



Republic of the Philippines  
NATIONAL PRIVACY COMMISSION

**PRIVACY POLICY OFFICE  
ADVISORY OPINION NO. 2017-65**

30 October 2017



**Re: CHILD ONLINE PROTECTION (COP) AND GOVERNMENT  
ACCESS TO SUSPECT'S MEDIA ACCOUNTS AND E-MAIL**

Dear ,

This pertains to your query received by the National Privacy Commission (NPC) on 18 October 2016, via email, regarding Child Online Protection (COP) vis-à-vis the Data Privacy Act of 2012 (DPA), particularly the latter's provision/s relating to law enforcement activities. You inquired regarding the following:

1. Whether the suspect's email and/or social media accounts can be opened by the government;
2. Whether the NPC can require such action; and
3. How the NPC participates in the government's initiative in COP.

In your email, you reiterated what Deputy Commissioner Patdu mentioned during the COP conference: "Online child abuse, exploitation and child pornography are not protected activities, and are recognized limitations on freedom of expression and right to privacy. Under the Data Privacy Act, law enforcement activities will not be unduly restricted, subject to requirements of due process. Existing laws safeguard the privacy of victims of child abuse and impose obligations on different sectors to cooperate in law enforcement investigations." Indeed, materials on child abuse, exploitation and child pornography are outside the protection of the free speech and expression clause. In *Eliseo F. Soriano vs. Ma. Consoliza P. Laguardia, et. al.* and *Eliseo F. Soriano vs. Movie and Television Review and Classification Board, et. al.*<sup>1</sup>, the Supreme Court ruled that:

"xxxThe freedom of expression, as with the other freedoms encased in the Bill of Rights, is, however, not absolute. It may be regulated to some extent to serve important public interests, some forms of speech not being protected. As has been held, the limits of the freedom of expression are reached when the expression touches upon matters of essentially private

---

<sup>1</sup> G.R. No. 164785 and G.R. No. 165636, 29 April 2009.

concern. In the oft-quoted expression of Justice Holmes, the constitutional guarantee obviously was not intended to give immunity for every possible use of language. From *Lucas v. Royo* comes this line: [T]he freedom to express ones sentiments and belief does not grant one the license to vilify in public the honor and integrity of another. Any sentiments must be expressed within the proper forum and with proper regard for the rights of others.

Indeed, as noted in *Chaplinsky v. State of New Hampshire*, there are certain well-defined and narrowly limited classes of speech that are harmful, the prevention and punishment of which has never been thought to raise any Constitutional problems. In net effect, some forms of speech are not protected by the Constitution, meaning that restrictions on unprotected speech may be decreed without running afoul of the freedom of speech clause. A speech would fall under the unprotected type if the utterances involved are no essential part of any exposition of ideas, and are of such slight social value as a step of truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality. Being of little or no value, there is, in dealing with or regulating them, no imperative call for the application of the clear and present danger rule or the balancing-of-interest test, they being essentially modes of weighing competing values, or, with like effect, determining which of the clashing interests should be advanced.”<sup>2</sup>

Drawing from the ruling above, it is evident that although each and every citizen is granted the freedom to express his opinion through any available means- print, television or electronic media, such right is not absolute and is limited by considerations such as public interest, subject matter or content of the material, relevance and appropriateness of sentiments and public order and morality.<sup>3</sup> Thus, materials on child abuse, exploitation and child pornography are outside the ambit of protection and recognition given to materials containing relevant subjects with values, social and public importance.

*Whether or not the email and/or social media accounts of suspects can be opened by the government; whether the NPC can require such action*

In the absence of any regulation, lawful order and state interest, for all other circumstances wherein citizens have proven to have a reasonable expectation of privacy, the right to privacy is a right protected by the guarantee against unreasonable searches and seizures provided in Article III of the 1987 Constitution stating that citizens have the right to be secure in their persons, houses, papers and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable.<sup>4</sup> The 1987 Philippine Constitution also provides, in Article 3, Section 3(1) that “the *privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.*”

---

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> *Supra* note 9.

Sections 9 and 11 of the Anti-Child Pornography Act<sup>5</sup> clearly states the duty of Internet Service Providers and Internet Content Host to notify the Philippine National Police of the National Bureau of Investigation the facts and circumstances relating to a suspected incident of child pornography, and preserve such evidence, *to wit*:

Section 9. Duties of an Internet Service Provider (ISP) - All internet service providers (ISPs) shall notify the Philippine National Policy (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of such person: Provided, That no ISP shall be held civilly liable for damage on account of any notice given in good faith in compliance with this section.

Furthermore, an ISP shall preserve such evidence for purpose of investigation and prosecution by relevant authorities.

An ISP shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography.

xx

x

xx

**Section 11. Duties of an Internet Content Host.** - An internet content host shall:

- (a) Not host any form of child pornography on its internet address;
- (b) Within seven (7) days, report the presence of any form of child pornography, as well as the particulars of the person maintaining, hosting, distributing or in any manner contributing to such internet address, to the proper authorities; and
- (c) Preserve such evidence for purposes of investigation and prosecution by relevant authorities.

An internet content host shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address that contains any form of child pornography.

An internet content host who shall knowingly, willfully and intentionally violate this provision shall be subject to the penalty provided under Section 15(j) of this Act: Provided, That the failure of the internet content host to remove any form of child pornography within forty-eight (48) hours from receiving the notice that any form of child pornography is hitting its server shall be conclusive evidence of willful and intentional violation thereof. (Emphasis and underscoring supplied).

It can be noted that nowhere in the provisions above allow for the access or opening of a suspected offender's e-mail and/or social media accounts. The government, through the law enforcement agencies is only directed to obtain certain information relevant to the investigation and further prosecution of offenders. Based on the foregoing, just like any other document, personal writing or material, social media platforms deserve the same amount of protection because it is indeed still a form of communication, only online. Therefore, the law

---

<sup>5</sup> AN ACT DEFINING THE CRIME OF CHILD PORNOGRAPHY, PRESCRIBING PENALTIES THEREFOR AND FOR OTHER PURPOSES, (17 NOVEMBER 2009).

enforcers cannot compel such access to emails and/or social media accounts of suspects without due process and without a lawful order from the court.

In relation to the provision of the DPA on law enforcement, Section 4 of the law and Section 5 of the IRR exempt specific types or classes of information from its scope. In particular, paragraph (d) of the latter states:

“Section 5. Special Cases. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned: xxx

d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act, Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act, and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA); xxx

Provided, that the non--applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.” (underscoring supplied).

Only specific information necessary to fulfill the mandate of the public authority concerned shall be considered exempt from the coverage of the law and its IRR. Personal information controllers or processors remain subject to the provisions of the law, especially those concerning the implementation of security measures for the purpose of data protection.

Primarily, it is important to determine whether the information to be gathered or collected by the law enforcement agencies involve personal data. It must be remembered that the jurisdiction of the NPC is on personal data. The NPC cannot require law enforcement agencies to execute unauthorized opening of social media and/or email accounts of suspected offenders. The NPC may initiate its own investigation on matters that fall within its jurisdiction, but will also be subject to limitations of the Constitution.

#### *Participation by the NPC in the COP*

The COP is a global initiative aimed at protecting children from all potential risks in cyberspace and providing them with ample resources that respond to their needs directly or through agents.<sup>6</sup> Far from dealing solely with child pornography, it actually seeks to address every possible violation committed against and/or that inflict damage against children online (i.e., sexual, mental, physical, psychological, and emotional). This necessarily involves the enactment and implementation of multiple policies in any given jurisdiction. In the Philippines, such policies, among others, include Republic Act No. 9975, otherwise known as the Anti-Child Pornography Act (ACPA), which law promotes and protects the general well-

---

<sup>6</sup> New Guidelines for Industry on Protecting Children Online, (05 September 2014), accessed on 28 March 2017, available at [https://www.unicef.org/media/media\\_75637.html](https://www.unicef.org/media/media_75637.html)

being of the youth, while penalizing specific prohibited acts, providing for the care of victims, rehabilitation services, and the conduct of awareness campaigns, and Republic Act No. 9262, or the Anti-Violence Against Women and their Children Act of 2004 (AVAWC), which protects women and their children against any form of violence.

At present, the participation of the NPC in the Philippine government's COP initiatives lies in the campaign to combat the issue via policy coordination. The Commission ensures that guidelines, rules, and regulations that are formulated to meet COP objectives are not only effective, but also cognizant of the rights and interests of all parties—including suspected offenders. For this purpose, the NPC participates in various group discussions and consultations on the subject between and among law enforcement agencies, other government agencies, the private sector, and civil society. The NPC is looking forward to working with other sectors, agencies and non-government organizations in promoting the rights of the child and is fully supportive in all other COP programs.

For your reference.

Sincerely,

**(Sgd.) RAYMUND ENRIQUEZ LIBORO**  
Privacy Commissioner and Chairman