CO-ME-LEAK:
The Biggest Data Privacy Violation in Our Time

Dawna Bandiola and Lorenzo Delgado

The 1987 Constitution[1] provides the powers and functions of the COMELEC, one of which is the enforcement and administration of all laws and regulations relative to the conduct of election, plebiscite, initiative, and referendum. During the election hype, there was a COMELEC Leak exposing voters' information to the public. Personal data of up to approximately 70 million registered voters in the Philippines was compromised[2] but despite this, the COMELEC through their spokeperson, merely shrugged it off saying that *"There is no sensitive information there."*[3]

Under Section 3 (l) of the Data Privacy Act the term "Sensitive personal information" refers to the following personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.

Contrary to the COMELEC's claim however, a hacker group called LulzSec Pilipinas4 claims to have hacked comelec.ph and that they have dumped the database of about 70 million of Filipino voters and have published all the data at archive.org. According to them, the database contains a lot of sensitive information, such as the voter's sex, civil status, year of birth, month of birth, day of birth, birth province, birth city, resident province, resident city, resident barangay, street, precinct, precinct code, fingerprint data and passport information. They also made a search engine over that sensitive data, all for the sake of "lulz" causing a massive breach of data privacy in our country, which shows that the COMELEC was correct in saying that there is no sensitive information there. They are not sensitive data, rather they are ultra-sensitive. And it is not just the voters' information which is vulnerable, they recently leaked the Certificate of Candidacy of 12 Senators.[5]

---

[1] Const. (1987), Article IX Sec. 2

[2] Retrieved from http://manila.coconuts.co/2016/04/21/hackers-group-search-engine-presents-leaked-filipino-voters-data

[3] Retrieved from https://blog.malwarebytes.com/cybercrime/2016/04/comelec-breach-data-released-online-fully-searchable/

[4] Lulzsec Pilipinas is a local version of the hacking group lulzsec International who was responsible of several high profiled attacks years ago

[5] Retrieved from https://www.pinoyhacknews.com/lulzsec-pilipinas-strikes

[6]

An internet and ICT rights advocate organization[7] posted tips to help protect the Filipinos from identity theft, due to the leak exposing their pertinent personal information. The voters' information stolen from the COMELEC can be used in a million different ways by unscrupulous marketers, politicians, and criminals to the prejudice of the public in general such that, it may lead to identity theft, flying voters, and manipulation of the election results.

Due to the vast evolution of technology, COMELEC has been facing these situations that would challenge its competency and transparency as a constitutional electoral body. One such situation is data hacking. It is defined as the gaining of access, whether wanted or unwanted, to a computer and viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer.[8]

Now the very issue that comes to mind is that: whether or not the COMELEC is at fault. Is the COMELEC responsible for the leak? Can they be held liable?

The COMELEC, in our opinion, is responsible based on the following reasons:

First, the law expressly mandates that it is its duty to preserve the sanctity of every voter's information. *Absoluta sentential expositore non indiget*, when the language of the law is clear, no explanation of it is required.[9] Failure to comply with its duties raises a prima facie presumption that the COMELEC is remiss in the performance of these duties. Section 20 of the Data Privacy Act provides the following:

> SEC. 20. Security of Personal Information. – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.
> (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

Section 21 thereof states that each personal information control is responsible for the personal information which it has in its possession:

> SEC. 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for

[6] Retrieved from https://www.pinoyhacknews.com/lulzsec-pilipinas-strikes

[7] Retrieved from Democracy.Net.PH

[8] Data Hacking, available at http://www.urbandictionary.com/define.php (last visited November 30, 2016)

[9] Augustus Caezar Gan vs Hon. Antonio Reyes, G.R. No. 145527 May 28, 2002

> processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

Second, common sense dictates that when something wrong happens nvolving the rights of another, (in this case the voters) the person who has knowledge of such violation (the COMELEC) should immediately notify or disclose it to the person or persons whose rights were violated. In fact Section 20 (f) of the Data Privacy Act provides that:

> (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. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. xxx

Instead of warning the public as to the unfortunate incident and the prejudicial effects of the hacking incident, instead of telling them what to do and how to protect their privacy and personal information which were supplied to them, confident that they would safeguard it, instead of being honest to the public, they chose to disregard the existence of the issue claiming that there is no sensitive information leaked, contrary not only to the said law, but also to the policy of the State in promoting a high standard of ethics in public service. It is an elementary rule in law that public officials and employees shall at all times be accountable to the people and shall discharge their duties with utmost responsibility, integrity, competence, and loyalty.

Third, in failing to report the hacking incident to the National Privacy Commission, the COMELEC did not discharge its duties with utmost responsibility, integrity, competence and loyalty. In claiming that there was no sensitive information involved, COMELEC did not act with utmost responsibility which manifest that they chose to uphold their own personal interest over that of the public by avoiding hacking incident rather than recognizing it and assuming responsibility thereof. In our opinion they violated the norms of conduct of public officials as provided in R.A. 6713 known as the Code of Conduct and Ethical Standards for Public Officials and Employees. Under Section 4 A (e) of the said law the COMELEC should have been responsive to the public. The Commission is duty bound to extend prompt, courteous, and adequate service to the public, and to provide information and to ensure its openness of information. The Data Privacy Act imposed duties on data controllers and protects the rights of data subjects. Under Rule VII Section 30 of the Implementing Rules, it provides that:

> **Section 30. Responsibility of Heads of Agencies.** All sensitive personal information maintained by the government, its agencies, and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, subject to these Rules and other issuances of the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein. The Commission shall monitor government agency compliance and may recommend the necessary action in order to satisfy the minimum standards

Since the data which was maintained by the COMELEC were sensitive personal information, and since the law expressly provides for their responsibility with respect to such

information they are clearly responsible. They have a duty to report the incident to the National Privacy Commission, and the data subjects clearly have the right to be informed[10] of what has transpired, which is related to their data information, and in connection to this the data subject also have the right to be indemnified for any damages sustained due to the unlawfully obtained or unauthorized use of their personal data, taking into account any violation of their rights and freedoms as data subjects.

However, responsibility is not automatically tantamount to liability. In Vinuya v. Romulo, the Supreme Court held that "the question whether the Philippine government should espouse claims of its nationals against a foreign government is a foreign relations matter, the authority for which is demonstrably committed by our Constitution not to the courts but to the political branches."11 Immunity then, unlike in other jurisdictions, is determined not by the courts of law but by the executive branches. Thus, even if the court finds that the COMELEC is responsible for the data leak, the executive branches could easily defeat the claim by invoking the royal prerogative of dishonesty, and conveniently hide under the State's cloak of invincibility against suit.

Conclusion

The only solution is to aim and focus on the improvement of security codes used in safeguarding the voters' records. The COMELEC must be proactive, rather than reactive. However, the Commission cannot do it alone since not all key officials of COMELEC are tech-savvy. The commission must seek assistance and coordinate with Information and Communication Technology (ICT) experts in order to address the current situation. It cannot be denied that data hacking, a form of cybercrime, is now prevalent. But still, it is avoidable. As a Constitutional commission, COMELEC should bear the consequences of all matters falling within its authority and must endeavor to resolve all matters that would threaten its competency and credibility. It must be able to take into consideration all factors that would help improve the performance of its functions to ensure the people of a clean election.

[10] R.A. No. 10173, Section 16

[11] G.R. No. 162230, April 28, 2010.