Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-024

4 May 2018

[redacted]

Re: REPORTING OF ALLEGED CRIMINALS' PERSONAL DATA

Dear [redacted],

This has reference to your inquiry received by the National Privacy Commission (NPC) *via e-mail.* You asked how the Data Privacy Act (DPA) of 2012 and its Implementing Rules and Regulations (IRR) affect the practice of some security agencies or establishments of reporting to the Philippine National Police (PNP) and barangay officials, criminal elements who are caught within their premises. You likewise asked if the disclosure of personal information of the alleged suspect such as his/her name, photo, or address, for apprehension purposes, as well as posting of the same in public places, would constitute a violation of the DPA.

Reporting to the police and other law enforcement agencies in relation to a criminal investigation

The practice of security agencies and establishments of reporting to the PNP or barangay officials criminal incidents which happened within their premises and personal information on an alleged criminal offender (data subject[1]), do not constitute a violation of Republic Act (R.A.) No. 10173, otherwise known as the Data Privacy Act (DPA) of 2012.

The processing[2] of personal information of a possible suspect, by reporting to police officers and/or barangay officials of proper jurisdiction, is allowed under Section 12(e) of R.A. No. 10173, specifically the following provision:

> "(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

[1] R.A. No. 10173, §3(c) - Data subject refers to an individual whose personal information is processed.
[2] *Id.*, §3(j) - Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

> functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate;"

Further, Section 13(f) of the DPA relating to lawful processing of sensitive personal information states that:

> "(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."

In reporting cases to law enforcement authorities, certain personal information[3] about the suspected perpetrator of the crime will be divulged. This may include names and photographs. This is necessary in order for the police officers to determine and verify the facts of a case, and to aid in their investigation.

In the same manner, police officers' act of gathering data is allowed in accordance with Section 24 of the Republic Act No. 6975[4], which states that the powers and functions of the PNP include, among others, to:

1. Enforce all laws and ordinances relative to the protection of lives and properties;
2. Maintain peace and order and take all necessary steps to ensure public safety;
3. Investigate and prevent crimes, effect the arrest of criminal offenders, bring offenders to justice and assist in their prosecution; and
4. Exercise the general powers to make arrest, search and seizure in accordance with the Constitution and pertinent laws.

Thus, the disclosure of personal information of suspected criminals to law enforcement officers is allowed under the DPA when it is in pursuant to its mandate to investigate and prevent crimes.

Investigation refers to the collection of facts to accomplish a three-fold aim: a. to identify the suspect; b. to locate the suspect; and c. to provide evidence of his guilt. In the performance of his duties, the investigator must seek to establish the six (6) cardinal points of investigation, namely: what specific offense has been committed; how the offense was committed; who committed it; where the offense was committed; when it was committed; and why it was committed. Taking of sworn statements of suspects and witnesses is also part of the investigation protocol.

To emphasize this further, while the DPA aims to protect personal and sensitive personal information in information and communications systems in both the government and the private sector, it should not be construed to be limiting the powers and functions of government instrumentalities, especially the law enforcement, in terms of fulfilling their mandate to promote peace and order and ensure public safety for the country.

---

[3] *Id.*, §3(g) - 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.

[4] AN ACT ESTABLISHING THE PHILIPPINE NATIONAL POLICE UNDER A REORGANIZED DEPARTMENT OF THE INTERIOR AND LOCAL GOVERNMENT, AND FOR OTHER PURPOSES

Posting of name and photo relating to suspects of a crime in public places

General considerations on the posting of personal data of suspects in public places should include the balancing of the rights of the data subject vis-à-vis those of the general public.[5]

According to the DPA, the processing of personal information shall only be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.[6]

The public posting of personal information may be allowed in certain instances, i.e. wanted suspects, those who escaped custody, etc.[7] Note that other means of tracing the location of the person should have first been tried where practical.[8]

We note also the common practice of some establishments of posting photos of suspected shoplifters. The Office of Personal Data Protection (OPDP) in Macau have demanded that the same be stopped, reasoning that although it is legal for establishments to install surveillance systems in their premises for security purposes, the image data derived therefrom may not be processed or used for something other than said security purpose. This would exclude the public posting of images of suspected shoplifters and labelling them as such.[9] If video data indicates shoplifting, it should have been referred to the police.[10]

In the Philippines, the use of surveillance systems is likewise considered processing of personal data, and must therefore comply with the requirements of the DPA. These surveillance mechanisms are commonly utilized by establishments for legitimate security purposes, and may have proper basis for lawful processing under the DPA[11] which do not require consent of the data subjects.

However, based on the given circumstances, those establishments engaged in public announcements of an alleged suspect's personal information, are processing in a manner that is unauthorized by the DPA. Such public disclosure of personal data, in particular the alleged suspect's photo, whether derived from the establishment's surveillance footages or acquired elsewhere, may constitute a violation of the provisions of the same law (e.g., rights of the data subjects[12]).

---

[5] Association of Chief Police Officer of England, Wales & Northern Ireland, GUIDANCE ON THE RELEASE OF IMAGES OF SUSPECTS AND DEFENDANTS, May 2009, available at http://library.college.police.uk/docs/acpo/ACPO-Guidance-Release-Images-Suspects-Media.pdf
[6] *RA No. 10173*, §11.
[7] Supra note 5.
[8] Id.
[9] Greenleaf, Graham. Asian Data Privacy Laws: Trade and Human Rights Perspectives. 2014. Available at https://books.google.com.ph/books?id=0eAuBQAAQBAJ&pg=PA277&lpg=PA277&dq=posting+of+alleged+suspects+%2B+pictures+%2B+public+disclosure&source=bl&ots=48_oDNQSAr&sig=mdTtvxwjdamUeUi1_5e8bdSG3vk&hl=en&sa=X&ved=0ahUKEwjn3quG7-DZAhUIvLwKHb2XCRUQ6AEIWDAE#v=onepage&q=posting%20of%20alleged%20suspects%20%2B%20pictures%20%2B%20public%20disclosure&f=false
[10] Id.
[11] See: R.A. No. 10173, §12-13.
[12] See: R.A. No. 10173, §16-19; Implementing Rules and Regulations (IRR) of R.A. No. 10173, §34-37.

In addition, any processing of personal information must be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.[13] We emphasize that such activity already deviates from the original purpose which is to ensure that the premises are secured and protected. By publicly posting the information of a possible suspect, the purpose becomes an intentional association of the person to the crime for the public's scrutiny, instead of leaving the matter to the police.

Furthermore, the said posting violates the principle of proportionality for being an unnecessary and excessive processing of personal data.[14] Processing could only be allowed if there are no other means to fulfill a legitimate purpose, which is clearly not the case.[15]

These establishments, as personal information controllers (PIC)[16], are also obliged by the DPA to implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.[17]

Ultimately, in any processing of personal data, it is reminded that PICs give due respect to the fundamental rights, and freedoms of the data subjects which require protection under the Philippine Constitution.

The opinion provided herein is based on the limited information provided and is not intended to address other issues which are not subject of the inquiry.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

---

[13] IRR of R.A. No. 10173, §18(b).
[14] Id., §18(c).
[15] Ibid.
[16] R.A. No. 10173, §3(h) - Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.
[17] See: R.A. No. 10173, §20; IRR of R.A. No. 10173, §25-29.