

NINETEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)



23 APR 24 A11 :34

RECEIVED BY: _____

SENATE

P.S. RES. NO. 574

Introduced by **Senator Francis "Tol" N. Tolentino**

RESOLUTION

DIRECTING THE APPROPRIATE SENATE COMMITTEE TO CONDUCT AN INQUIRY, IN AID OF LEGISLATION, INTO THE UNPRECEDENTED MASSIVE PERSONAL DATA BREACH OF THE DATABASES OF THE NATIONAL BUREAU OF INVESTIGATION (NBI), PHILIPPINE NATIONAL POLICE (PNP), AND OTHER AGENCIES, WHICH LEAKED MORE THAN ONE MILLION PERSONAL AND SENSITIVE RECORDS OF LAW ENFORCERS AND PRIVATE CITIZENS IN VIOLATION OF DATA PRIVACY, CYBERCRIME, AND OTHER LAWS.

Whereas, the State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;¹

Whereas, in *Spouses Hing vs Choachuy*, the Supreme Court declared that "[t]he right to privacy is enshrined in our Constitution and in our laws. It is defined as "the right to be free from unwarranted exploitation of one's person or from intrusion into one's private activities in such a way as to cause humiliation to a person's ordinary sensibilities." It is the right of an individual "to be free from unwarranted publicity, or to

¹ Section 2 of RA No. 10173 or the Data Privacy Act of 2012

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 let alone.";²

Whereas, on 19 April 2023, the Philippines was shocked by the news of an unprecedented data breach which exposed a massive amount of records from multiple government databases which includes the National Bureau of Investigation (NBI), Philippine National Police (PNP), Bureau of Internal Revenue (BIR), and the Special Action Force (SAF);³

Whereas, VPNMentor, an independent site which reviews VPN services and covers privacy-related stories, published an online report from their researcher, Jeremiah Fowler, that the said data breach comprised of the following:

- a. Total size: **817.54 gigabytes**
- b. Total number of records exposed: **1,279,437**
- c. **Employee and Applicant Identification Records:** Scanned and photographed images of original documents that included: birth certificates, educational record transcripts, diplomas, tax filing records, passport and police identification cards. Included in the files were combined records certifying that there are no pending cases or criminal history for the officer. These included Republic of the Philippines Justice Department's certification, local or regional court records, and the National Bureau of Investigation (NBI) identification and clearance documents;

Whereas, under the **Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012"**, "PERSONAL DATA BREACH" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;"⁴

Whereas, no less than the source of the data breach report, Mr. Fowler, noted some very disturbing developments⁵ prior to the publication of his findings, to wit:

- a. **He discovered the unprotected PNP database in mid-January and promptly informed the authorities of its exposure;**

² G.R. No. 179736, June 26, 2013

³ [Over 1M records from NBI, PNP, other agencies leaked in massive data breach | Inquirer News](#)

⁴ <https://www.officialgazette.gov.ph/images/uploads/20160825-IRR-RA-10173-data-privacy.pdf>

⁵ <https://newsinfo.inquirer.net/1758689/for-weeks-pnp-staff-database-was-exposed-cyber-expert>

- b. **It was not until the second week of March (2023) when action was taken and public access to the database was removed;**
- c. By then, the database had been exposed for at least six weeks, although he said it was unclear exactly how long the database had been accessible or if anyone else might have gained access to it;
- d. And that upon discovering the database he sent over 15 “**responsible disclosure** notices⁶ over several weeks” to multiple Philippine government agencies;

Whereas, the same cybersecurity researcher, Mr. Fowler, unfortunately has concluded that **there most certainly was a breach and all of the records were related to individuals in law enforcement**, and that these should have not been exposed or accessible without password protection⁷;

Whereas, according to the prominent IT and cybersecurity firm, IBM Security, in their *Cost of a Data Breach Report 2022*, the average cost of a data breach for an ASEAN country like the Philippines⁸ is upwards of 157 million pesos (\$2.87 million), however, this would definitely entail incalculable loss largely to the individuals whose **sensitive personal information**⁹ and official documents have been compromised, not to mention the legal, financial, reputational, and operational ramifications of the this data breach to the government agencies concerned;

Whereas, the sale of these breached data is a very lucrative industry in the blackmarket, thus we can most probably expect a good number of identity theft and fraudulent claims cases as a result of this incident. Unfortunately, we cannot yet determine the actual extent of the damage since what we just know now is that only the data of law enforcement members have been breached. We are not sure yet if even the data of the general public has likewise been compromised;

Whereas, this alleged breach should be seriously investigated and urgently addressed by the agencies concerned as it not only compromised the personal information of the people included in the data breach but also undermines the

⁶ Under a **responsible disclosure** protocol, cybersecurity researchers tell the system providers about the vulnerability and provide the latter with reasonable timelines to investigate and fix them. Then, they publicly disclose vulnerabilities once they have been patched (remediated).

⁷ <https://newsinfo.inquirer.net/1758689/for-weeks-pnp-staff-database-was-exposed-cyber-expert>

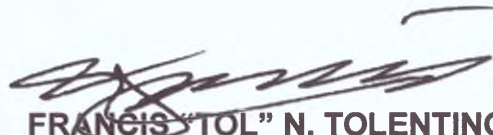
⁸ <https://www.ibm.com/downloads/cas/3R8N1DZJ>.

⁹ As defined by Sec. 3(l) of Republic Act No. 10173, also known as the “Data Privacy Act of 2012”.

confidentiality, sanctity and security of the data collected by these agencies. Worse, the said breached might even compromise the country's national security; **Now, therefore,**

Be it resolved, as it is hereby resolved, to direct as it hereby directs the appropriate Senate Committee to conduct an inquiry in aid of legislation, into the unprecedented massive personal data breach of the databases of the National Bureau of Investigation (NBI), Philippine National Police (PNP), and other agencies, which leaked more than one million sensitive personal records and official documents of law enforcers and private citizens in violation of data privacy, cybercrime and other laws.

Adopted,


FRANCIS "TOL" N. TOLENTINO
Senator 