Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-090[1]

28 November 2018

[redacted]

Re: DATA PRIVACY AND OFFICE-ISSUED MOBILE DEVICES

Dear [redacted],

We write in response to your inquiry regarding the use of office-issued mobile devices in relation to the Data Privacy Act of 2012[2] (DPA). In particular, you are asking whether the access of your employer to your personal iCloud account using an office-issued mobile device would be in violation of your rights to data privacy or constitute any of the offenses punishable under the DPA.

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.

Reasonable expectation of privacy

The Supreme Court in *Ople v. Torres*[3] recognized the zones of privacy protected in our laws, based on the Civil Code provision which provides that every person shall respect the dignity, personality, privacy, and peace of mind of his neighbors and other persons. It also punishes as actionable torts several acts by a person of meddling and prying into the privacy of another.[4] Likewise, it recognized the privacy of communication and correspondence and

[1] Tags: Reasonable expectation of privacy; employment; office-issued mobile device; unauthorized processing
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission and for other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] GR No. 127685, July 23, 1998.
[4] Civil Code of the Philippines, Article 26.

holds a public officer or employee, or any private individual liable for damages for any violation of the rights and liberties of another person.[5]

The ruling in *Ople v. Torres* also expounded on the "reasonable expectation of privacy" test in ascertaining whether there is a violation of the right to privacy. This test determines whether a person has a reasonable or objective expectation of privacy and whether the expectation has been violated. The reasonableness of a person's expectation of privacy depends on a two-part test:

(1) whether by his conduct, the individual has exhibited an expectation of privacy; and
(2) whether this expectation is one that society recognizes as reasonable.

The factual circumstances of the case determine the reasonableness of the expectation. Similarly, customs, community norms, and practices may, therefore, limit or extend an individual's reasonable expectation of privacy. The reasonableness of a person's expectation of privacy must then be determined on a case-to-case basis.[6]

Expectation of privacy in the employment context

It is noteworthy to mention that the reasonable expectation test was used at a time when the there were no laws on data protection and informational privacy.

Likewise, courts have generally held that employees have a decreased expectation of privacy with respect to work devices, email accounts, and internet surfing activities.[7] The same may be said for the contents therein, since there is an assumption that its use will be limited to work-related purposes.

Yet, with the DPA now in place, the reasonable expectation test should be revisited and interpreted in the context of the law.

By virtue of a legislation on data protection and privacy, the assumption is that individuals now have an expectation of privacy. As to the second element, data privacy is now more than a reasonable expectation – it is now enshrined in the DPA.[8] The reasonable expectation of privacy test then should take into consideration the standards provided under the DPA.

This means that employees must be aware of the nature, purpose, and extent of the processing of his or her personal data in the workplace. The processing of personal information of employees shall also be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Lastly, the processing of such information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[9]

Considering this, companies should revisit policies on the use of electronic communication devices, taking into consideration the DPA, especially data privacy principles and data subjects' rights. This translates to clear and well-defined policies and practices as to the extent of monitoring, degree of intrusion, consequence to employees, and procedural guarantees against arbitrariness.

---

[5] *Id*. Article 32.
[6] *Id.*
[7] See: Pollo v. David, G.R. No. 181881, (2011); O'Connor v. Ortega 480 U.S. 709 (1987).
[8] Data Privacy Act of 2012, § 2.
[9] *Id.* § 11.

Expectation of privacy in personal iCloud account; unauthorized processing

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.[10] 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.*,[11] 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.

In *Copland v. the United Kingdom*,[12] 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[13] 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.

The alleged use of your account to pry and investigate on other employees and the improper order from the management to not log out your account have put you on guard and secure your personal iCloud account.

Hence, the act of the HR employee of accessing your personal iCloud account without your consent may constitute violation of your privacy. Furthermore, such unauthorized access into may constitute unauthorized processing under the DPA. The elements of the offense are as follows:

1. the accused processed the information of the data subject;
2. that the information processed was personal information;
3. that the processing was done without the consent of the data subject, or without authority under this Act or any existing law.

An iCloud account is considered as personal information under the law.[14] As stated in your

[10] Article 29 Working Party, Opinion 2/2017 on data processing at work (2017).
[11] 201 N.J. 300, 990 A.2d. 650 (2010)
[12] ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007.
[13] ECtHR, *Barbulescu v. Romania* [GC], No. 61496/08, 5 September 2017.
[14] Data Privacy Act of 2012, § 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.

email, your personal iCloud was accessed without your express authorization and you were forced to log back in even after resignation. The act of the employer of accessing your iCloud account without your knowledge and consent, and without authority under the law may be unauthorized processing of personal information.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

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