workplace cannot reduce private social life in the workplace to zero**. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.
- In your case, factual circumstances clearly show an expectation of privacy **when you have taken precautionary steps to protect your privacy after being put in preventive suspension. Before surrendering the mobile device upon resignation, you opted to delete the messaging applications as well as the messages contained therein**. Such expectation of privacy is reasonable considering that you have resigned from the company, and in light of the DPA.

Right to Privacy Not Absolute

- The right to privacy cannot be invoked to resist publication and dissemination of matters of public interest.
- Legislators, as public figures, enjoy a more limited right to privacy as compared to ordinary individuals, and their actions are subject to closer scrutiny.
- The right of the people to access information on matters of public concern prevails over the right to privacy of financial transactions. (*Valmonte v. Belmonte*, G.R. No. 74930, February 13, 1989)

Standards of the Right to Privacy

- 3 Standards of the Right to Privacy under *Vivares v. St. Theresa's College*, G.R. No. 202666, September 29, 2014:
  1. **Locational or Situational Privacy** – pertains to privacy that is felt in a physical space. It may be violated through an act of trespass or through an unlawful search.
  2. **Informational Privacy** – refers to the interest in avoiding disclosure of personal matters; and
  3. **Decisional Privacy** – involves the right to independence in making important decisions.

Privacy on Facebook (Vivares case)

- 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. And this intention can materialize in cyberspace through the 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.**
- 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.

Privacy on Facebook (Vivares case) (con’t)

- OSN users should be aware of the risks that they expose themselves to whenever they engage in cyberspace activities. Accordingly, they should be cautious enough to control their privacy and to exercise sound discretion regarding how much information about themselves they are willing to give up. Internet consumers ought to be aware that, by entering or uploading any 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.

Cybersex

- In *Disini v. Executive Secretary*, G.R. No. 203335, February 18, 2014, the petitioners assailed Section 4(c)(1) of the R.A. 10175 or the Cybercrime Prevention Act which prohibited cybersex, expressing fears that private communications of sexual character between husband and wife or consenting adults, which are not regarded as crimes, would be regarded as crimes when done in cyberspace.
- The Supreme Court rejected this argument, saying that the understanding of the legislators is that the element of “engaging in a business” is necessary to constitute illegal cybersex under Section 4(c)(1) of R.A. 10175. Meaning, the said law actually punishes cyber prostitution and pornography for favor and consideration.

Mandatory Drug Tests

- The Supreme Court, in *Social Justice Society v. Dangerous Drugs Board*, G.R. No. 157870, November 3, 2008, ruled on mandatory, random , and “suspicionless” drug tests of students and employees under R.A. 9165 or the Comprehensive Dangerous Drugs Act of 2002:
  - Students – valid, they waived their right to privacy when they enroll in a school, specifically when they committed to comply with reasonable school rules and regulations;
  - Private and government employees – valid, private employees are considered to have a reduced expectation of privacy when they are employed, and government employees are required to be accountable at all times to the people.

Data Privacy Act of 2012

Republic Act No. 10173

(took effect on Sept. 8, 2012)

Score and Personal Information

- Scope - This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines xxx (Section 4)
- Personal Information - Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. (Section 3(g))

Sensitive Personal Information

- Sensitive Personal Information - Sensitive personal information refers to personal information:
  a) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
  b) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
  c) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and
  d) Specifically established by an executive order or an act of Congress to be kept classified.

Processing of Personal Information

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

Processing of Sensitive Personal Information

- SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
  - (a) The data subject has given his or her **consent, specific to the purpose prior to the processing**, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
  - (b) The processing of the same is **provided for by existing laws and regulations**: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
  - (c) The processing is necessary to **protect the life and health of the data subject or another person**, and the data subject is not legally or physically able to express his or her consent prior to the processing;
  - (d) The processing is necessary to **achieve the lawful and noncommercial objectives of public organizations and their associations**: Provided, That such processing is only confined and related to the *bona fide* members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;
  - (e) The processing is necessary for **purposes of medical treatment**, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
  - **(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.**

Non-Applicability

- SEC. 19. Non-Applicability. – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of **scientific and statistical research** and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the **purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject**.

NPC Privacy Policy Office Advisory Opinion No. 2020-043

Is it a violation of the DPA to take screenshots of a private conversation between two individuals, without the consent of both parties? The screenshots were then sent out to a third person without my consent.

- It must first be determined whether such screenshots actually involve personal or sensitive personal information (collectively, personal data).
- The DPA applies to the processing of all types of personal information3 and to any natural and juridical person involved in personal information processing. Processing involves a wide set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.4
- It is worthy to note that the processing, i.e. sending out the screenshot to another person, will only come under the scope of the DPA if personal data is indeed involved – if the conversation/screenshot itself allows for the identification of the parties. If it is simply the content of the conversation, with names and other identifiers redacted or cropped out of the screenshot, it might not be within the scope of the DPA.

NPC Privacy Policy Office Advisory Opinion No. 2020-043 (con't)

- Another factor to consider is whether processing was done by the person in connection with his or her personal, family, or household affairs pursuant to Section 3(h)(2) of the DPA. In such cases, the person is not considered as personal information controller (PIC), and hence, to a certain extent, such processing is generally excluded from the scope of the DPA.
- Nevertheless, depending on the attendant circumstances, the taking of the screenshot and its transmittal to a third party, may not fall under the abovementioned exclusion.
- Hence, the disclosure of a private conversation involving personal data without consent of the parties involved, or without some other lawful basis for processing of personal data under the DPA, may be construed as unauthorized processing, but this is highly dependent on other attendant circumstances of the case as discussed above.

Screenshots may be used as evidence

- Screenshots may be considered a documentary evidence based on the Revised Rules on Evidence and pursuant to the functional equivalence and non-discrimination principles under the E-Commerce Act of 2000 and the Rules on Electronic Evidence. (NPC Privacy Policy Office Advisory Opinion No. 2020-043)
- Photographs and conversations in the Facebook Messages between the accused and the minor victim can be used against the accused to determine his liability for child pornography under the Cybercrime Prevention Act of 2012. (*Cadajas v. People*, G.R. No. 247348, November 16, 2021)
- Online chat logs and videos as evidence does not violate the right to privacy if they are used to determine if a crime has been committed. The DPA allows the processing of sensitive personal information when it relates to the determination of criminal liability of a data subject (Sec. 19) and when necessary for the protection of lawful rights and interests of persons in court proceedings. (Sec. 13) (*People v. Eul Vincent O. Rodriguez*, G.R. No. 263603, October 9, 2024)

CCTV Footage may be used as evidence

- The Rules on Electronic Evidence expressly provide for the admissibility of video recordings as evidence in court, provided that: (1) it shall be shown, presented or displayed to the court; and (2) it shall be identified, explained or authenticated by the person who made the recording or by some other person competent to testify on the accuracy thereof. (Section 1, Rule 11 of the Rules on Electronic Evidence)
- Persons authorized to authenticate the video or CCTV recording is not limited solely to the person who made the recording but also by another witness who can testify to its accuracy. (*People v. Manansala*, G.R. No. 233104, 02 September 2020)
- The party presenting the recording to account for: (1) its origin; (2) how it was transferred to a storage device; and (3) how it reached the trial court for its presentation. (*People v. Concepcion*, G.R. No. 249500, 06 December 2021)

Thank you and study well