



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

RLA,

Complainant,

NPC 18-010

-versus-

(Formerly CID Case No. 18-D-010)

For: Violation of the Data Privacy Act)

PXE,

Respondent.

x-----x

DECISION

LIBORO, P.C.:

Before this Commission is a Complaint filed by RLA (Complainant) against Respondent PXE for violation of the Data Privacy Act of 2012 (“DPA” or “Data Privacy Act”) when it published the Complainant’s personal information in its White Pages without the consent of the Complainant.

Facts¹

Complainant alleged that he was a regular employee of KPI (KPI) and that he was provided a PXE Digital Subscriber Line (DSL) subscription as part of his employment package. Further, that on 12 January 2016, he filled out a PXE DSL subscription application form that was submitted to Respondent to activate the DSL facility installed at his then residence at Las Piñas City.

¹ Fact-Finding Report dated 13 October 2020.

On 12 April 2016, Complainant requested the same DSL facility to be transferred to his new residential address also at Las Piñas City.

Complainant narrated that on 21 March 2018, someone called and looked for him through his PXE-issued landline number that was bundled together with the DSL subscription. The caller allegedly wanted to offer some products to KPI. The caller told him that she obtained his number and address from PXE's telephone directory – the White Pages.

Alarmed, Complainant called PXE's hotline number and sent an email to smecare@PXE.com.ph to inquire why his number and address were published in their directory without his consent.

The PXE customer service representative mentioned that Complainant's telephone number was tagged as confidential in PXE's system.

Complainant sent another email to smecare@PXE.com.ph for further clarification why his personal information was published in PXE's telephone directory. The customer service representative told Complainant that the involved number has been tagged as published in PXE's telephone directory listing since it was not requested as confidential via customer information form upon application. Complainant stated that there was no such option on the application form. Acting on Complainant's concern, PXE's agent replied that his personal information would be tagged as confidential and will no longer be published in the 2018 telephone directory. Complainant avers that the agent's response supports his allegation that his personal information was originally published and was not treated as confidential.

Complainant asserted that PXE's disclosure of his personal information was done without his consent and it poses great risk to

his security and to his family. He further claims that his father's life was in danger and as a proof he adduced DSWD Certificate. According to the Complainant, he must protect his father's welfare at all cost, including keeping his personal information confidential, even from their relatives and friends.

On 04 July 2018, this Commission, through the Complaints and Investigation Division (CID), conducted a Discovery Conference where both parties appeared. Both parties requested for continuance of their discussion of the case.

On 11 August 2018, another Discovery Conference was conducted. This time, the parties manifested that they are both willing to enter into an amicable settlement. Thus, they were given a period of fifteen (15) days from the date of the Discovery Conference or until 26 August 2018 to submit a notarized Compromise Agreement. However, the parties were unable to settle the case amicably within the given time.

On 05 October 2018, PXE filed its responsive Comment. PXE argued that it is mandated by law to issue a listing directory of the names, addresses, and telephone numbers of all its subscribers. The publication of Complainant's personal information was done in the performance of its mandate under existing Philippine laws.

In particular, PXE stated that under Section 149 of Commonwealth Act No. 146, otherwise known as the Public Service Act, PXE, as an entity operating a "telephone public service" is required, at least once a year, to issue a listing directory showing therein the names of all subscribers, together with their addresses, telephone numbers and such other information as may of interest to subscriber's everyday use of his telephone. In compliance with its obligations under the laws and regulations mentioned above, PXE implemented its internal rules that was approved by the Public Service Commission in 1970.

PXE also contended that it was merely acting upon the instructions of its customer, KPI, which was the personal information controller of the Complainant's personal information. It explained that PXE is in the business of providing communication services to corporations. PXE transacts with corporate/group clients/customers even if the ultimate recipients of the communication services it provided are individual persons connected to the corporate clientele. In PXE's process, the corporate clients/customers provide the required information of the end-user to facilitate the rendition of services, among others.

The relevant subscription agreements/contracts were unequivocally signed between PXE and KPI. KPI, as a corporate client of PXE, was the provider of DSL subscriptions for the benefit of its employees including the Complainant. In other words, it was KPI that applied for a corporate DSL account with PXE on behalf of Complainant. Moreover, the required application form was made in the name of KPI and from PXE's perspective, it appeared that Complainant had no participation in accomplishing the forms. Considering that the application involved was a corporate account, PXE published the details indicated in the application form in the White pages - Government and Business Book 2017.

PXE elaborated that the terms and conditions of the application form stated that it shall provide its telephone services in accordance with the rules and regulations issued by other appropriate government agencies. It is KPI, as a corporate subscriber of PXE's services, which has the option to decide whether to publish the names, addresses and telephone numbers provided in the DSL subscription application form.

PXE further argued that KPI as the personal information controller of Complainant, has the duty to ensure that the rights of Complainant as a data subject are upheld. KPI was responsible for ensuring that Complainant gave his informed consent to the processing of his personal information. KPI should have informed

Complainant of its option not to be listed in the directory for publication and relay the chosen option to PXE as the personal information processor. However, KPI never requested from PXE not to publish Complainant's personal information. Had KPI clarified with PXE that Complainant intended to keep his personal information confidential, PXE would have complied.

For PXE, no breach was concealed because the publication of Complainant's information was made under legal compliance and was known to KPI. PXE explained that intentional breach is committed when a person knowingly and unlawfully violates data confidentiality and security data systems or breaks into system where personal and sensitive personal information are stored. Complainant also failed to show how PXE unlawfully obtained his personal data, as it obtained his personal information under its agreement with KPI.

PXE raised that Complainant has no proof of actual threat of abduction on his father and that the publication of his whereabouts caused security risks to the safety of his family. He failed to show how the publication of directory risked the safety of his family because his whereabouts can be easily known on his and his family's posts on Facebook, all set to public mode. Such act is contrary to his claim that he and his family were in hiding from the abductors of his father.

As remedial action, PXE updated the DSL application forms for corporate accounts and the relevant internal rules in processing such accounts.

PXE took immediate action to reinforce its procedure for handling customer cases and concerns on data privacy and protection.

On 05 October 2018, Complainant in his Reply argued that PXE's statutory obligation to automatically publish their subscribers' personal information even without prior consent of the data subject is a clear violation of National Telecommunication Commission (NTC) Memorandum Circular No. 05-06-2007, known as Consumer Protection Guidelines, and the Data Privacy Act.

Complainant gave his consent to his employer, KPI, only for purpose of availing the DSL facility at his residence as part of the employment privilege. Had he known that his information will be published, he would have stopped the processing of his application.

Complainant also stated that KPI was not aware that PXE can automatically decide to publish the subscriber's personal information since its request to PXE was only to install the DSL facility. The option not to publish its subscribers' personal information is nowhere to be found on the application form. He also alleged that the terms and conditions at the back of the application form is not readable and it is not indicated that the personal information will be processed for public disclosure.

In a meeting with PXE's Data Privacy Team on 13 July 2018, Complainant presented the police report, DSWD certifications and court cases indicating that his father's life was threatened due to the exposure of their address. During the said meeting, PXE, through its Chief Data Privacy Officer, offered an immediate option to change his telephone number or a CCTV be installed at Complainant's existing residence. Complainant perceived these offers as a recognition on the part of PXE of the severity of Complainant's situation.

Complainant justified that his posting of pictures on social media was for their friends and relatives, who were unable to visit or talk to them personally for security reasons. Furthermore, Complainant also alleged that he used aliases on his social media account to protect his identity and the pictures were taken outside

Complainant's present residence. Complainant believes that his father should neither be deprived of his liberty to enjoy life with his family nor be locked in a certain place.

Complainant alleged that he and his father relocated several times after the abduction of the latter. After some time, Complainant needed to relocate his father to a different place to secure his safety. However, when PXE published his address in its White Pages, Complainant knew that his safety and that of his father were jeopardized after somebody called his landline telephone to verify his name and residential address as seen on the PXE's White Pages. Complainant believed that the publication of his personal information can never be corrected because it can no longer be recalled from the public. The only remedy he had in mind was to relocate again to another place.

Due to such publication, Complainant accused PXE of violating the following provisions of the DPA:

- a. Section 28 for *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes*, when Complainant was not informed of the purpose for processing his personal information and to whom said information will be disclosed;
- b. Section 29 for *Unauthorized Access or Intentional Breach*, when Complainant's personal information was published intentionally and knowingly published even with the presence of the prevailing law under National Telecommunication Commission and Data Privacy Act;
- c. Section 30 for *Concealment of Security Breaches Involving Sensitive Personal Information*, when PXE's customer service representative told Complainant that his personal information was already tagged as confidential during his

initial inquiry in March 2018 when it only started to be confidential for their June 2018 publication; and

- d. Section 32 for *Unauthorized Disclosure*, when Complainant's personal information was published in PXE's White Pages without his consent.

Complainant prayed for actual damages representing the cost of their several relocations to safeguard their welfare and for moral damages representing the mental anguish, fright, anxiety, sleepless nights, and emotional stress caused to the Complainant for jeopardizing the safety of his family due to the disclosure of their exact address.

Issue

Whether or not the publication of Complainant's personal information particularly, his name and residential address, in the White Pages by PXE, is in violation of Sections 28, 29, 30 and 32 of the Data Privacy Act.

Discussion

The Complainant's contentions are partly meritorious.

I. Personal data is involved and PXE is a personal information controller

The facts establish that the name, telephone number and residential address were published in PXE's 2017 telephone directory, also called as White Pages.

Under the Data Privacy Act, *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.²

The name, telephone number and residence address of Complainant are considered personal information under the DPA because his identity is apparent based on the given information. PXE, as the entity holding his mentioned personal information, can also directly ascertain his identity therefrom.

Furthermore, under the Data Privacy Act, a *personal information controller* (PIC) is defined as, “a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.”³ Meanwhile, *personal information processor* (PIP) is “any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.”⁴

In this case, the Complainant’s personal information, as found in the PXE application form, was supplied by his employer, KPI. The subscription was named under KPI for the account of Complainant. This is also supported in the customer conforme portion of the form where Mr. BCA, President and General Manager of KPI, is the signatory in the application form. KPI’s address is also indicated in the billing portion of the form.

KPI, being the corporate customer of PXE, supplied to the latter the personal information of their employees who will be provided with PXE’s services as part of employment benefits.

² Republic Act No. 10173, Section 3 (g).

³ Republic Act No. 10173, Section 3(h).

⁴ *Id.*, at Section 3(i).

However, it is PXE that decided what information were collected from KPI's employees, including that of the Complainant, to apply for PXE's services. KPI merely supplied the personal information of its employees to PXE, but the control over the personal information provided remained with PXE.

PXE processed the personal information of the Complainant for the purposes of DSL subscription and publishing of personal information in the White Pages. Thus, PXE, for the purposes discussed about above, is the PIC and not simply the PIP.

II. PXE's violation of the Data Privacy Act

a. Processing of Personal Information for Unauthorized Purposes

Section 28 of the DPA penalizes processing of personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws, to quote:

SEC. 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. - The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information **for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.** (Emphasis and underlining supplied)

To be held liable under section 28 the PIC/PIP must process personal data in violation of the purpose consented to or authorized by the data subject, or otherwise authorized by the DPA or under existing laws.

Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information.⁵

When the processing of personal information is based on consent, the PIC must obtain the consent in relation to the declared purpose for processing. The consent must likewise be evidenced by written, electronic or recorded means.⁶

In this case, the recorded means that manifest the consent of the Complainant is PXE's Application Form⁷ and the attached PXE's Terms and Conditions that was printed on the back of the Form.⁸ We note however, that while the Terms and Conditions discuss the contractual relations that govern the usage, grant and maintenance of the DSL services between the Complainant and PXE, the same does not include authority or consent to publish the list of names, contact information and address in the White Pages.

Thus, we find that the consent given by Complainant in filling up the application form relates only to the use and limitations of the DSL services offered by PXE, and not as to the publication of Complainant's personal information in the White Pages. Stated simply, the processing by PXE was done for purposes not authorized by Complainant.

⁵ Section 3 (b), Data Privacy Act of 2012

⁶ *Id.*

⁷ Records at pp. 3

⁸ Records at pp. 4

This being the case, we now come into the determination on whether PXE processed Complainant's information in conformity with the DPA and other existing laws.

The Data Privacy Act, as a general rule, allows for the processing of personal information when at least one criterion for lawful processing under Section 12⁹ is present, thus:

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;

x x x

PXE argued that it is required to publish the personal information of Complainant pursuant to a legal obligation as required by Commonwealth Act No. 146, otherwise known as the Public Service Act, which has been amended by Commonwealth Act No. 454 which provides for the regulation of public services, specifically wire and wireless communication.

Revised Order No. 1 or the Public Service Commission Rules and Regulations for all Public Services was further enacted to implement the Public Service Act. Section 149 of Revised Order No. 1 clearly mandates each telephone public service to issue a listing directory at least once a year, *to wit*:

⁹ Emphasis and underlining supplied.

Telephone Directory. – Each telephone public service shall at least once a year issue a listing directory showing therein the names of all subscribers arranged in alphabetical order, their addresses and telephone numbers and such other information as may be of interest to a subscriber's everyday use of his telephone. Each subscriber shall be entitled to a free copy of the directory.

Based on the above-cited provision, PXE as provider of telephone services to the public has authority to publish Complainant's name, address, and telephone number. The processing of Complainant's personal information, particularly, the publication of his personal information in the directory, is allowed under the rules and regulations issued for implementing the Public Service Act.

In relation to such directive, the NTC issued Memorandum Circular No. 05-06-2007 dated 08 June 2007, stating that the consumers or subscribers of telecommunication operators shall be given the option not to be listed in the publication:

Section 2.2-Any data supplied by the consumer shall be treated as confidential by the entity or service provider mentioned under Section 1.1 hereof and shall not be used for purposes not authorized by him. Upon subscription, he shall be informed of his right to privacy and the manner by which his data would be protected. In cases where a public directory listing of subscribers is regularly published by the service provider, the consumer shall be given the option not to be listed in succeeding publications.

This effectively subjected Section 149 of the Public Service Commission Rules and Regulations for all Public Services to the condition set forth by NTC Memorandum Circular No. 05-06-2007 dated 08 June 2007. While the telephone service provider has the duty to publish yearly telephone directory, it now has the correlative duty to do so in a manner that upholds the data subject's rights to data privacy.

In NPC Advisory Opinion No. 18-021, the NPC Privacy Policy Office (PPO) was sought to clarify the claim of PXE that its “base of customers whose details have been printed have not expressly provided their consent to print their details in the existing DPC White Pages that meet the standards of a valid consent as contemplated by the DPA and DPA IRR.”

Upon evaluation, the NPC-PPO opined that subscribers have the right to decide whether they want their name, address, and telephone number to be listed and included in the directory for publication. Hence, the NPC recommended the strict implementation of the said NTC Memorandum Circular.

Pieces of evidence at hand, particularly the PXE Application Form¹⁰ that was submitted by KPI on behalf of Complainant on 12 January 2016 to PXE, revealed that said form did not include an option to be excluded from the public directories published by PXE.

Without such option, the data subjects such as Complainant will not have an opportunity to give their consent to the publication of their personal information in public directories.

PXE likewise argued that the processing of personal information of Complainant is necessary and is related to the fulfillment of a contract with the data subject.

A cursory reading of the Subscription Form¹¹ and PXE’s Home DSL Terms and Conditions¹² reveal that the publication of Complainant’s personal information is not necessary nor related to the application and subsequent grant of the DSL services. On the contrary, the contract between PXE and its subscribers primarily relate to the use of the DSL services. This being the case, this

¹⁰ Records at pp. 3.

¹¹ *Id.*

¹² Records at pp. 3

Commission finds that PXE processed the personal information of Complainant in a manner not related to the fulfillment of a contract with the data subject.

Foregoing considered, PXE has neither obtained the consent of the Complainant to publish his personal information in the White Pages, nor it is otherwise authorized under the Data Privacy Act or any existing law. Hence, PXE is liable for violating Section 28 of the DPA.

*b. Unauthorized Access or
Intentional Breach*

Unauthorized Access or Intentional Breach can be committed, under Section 29 of the Data Privacy Act, by persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

The violation of this provision entails the following elements:

1. The existence of a system where personal and sensitive personal information is stored; and
2. That a person breaks in any way into the system knowingly and unlawfully, or by violating the confidentiality and security of data systems.

Here, the Complainant failed to prove that PXE or any of its agents accessed his personal information knowingly and unlawfully, or by violating the confidentiality and security of data systems. No proof was adduced showing that PXE's customer service representatives knowingly and unlawfully, or violating the confidentiality and security of data systems, broke into PXE's data storage system. Rather, the White Pages is a document that is readily available for public access.

Absent is the element of breaking into any system storing personal information. Thus, PXE cannot be found to have committed unauthorized access or intentional breach.

c. Concealment of Security Breaches Involving Sensitive Personal Information

Concealment of security breaches involving sensitive personal information can be committed, under Section 30 of the Data Privacy Act, by persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 30 (F), intentionally or by omission conceals the fact of such security breach.

For a PIC or PIP to be liable under said section, it is necessary that the breach involved sensitive personal information, or the breach refers to a nature of breach characterized by Section 20 (F) of the DPA, to wit:

(f) The personal information controller shall promptly notify the Commission and affected data subjects when **sensitive personal information** or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (but such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. (Emphasis supplied)

x x x

Records established that Complainant's name, telephone number and residential address are involved.

As to the first requirement: the breach concealed involves sensitive personal information. We note that the details disclosed in

the White Pages are not included in the enumeration of sensitive personal information¹³ explicitly provided by the DPA.

Corollary to this, there is likewise nothing in facts and circumstances will establish that the above-mentioned details will enable identify fraud against Complainant and warrants immediate notification by PXE.

This Commission would like to emphasize that name of Complainant, as published in the white pages is “KPI Philippines Inc Fao RLA” Read plainly, we find that the published name is not a direct and accurate representation of Complainant’s full name. This circumstance, coupled with the fact that only the telephone number and residential addresses were disclosed, are not sufficient to enable a third person to steal the identity of Complainant in this case.

In view of the foregoing, this Commission determines that PXE is not liable for violation of Section 30 of the Data Privacy Act.

*d. Unauthorized Disclosure of
Personal Information*

Unauthorized Disclosure of Personal is punishable under Section 32 of the DPA which provides:

SEC. 32. Unauthorized Disclosure. – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

¹³ Section 3 (l), R.A. 10173

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party **sensitive personal information** not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

Section 32 of the DPA penalizes disclosure of personal information not falling within Section 31 of the DPA or due to malicious disclosure. To be liable under Section 32, the following elements must concur:

- a. The accused is a personal information controller or personal information processor or any of its officials, employees or agents'
- b. the accused made a disclosure of information;
- c. the information relates to personal information;
- d. the accused disclosed the information to a third party;
- e. the disclosure was without the consent of the data subject.
- f. That the disclosure was not malicious or done in bad faith.

The previous discussions establish the existence of the first, second, third, fifth, and sixth elements of unauthorized disclosure of personal information. Hence, we now determine whether the fourth element is present in this case.

Upon evaluation and adjudication, this Commission rules in the positive.

It must be noted that the copies of PXE's 2017 White Page or Directory is distributed to its subscribers. All the personal

information found therein are disclosed to PXE' subscribers and to other persons who may be given a copy thereof. Persons who received a copy of said directory is considered a third party regarding the processing of Complainant's personal information. Thus, Complainant's personal information was disclosed to third parties.

With all the elements present, the Commission holds PXE liable for violating Section 32 of the DPA.

*III. Criminal Liability of PXE's
Board of Directors and Responsible
Officers*

Having established that PXE committed violations of the DPA particularly for the Processing of Personal Information for Unauthorized Purposes, and for Unauthorized Disclosure of Personal Information, this Commission now determines the criminal liability of PXE's board of directors and responsible officers.

For ready reference, we reproduce the pertinent violations of PXE as discussed above:

*SEC. 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. - The processing of personal information for unauthorized purposes shall be **penalized by imprisonment** ranging from one (1) year and six (6) months to five (5) years **and a fine** of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed **on persons processing personal information for purposes not authorized by the data subject**, or otherwise authorized under this Act or under existing laws. (Emphasis and underlining supplied)*

SEC. 32. *Unauthorized Disclosure.* – (a) **Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party** personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00). (Emphasis and underlining supplied)

Pursuant to the aforesaid, Sections 28 and 32 of the DPA impose both imprisonment and fine for persons who commit the violations, including the PICs officials, employees or agents who caused the unauthorized processing and disclosure of personal data.

At the onset, this Commission stresses that the Data Privacy Act was enacted and devised to safeguard the right to informational privacy of individuals and to ensure free flow of information.

The State Policy behind the passage of the DPA is founded on nation-building through a data resilient Philippines. It also aims to enable Philippines as an internationally competitive body by participating in international engagements and other forms of commitments involving data privacy and protection.

Corollary to this, Sections 28 and 32 of the DPA were intended to impose exacting standards in the protection of data, and the penal liabilities thereon were intended to ensure compliance.

To this extent, in case of a corporation, the law may hold the Board of Directors and Corporate Officers of the PIC as criminally liable and may receive penal sanction for violations of the DPA when it is proven that because of their gross negligence, they allowed the commission of the crime explicitly provided in the DPA.. This is explicitly provided under Section 34 of the DPA itself, which provides: It provides that:

SEC. 34. *Extent of Liability.* - If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, **who participated in, or by their gross negligence, allowed the commission of the crime.** (Emphasis supplied)

The same provision is also reflected in Section 30 of the Corporate Code of the Philippines which provides:

Section 30. *Liability of Directors, Trustees or Officers.* - Directors or trustees **who willfully and knowingly vote for or assent to patently unlawful acts of the corporation** or who are guilty of gross negligence or bad faith in directing the affairs of the corporation or acquire any personal or pecuniary interest in conflict with their duty as such directors or trustees shall be liable jointly and severally for all damages resulting therefrom suffered by the corporation, its stockholders or members and other persons. (Emphasis and underlining supplied)

In certain cases, this Commission held Corporate Board of Directors, Officials and Officers may be criminally liable for violating the provisions of the DPA where it was established that said Directors and/or officers participated in, or by their gross negligence, allowed the commission of the crime.

Corollary to the aforesaid, in the landmark case of *Ching v. Secretary of Justice*¹⁴ for criminal liability of corporations the Supreme Court explained that:

If the crime is committed by a corporation or other juridical entity, the directors, officers, employees or other officers thereof responsible for the offense shall be charged and penalized for the crime, precisely because of the nature of the crime and the penalty therefor. A corporation cannot be arrested and imprisoned; hence, cannot be penalized for a crime punishable by imprisonment. However, a corporation may be charged and prosecuted for a crime

¹⁴ Ching v. Secretary of Justice, G.R. No. 164317, [February 6, 2006], 517 PHIL 151-178

if the impossible penalty is fine. Even if the statute prescribes both fine and imprisonment as penalty, a corporation may be prosecuted and, if found guilty, may be fined.

A crime is the doing of that which the penal code forbids to be done or omitting to do what it commands. A necessary part of the definition of every crime is the designation of the author of the crime upon whom the penalty is to be inflicted. When a criminal statute designates an act of a corporation or a crime and prescribes punishment therefor, it creates a criminal offense which, otherwise, would not exist and such can be committed only by the corporation. But when a penal statute does not expressly apply to corporations, it does not create an offense for which a corporation may be punished. On the other hand, if the State, by statute, defines a crime that may be committed by a corporation but prescribes the penalty therefor to be suffered by the officers, directors, or employees of such corporation or other persons responsible for the offense, only such individuals will suffer such penalty. Corporate officers or employees, through whose act, default or omission the corporation commits a crime, are themselves individually guilty of the crime.

Since a corporation, like PXE, can only act through its Board of Directors, Corporate Officers, and employees, these DPA violations must have been committed by the Board of Directors, Corporate Officers, or employees of PXE either directly or through their gross negligence. Information necessary to identify these responsible officers / employees is usually within the control of the respondent PIC and not readily or easily available to the Complainant.

In this case, a thorough and meticulous investigation must be conducted to determine those liable officers who willfully or knowingly participated in, or by their gross negligence, allowed the commission of the crime. However, upon careful perusal of the evidence submitted and the Complaint itself, the information necessary to identify these liable officers or employees are not readily available. Thus, a further investigation is necessary.

In view of this, this Commission REMAND this case to the Complaints and Investigation Division for further investigation and

for the determination of the responsible officers of PXE, who by participation, negligence, or omission, allowed the violations of Section 28 and 32 of the DPA.

Complainant is entitled to the award of nominal damages

As established above, the Respondent processed Complainant's personal information for unauthorized purposes which resulted to unauthorized disclosure of Complainant's personal information in the White Pages without or against the consent of the Complainant.

However, this Commission notes that Complainant was not able to satisfactorily establish his loss, including the perceived threat of another abduction incident of his father. While evidence submitted by Complainant indicates that there was a previous abduction attempt against Complainant's father, it does not immediately follow that the publication in the White Pages would inevitably result in another abduction attempt. Hence, the threat may be more apparent than real.

As provided by the Supreme Court, in the case of *Arreola v. Court of Appeals*:¹⁵

Nominal damage is recoverable where a legal right is technically violated and must be vindicated against an invasion that has produced no actual present loss of any kind, or where there has been a breach of contract and no substantial injury or actual damages whatsoever have been or can be shown.

Since no present loss of any kind, substantial injury, or actual damages have been proved by Complainant, this Commission awards the nominal damages of Fifty Thousand Pesos (P50,000.00) to the Complainant.

¹⁵Areola v. Court of Appeals, G.R. No. 95641, [September 22, 1994], 306 PHIL 656-667

WHEREFORE, all these premises considered, this Commission resolves to **AWARD** Complainant, RLA, nominal damages in the amount of Fifty Thousand Pesos (P50,000.00) for Respondent PXE Enterprise's violation of Complainant's rights under the Data Privacy Act.

Moreover, this Commission resolves to **REMAND** this case to the Complaints and Investigation Division for the limited purpose of determining and identifying the responsible persons, officers, or individuals of PXE Enterprise who caused the violations of Sections 28 and 32 of the DPA prior to recommending the matter to the Secretary of Justice for criminal prosecution.

SO ORDERED.

Pasay City, Philippines;
17 December 2020

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.) (Sgd.)
LEANDRO ANGELO Y. AGUIRRE **JOHN HENRY D. NAGA**
Deputy Privacy Commissioner Deputy Privacy Commissioner

Copy furnished:

RLA

Complainant

PXE INC.

Respondent

Chief Data Privacy Officer

**COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
NATIONAL PRIVACY COMMISSION**