REVISITING THE BREACH

A BRIEFING PAPER ON THE 2016 COMELEC DATA LEAK

Jamael Jacob
Jessamine Pacis

FOUNDATION FOR MEDIA ALTERNATIVES (2018)

ABOUT FMA

The Foundation for Media Alternatives (FMA) is a non-profit service institution whose mission is to assist citizens and communities—especially civil society organizations (CSOs) and other development stakeholders—in their strategic and appropriate use of the various information and communications media for democratization and popular empowerment.

Since its formation in 1987, FMA has sought to enhance the popularization and social marketing of development-oriented issues and campaigns through media-related interventions, social communication projects and cultural work. In 1996, FMA streamlined its programs and services in both traditional and new media, with a major focus on information and communications technologies (ICTs), to enable communities to assert their communication rights and defend their rights to information and access to knowledge, towards progressive social transformation.

FMA seeks to develop programs and projects that strategically address the questions of access to and equity of disadvantaged sectors in the area of information and communications – and in locating the so-called digital divide within existing socio-political divides, including gender. These involve:

- Promoting equitable partnerships for innovating connectivity and community access alternatives to assert the agenda of disadvantaged communities;
- Facilitating capacity-building sessions for CSOs in the area of ICT literacy, ICT management, online collaboration or advocacy, and secure online communications;
- Helping CSOs manage development content through appropriate tools and technologies towards building vibrant online communities and knowledge networks; and
- Enhancing multi-stakeholder consensus-building on strategic information and communication agendas, via action-oriented research, constituency-building and public advocacy.

What Happened

On 27 March 2016, news[1] broke out that two (2) groups—*Anonymous Philippines* and *LulzSec Pilipinas*—had hacked the website of the Commission on Elections (Comelec), the government agency charged with the administration and enforcement of the Philippines's election policies.[2] Between them, the attack orchestrated by *LulzSec* was regarded as more serious and had greater potential to cause damage, being the country's first major leak involving government-held personal data.[3]

Through their *Facebook* account, *LulzSec* owned up to having illegally accessed and downloaded 340GB worth of data from the *Comelec* database. Apparently, the hack involved personal information belonging to 55 million registered Filipino voters.[4]

The following day, just before midnight, *LulzSec* released their stolen cache of data online. The group put up three mirror links,[5] thereby ensuring maximum accessibility.[6] In a post, the group claimed that while some of the data were encrypted, they had the algorithms necessary to crack the code.[7]

Before long, the incident was picked up by the media and concerns about its potential harm grew. This prompted *Comelec* spokesperson James Jimenez to release a statement downplaying the impact of the leak. He claimed that the compromised database was accessible to the public anyway,[8] and that, more importantly, no sensitive personal information were involved. According to Jimenez, the hackers only managed to secure a list of names and addresses, and nothing more; the possibility that the leaked information could be used for identity theft was remote, if not unlikely.[9] His statement was echoed by then- *Comelec* chairman, Andres Bautista.[10]

About a week later, on April 6, cybersecurity firm *Trend Micro* published a blog post describing the leak as possibly "one of the biggest government-related data breaches in history," and compared it to 2015's hacking of the Office of Personnel Management in the United States, which led to the disclosure of personal information belonging to approximately 20 million U.S. citizens.

The *Comelec* was quick to challenge *Trend Micro*'s exposé, and insisted that the firm (and other researchers who claimed to have investigated the breach) could not have made a proper assessment

---

[1] It is worth nothing, however, that Jonel De Asis, the second hacker arrested in relation to this incident, supposedly admitted in an interview that he had already penetrated the Comelec website and accessed its database prior to March 27. See: *Hacker who allegedly leaked Comelec data now in NBI custody*, CNN Philippines Staff, April 29, 2016.
Source: http://cnnphilippines.com/news/2016/04/29/Comelec-hacker-data-leak.html.

[2] *Comelec: No biometrics data leaked after hack*, Levi A. So, April 12, 2016.
Source: http://www.philstar.com/headlines/2016/04/12/1572140/comelec-says-no-biometrics-data-leaked-after-hack.

[3] *Comelec data leaked by hackers*, Rappler.com, March 28, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/127315-comelec-data-hackers

[4] *Comelec hacking threatens security of voters: Trend Micro*, Jojo Malig, April 7, 2016.
Source: http://news.abs-cbn.com/halalan2016/focus/04/07/16/comelec-hacking-threatens-security-of-voters-trend-micro

[5] *Comelec data leaked by hackers*, Rappler.com, March 28, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/127315-comelec-data-hackers

[6] *Comelec: No biometrics data leaked after hack*, Levi A. So, April 12, 2016.
Source: http://www.philstar.com/headlines/2016/04/12/1572140/comelec-says-no-biometrics-data-leaked-after-hack.
See also: *Philippines elections hack 'leaks voter data'*, Leisha Chi, April 11, 2016.
Source: http://www.bbc.com/news/technology-36013713

[7] *Comelec data leaked by hackers*, Rappler.com, March 28, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/127315-comelec-data-hackers

[8] *Comelec: No biometrics in leaked data*, JC Gotinga, April 12, 2016.
Source: http://cnnphilippines.com/news/2016/04/12/Comelec-No-biometrics-in-leaked-data-hack.html

[9] Jimenez also downplayed the idea of using the data in the leaked files to commit identity theft. "[They] have a list of names and addresses. That's pretty much it. I think it's going to be more complicated than that, when creating a bank account, for instance."

[10] *Comelec hacking threatens security of voters: Trend Micro*, Jojo Malig, April 7, 2016.
Source: http://news.abs-cbn.com/halalan2016/focus/04/07/16/comelec-hacking-threatens-security-of-voters-trend-micro

since it had no access to the Commission's actual database.[11] The Commission insisted anew that no sensitive data (i.e., biometrics) were included in the compromised database.[12]

Around that time, the National Bureau of Investigation (NBI), which had been called in to work on the case,[13] claimed that they already had good leads. In a press conference, NBI Cybercrime Division Chief Ronald Aguto, Jr., explained that agents were already tracking a couple of suspects after having successfully identified the IP addresses used in the attacks, and through traditional human intelligence.[14] He emphasized that the Bureau was coordinating with other law enforcement agencies, including their foreign counterparts,[15] and that arrests were likely to be made in the next coming days leading to the filing of appropriate charges against the perpetrators.[16]

Meanwhile, the recently appointed[17] National Privacy Commission (NPC) officials, who had been following the case closely, requested from *Comelec* a report on the incident.

On 14 April 2016, IT security expert and blogger Troy Hunt released a detailed analysis of the breach, including an account of how he managed to verify some of the leaked information using his online platform, "*Have I been pwned*". By reaching out to people whose emails were included in the database, he was able to confirm the authenticity and accuracy of at least a portion of the leaked data. It turned out that the leaked data included information on the height, weight, names of parents, and passport numbers of certain individuals.[18] Hunt's report effectively challenged the *Comelec*'s earlier claim that no sensitive information were accessed via the leak.

Nearly a week later, on April 19, the worst-case scenario envisioned by some observers was realized: a website containing the compromised data was launched. It featured a search engine functionality that provided a quick and easy way to rummage through the personal information of all Filipino registered voters affected by the breach. Following the public's panicked reactions to the website, *Comelec* spokesperson Jimenez apologized for what he referred to as a "continuing attack on [voters'] privacy," and assured the public that the Commission was doing everything to resolve the situation as quickly as possible.[19] He explained that the Commission was willing to sanction its own people for having allowed such "unprecedented breach of online security"[20] [21]. He added that measures had already been set in motion, such as reassigning the people maintaining the agency website to

---

[11] *Comelec: No biometrics in leaked data*, JC Gotinga, April 12, 2016.
Source: http://cnnphilippines.com/news/2016/04/12/Comelec-No-biometrics-in-leaked-data-hack.html;
See also: *Comelec: No biometrics data leaked after hack*, Levi A. So, April 12, 2016.
Source: http://www.philstar.com/headlines/2016/04/12/1572140/comelec-says-no-biometrics-data-leaked-after-hack

[12] *Comelec: No biometrics in leaked data*, CNN Philippines, April 12, 2016.
Source: http://cnnphilippines.com/news/2016/04/12/Comelec-No-biometrics-in-leaked-data-hack.html

[13] *Comelec hacking threatens security of voters: Trend Micro*, Jojo Malig, April 7, 2016.
Source: http://news.abs-cbn.com/halalan2016/focus/04/07/16/comelec-hacking-threatens-security-of-voters-trend-micro

[14] *Claiming good leads, NBI sees arrests soon on Comelec hacking, data dump*, Jet Villa, April 12, 2016.
Source: http://interaksyon.com/article/126361/claiming-good-leads-nbi-sees-arrests-soon-on-comelec-hacking-data-dump;
See also: *Hacking of Comelec voters' list continues*, Nancy C. Carvajal, April 1, 2016.
Source: http://technology.inquirer.net/47495/hacking-of-comelec-voters-list-continues

[15] *Claiming good leads, NBI sees arrests soon on Comelec hacking, data dump,* Jet Villa, April 12, 2016.
Source: http://interaksyon.com/article/126361/claiming-good-leads-nbi-sees-arrests-soon-on-comelec-hacking-data-dump

[16] *Comelec: No biometrics in leaked data*, JC Gotinga, April 12, 2016.
Source: http://cnnphilippines.com/news/2016/04/12/Comelec-No-biometrics-in-leaked-data-hack.html;
See also: *Comelec to sue hackers 'in next few days'*, Paterno Esmaquel II, April 12, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/129203-comelec-sue-hackers-website-data-leak

[17] The Commission was formed only on 8 March 2016.
See: *Nat'l Privacy Commission probes Comelec hacking*, ABS-CBN News, April 29, 2016.
Source: http://news.abs-cbn.com/halalan2016/nation/04/29/16/natl-privacy-commission-probes-comelec-hacking

[18] *When a nation is hacked: Understanding the ginormous Philippines data breach*, Troy Hunt, April 14, 2016.
Source: http://www.troyhunt.com/2016/04/when-nation-is-hacked-understanding.html?m=1

[19] *Sorry over leaked data, Comelec tells public to change passwords*, Camille Diola, April 21, 2016.
Source:http://www.philstar.com/headlines/2016/04/21/1575376/sorry-over-leaked-data-comelec-tells-public-change-passwords

[20] *Comelec to sue hackers 'in next few days'*, Paterno Esmaquel II, April 12, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/129203-comelec-sue-hackers-website-data-leak

[21] Ibid.

"non-sensitive tasks" while investigation was ongoing.[22] Commissioner Rowena Guanzon also raised the issue of accountability on the part of their organization, stating that the *Comelec* should consider firing its own people if found guilty of gross neglect.[23]

The first big break in the case came the next day when Paul Biteng, a young IT graduate, was arrested on suspicion of being among the hackers involved in the incident. Speaking to the media, the *Comelec* and the NBI stated that they were still pursuing Biteng's two accomplices.

Two days later, on April 22, *Comelec* spokesperson Jimenez stated that the extent of Biteng's involvement was still being investigated. He clarified that, while Biteng's involvement in the defacement of the Commission's website was fairly certain, his connection to the data breach had yet to be established.[24] Around this time, the Commission on Human Rights also released a statement stating that it was investigating a possible violation of the right to privacy.[25]

Later that day, the website featuring the *Comelec* database was successfully taken down. It was widely reported that the Department of Justice (DOJ) had coordinated with its U.S. counterpart to carry out the operation.[26] It turned out that the website's domain host (GoDaddy) and security provider (Cloudflare) were both based in the States.[27]

That development notwithstanding, the database was still available via numerous torrent sites. This caused a minor controversy after several individuals came forward and alleged that one of the computers seeding the database could be traced back to the mail server address of the Office of the President (OP) at Malacañang Palace.[28]

The next day, then Undersecretary Manuel Quezon III of the Presidential Communications Development and Strategic Planning Office confirmed with the media that the OP's IT team had investigated the allegation that an OP computer was being used to distribute the compromised database. They also verified if the Palace's Internet domain and email server had, in fact, been breached.[29]According to him, their probe did not yield indication of any unusual activity. It was likely, he said, that someone had intentionally forged Malacañang's email domain to make it appear that the government was itself liable for downloading and seeding the *Comelec* database.

On April 25, human rights legal group Center for International Law Philippines (Centerlaw) sent a demand letter to the *Comelec* asking for immediate action on the breach.[30] The organization gave the Commission twenty-four (24) hours to respond and disclose to the public the measures it had taken to address the breach. *Centerlaw* threatened to file a complaint before the NPC if the *Comelec* fail to heed their demand.

At the same time, the NPC received a letter from FMA calling on the agency to take urgent and concerted action, including the conduct of an independent investigation of the incident. In an

---

[22] Ibid.
[23] *Commissioner Guanzon on Comelec leak: Who's at fault?*, Paterno Esmaquel II, April 21, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/130328-comelec-leak-website-hacking-accountability
[24] *Suspected hacker of Comelec website nabbed*, Paterno Esmaquel II, April 21, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/130252-suspected-hacker-comelec-website-nabbed
[25] *Banks warned vs identity theft 'Comeleak' website taken down*, Lawrence Agcaoili, April 23, 2016.
Source:http://www.philstar.com/headlines/2016/04/23/1575917/banks-warned-vs-identity-theft-comeleak-website-taken-down.
[26] *Searchable website of leaked Comelec data taken down*, Victor Barreriro Jr., April 22, 2016.
Source: http://www.rappler.com/technology/news/130407-website-leaked-comelec-data-taken-down
[27] *Banks warned vs identity theft 'Comeleak' website taken down*, Lawrence Agcaoili, April 23, 2016.
Source:http://www.philstar.com/headlines/2016/04/23/1575917/banks-warned-vs-identity-theft-comeleak-website-taken-down.
[28] *Entire Comelec database available via torrent; Malacañang 'seeding' it?*, Jung Garcia, April 22, 2016.
Source: http://www.interaksyon.com/infotech/entire-comelec-database-available-via-torrent-malacanang-seeding-it
[29] *#COMELEAK | Palace servers compromised? Are sensitive emails safe?*, Jing Garcia, April 25, 2016.
Source: http://www.interaksyon.com/infotech/comeleaks-palace-servers-compromised-are-sensitive-emails-safe
[30] *Manila prosecutor set to file charges vs Comelec 'hacker'*, Joel R. San Juan, April 25, 2016.
Source: http://www.businessmirror.com.ph/manila-prosecutor-set-to-file-charges-vs-comelec-hacker/

inter-agency meeting on the subject, the NPC also received confidential information regarding the breach.[31]

Meanwhile, the Manila Prosecutors Office recommended the filing of a criminal case against Biteng for violating Republic Act No. 10175, or the Cybercrime Prevention Act. While the NBI Cybercrime Division only charged Biteng with "illegal access", the prosecutor's office added two other offenses—data interference and misuse of device.[32] The complaint alleged that all three crimes were carried out involving "critical infrastructure" and thus called for a stiffer penalty.[33]

At this point, the *Comelec* was reported to have transferred the hosting services over its websites to the care of the Department of Science and Technology's Information and Communications Technology Office (DOST-ICTO).[34] Louis Casambre, executive director of DOST-ICTO at that time, confirmed the news and said that his office was already in close coordination with the *Comelec*.[35]

The following day, acting Justice Secretary Emmanuel Caparas said that international agencies had offered to assist the Philippine government in preventing a similar incident from happening again.[36] He added that a multi-agency meeting was conducted to discuss the extent of the breach, the nature of the compromised data, and the means through which the public could protect themselves from the illegal use of the data. The *Comelec* also responded to the NPC's request for a report on the incident.[37]

Two days later, another group, the *People's Freedom Party*, filed a petition with the Supreme Court asking for the suspension or postponement of the May 9 elections due to grave concerns raised by the data breach. Citing the incident and other controversies being linked to the polls, the group claimed that the holding of a "peaceful, honest, orderly, and credible" presidential election was no longer possible.[38]

On 29 April 2016, a second suspect in the case was arrested. Jonel De Asis, a 23-year old semi-conductor company worker, was presented to the media after being tagged as another hacker involved in the breach. According to at least one report,[39] De Asis admitted to being behind *LulzSec* and working with Biteng to carry out the attack. He maintained that his sole motivation for the hack was to expose the vulnerability of the *Comelec* website. He reassured the public that the data he accessed cannot be used to sabotage the elections, considering that a different system was going to run the vote-counting machines.

On 3 May 2016, the NPC formally notified the Comelec that it was investigating the incident. The NPC requested additional information and documents relating to the breach from the DOJ, DOST-ICTO, and FMA. It then commenced its fact-finding investigation two days later by conducting a meeting with *Comelec* personnel connected with the incident. While Chairman Bautista was invited to attend, Spokesperson Jimenez attended in his stead and informed the NPC that he had been designated as head of the Task Force within the *Comelec* that was also looking into the breach.

---

[31] Preliminary Report on the Fact Finding Investigation", dated June 27, 2016, p. 1.
[32] *Comelec hacker faces 60 years behind bars*, Aie Balagtas See, April 26, 2016.
Source: http://newsinfo.inquirer.net/781638/comelec-hacker-faces-60-years-behind-bars
[33] *P600,000 bail recommended for Comelec hacker*, Ghio Ong, April 26, 2016.
Source: http://www.philstar.com/headlines/2016/04/26/1576860/p600000-bail-recommended-comelec-hacker
[34] *Comelec to migrate web hosting services to DOST*, Jose Bimbo F. Santos, April 25, 2016.
Source: http://www.interaksyon.com/infotech/better-late-than-never-comelec-to-migrate-web-hosting-services-to-dost
[35] It is worth noting here that in 2013, the Office of the President issued Administrative Order No. 39, which requires government agencies to migrate to the government web hosting services of DOST-ICTO. However, it explicitly excludes Constitutional Bodies, such as the Comelec, from the mandatory application of its provisions. The Comelec continued to avail of the services of private service providers for its web hosting needs.
[36] *DOJ looking into other effects of Comelec data leak*, Ivy Saunar, April 26, 2016.
Source: http://cnnphilippines.com/news/2016/04/26/doj-on-effects-of-comeleak.html
[37] Preliminary Report on the Fact Finding Investigation", dated June 27, 2016, p. 2.
[38] *SC asked to suspend polls after Comelec data breach*, Tetch Torres-Tupas, April 27, 2016.
Source: http://newsinfo.inquirer.net/781941/sc-asked-to-suspend-polls-after-comelec-data-breach
[39] *Hacker who allegedly leaked Comelec data now in NBI custody*, Anjo Alimario, April 29, 2016.
Source: http://cnnphilippines.com/news/2016/04/29/Comelec-hacker-data-leak.html

The NPC conducted its next investigation hearing on May 19. The session was attended by members of the *Balik Manggagawa* Processing Division of the Philippine Overseas Employment Administration, the NBI Cybercrime Division, Eastern Telecoms, and FMA. Eastern Telecoms was the internet service provider of *Comelec*.

During the hearing, NBI Cybercrime Division Executive Officer Vic Lorenzo recounted that it was around 7:00 AM on March 28 when his office received a call from the *Comelec* informing them of its website's defacement. Their investigation on the matter essentially began that day, even as *Comelec*'s formal complaint was filed only on April 6, or more than a week later. Lorenzo also added that, on April 25, the Bureau met with the DOJ and provided them with a comprehensive report regarding their investigation. Asked about the involvement of the Cybercrime Investigation and Coordinating Center (CICC),[40] Lorenzo confirmed that the CICC had not yet been convened. Finally, Lorenzo acknowledged that they had yet to conduct a forensic investigation of the *Comelec* servers. The Bureau had no copy of the actual *Comelec* database allegedly compromised. What they had was a copy of a database that they found in the laptop of de Asis—the second suspect. The Bureau was under the impression that it was the same material uploaded by *LulzSec Pilipinas*, given their similar file sizes (320GB).

Meanwhile, *Eastern Telecoms* was asked to submit the bandwidth logs of the *Comelec* from March 15 to April 15. The NPC also requested for a comprehensive list of their services.

Other fact-finding sessions were held on May 23 and 25, as well as on June 13 and 14.[41]

On May 27, the *Comelec* submitted to the NPC for review its proposed public notification regarding the incident, which was later published on 21 June 2016.[42]

On 17 June 2016, *Centerlaw*, taking the cause of Dr. Jose Ramon Albert, filed an administrative complaint with the NPC. *Centerlaw* asked the NPC to enjoin *Comelec* to provide each registered voter with the following information: (a) nature of the breach; (b) sensitive personal information possibly involved; and (c) measures taken by the Commission to address the breach.[43]

The NPC eventually came out with a preliminary report, dated 27 June 2016. It established, among others, that: (a) a security breach that gave access to the *Comelec* database containing personal data had occurred; (b) some or all of the data may be used for identity fraud; (c) the breach occurred a week before the *Comelec* website was defaced, and took place over a period of 4-5 days; (d) *Comelec* instituted actions aimed at strengthening the security of its website and database; (e) violation of the DPA may have been committed; and (f) *Comelec* may have been remiss in its duties to protect the personal data of millions of Filipinos that were under its control and custody.

The NPC noted that the unauthorized access to the data appeared to be due to the following: (a) lack of a clear data governance policy in *Comelec*; (b) website vulnerabilities; and (c) failure to monitor security breaches regularly. It then resolved to: (a) notify the DOJ that the *Comelec* website had also been accessed by an IP address registered to the DOST; (b) conduct further clarificatory hearings; and (c) provide *Comelec* personnel with the opportunity to submit evidence and arguments on the issues.

On 28 December 2016, the NPC formally handed down its decision regarding the case. While it excused most *Comelec* personnel from liability, the NPC found *Comelec*, as an organization, and Chairman Bautista, as head of the agency at the time, guilty of actions (and inaction) that constitute violations of the DPA. It then issued the following directives to both respondents:

- appoint or designate a Data Protection Officer within one (1) month;

---

[40] An inter-agency body created by RA 10175 whose task, among others, is to monitor cybercrime cases being handled by prosecution and law enforcement agencies.
[41] Preliminary Report on the Fact Finding Investigation", dated June 27, 2016, p. 3.
[42] Ibid.
[43] *Comelec faces complaint over leak of voters' data*, Michael Bueza, June 17, 2016.
Source: http://www.rappler.com/nation/136778-comelec-national-privacy-commission-complaint-data-leak.

- conduct a Privacy Impact Assessment within two (2) months;
- create a Privacy Management Program within three (3) months;
- create a Breach Management Procedure within three (3) months, and run breach drills; and
- implement organizational, physical and technical security measures in accordance with the implementing rules of the DPA and the NPC's relevant circulars.

The NPC also ordered the *Comelec* to have an independent security audit carried out on its data processing systems for the next five years. The results of these audits must be relayed to the NPC.

The *Comelec* and Chairman Bautista filed a Joint Motion for Partial Reconsideration on 13 January 2017. They sought to set aside the NPC's findings regarding the culpability of both the Commission and Chairman Bautista in supposedly violating the DPA, and the recommendation to prosecute Chairman Bautista for a crime defined under the DPA.

The Motion was premised on three main arguments: (a) the Implementing Rules and Regulations (IRR) of the DPA had yet to be promulgated at the time of the breach; (b) the NPC had yet to define the so-called standards for data protection in government; and (c) *Comelec* had actually formulated and implemented policies and programs that subscribe to the generally accepted industry standards for the security and protection of personal data. The parties also went on to highlight that, as an impeachable officer, Chairman Bautista cannot be criminally charged with and prosecuted for a crime that results in his removal from office. Through it all, they continued to characterize the *Comelec* as a mere unsuspecting victim of circumstances.

Curiously, one *Comelec* Commissioner, Christian Robert Lim, filed a manifestation noting that he was not furnished a copy of the Motion. He said that he did not approve of its filing and implied that, while he did not agree with some parts of the NPC Decision, he found merit in the finding of liability on the part of Chairman Bautista.

On 31 July 2017, the NPC resolved the Motion by affirming its earlier decision, noting that no new arguments were raised by the parties. Among the reasons cited why it maintained its original ruling include:

- In its opinion, there is substantial evidence supporting the conclusion that the proximate cause of the data breach was Chairman Bautista's failure to provide vision and direction to the *Comelec*'s IT unit.
- It did not agree with the assertion that the issuance of its IRR is necessary before the provisions of the DPA can be enforced.
- It found the insistence by *Comelec* that no technical, physical, and organizational measures in data privacy existed at the time of the breach, inconsistent with its personnel's own statements, which sought to prove that *Comelec* had in fact complied with industry standards.
- It did not believe that the Constitutional protection enjoyed by Bautista as Chairman of the *Comelec* was violated.

The case has since been elevated to the Court of Appeals where it remains pending to this day.

What is at Stake

In their 6 April 2016 blog post,[44] *Trend Micro* reported that the "data dump" included information pertaining to over 55 million registered Filipino voters, including 1.3 million citizens residing or working overseas. *Trend Micro* further revealed that the data leak consisted of a large number of sensitive personal information, including millions of fingerprint records, passport numbers and their expiry dates, names of people running for office since the 2010 elections, and even a list of *Comelec* officials with administrative accounts in the Commission's computer system.

Rappler, an online news platform, also conducted their own investigation. They reported that *LulzSec* released a total of 16 databases, containing 355 tables in all. The largest database had a file size of more than 338 gigabytes—over 600 times bigger than all the others combined. It had 103 tables, the names of which seem to refer to election-related data (e.g., candidates, party list, elected, statistics, etc.). It contained 75.3 million rows of records about individuals, with 54.28 million of them not tagged as "disapproved". Incidentally, the latter figure approximates the number of registered voters for the 2016 elections, which, according to the *Comelec* was 54.36 million. While some personal data in the tables (e.g., voters' names, birth dates, and Voter's Identification Numbers or VINs) were encrypted, others (e.g., residential address and birthplace) were not and could be easily seen. For Filipino voters registered overseas, names, birth dates, VIN fields, and current residence addresses were encrypted. However, in certain cases, a person's birthplace, passport number, and the names of his/her parents could be identified by anyone familiar with the individual's real name.

Despite the large amount of exposed data, *Rappler* noted that based on the files they examined, there was no indication that fingerprint images or biometrics data were included in the leak.[45] Nonetheless, they concluded that the data disclosed by the breach were enough to confirm some personal details of registered voters.[46]

It would be the NPC, via its December 2016 Decision, that ended up providing the most comprehensive description of the breach. Finally putting the issue to rest, the agency stated that the incident affected the: (a) voter database in the *Precinct Finder* web application, containing 75,302,683 records; (b) voter database in the *Post Finder* web application, containing 1,376,067 records; (c) *iRehistro* registration database, with 139,301 records; (d) firearms ban database, containing 896,992 personal data records and 20,485 records of firearms serial numbers; and (e) the *Comelec* personnel database, containing records of 1,267 individuals.

How Bad Was It

Assessments as to the extent of damage caused (or risk posed) by the hacking incident and the subsequent data leak vary.

Naturally, *Comelec* constantly downplayed the risks associated with the breach. At the height of the controversy, it insisted on multiple occasions that the breach was not a significant cause for alarm. At one point, its spokesperson even floated the idea that the leaked database could actually be fake.[47]

Very few other government agencies, however, adopted a similar view. One government agency in particular that did not take the matter lightly was the country's central monetary authority. One official said that the information contained in the compromised database is a "good starting point for

---

[44] *Data Protection Mishap Leaves 55M Philippine Voters at Risk*, Trend Micro, April 6, 2016.
Source:http://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/

[45] *Comelec data leak puts Filipino voters 'at risk' – Trend Micro*, Michael Bueza, April 8, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/128716-comelec-data-leak-filipino-voters-risk-trend-micro

[46] *Experts fear identity theft, scams due to Comelec leak*, Michael Bueza and Wayne Manuel, April 1, 2016.
Source: http://www.rappler.com/newsbreak/in-depth/127870-comelec-leak-identity-theft-scams-experts

[47] *Comelec: No biometrics in leaked data*, JC Gotinga, April 12, 2016.
Source: http://cnnphilippines.com/news/2016/04/12/Comelec-No-biometrics-in-leaked-data-hack.html

identity theft".[48] Thus, on 22 April 2016, the *Bangko Sentral ng Pilipinas* (central bank of the Philippines) issued Memorandum No. M-2016-005, reminding all financial institutions to strengthen their "know-your-customer" practices.[49] It specifically reminded them to ask for additional proof in order to verify the identity of both old and new customers.[50]

In stark contrast—and perhaps, understandably so—*TrendMicro* personnel provided a more vivid (and alarming) picture. One senior manager said that the government's perceived weakness in cybersecurity (as exposed by the breach) made it vulnerable to electoral sabotage. He noted, for instance, that the leaked database was to be the same one used for the automated elections. Thus, anyone with a nefarious scheme to modify the poll results could do so. He recommended the hiring of information security personnel capable of handling sensitive data and identifying irregularities. This is a necessary investment, he said, given the increasing prevalence of hacking incidents.[51] His colleague and the firm's technical communications manager also chimed in and disputed the *Comelec*'s early attempt to downplay the breach, saying that contrary to the Commission's claims, some of the information exposed were highly sensitive. While some files would require technical skills to access, their availability online puts the data subjects constantly at risk of scams and identity theft. Like his colleague, the technical communications manager recommended a review of the *Comelec*'s security system and possibly a much-needed revamp.[52]

Other security firms went on to make similar statements. A senior executive for a private cloud solutions company said that the breach confirmed what they have been preaching about the role of encryption in safeguarding sensitive personal information.[53] He emphasized that incidents like this leak, whatever the motivations involved, are only bound to increase in frequency and magnitude. Another expert pointed out that basic security measures are no longer enough, especially for government agencies.[54] Cyber threats and their corresponding solutions (i.e., best practices) are evolving so fast that people would do well to just develop strategies that already assume the vulnerability of their systems.

There was at least one fingerprint expert though who came forward to corroborate the *Comelec*'s claim that biometric data included in the leak was useless. He said the data is not that easy to use (or abuse), as some people suggested.[55] Without access to a computer system capable of interpreting it, the data may actually be devoid of any value. He explained that some computer systems are built specifically for the countries that commissioned their development. Here, the system involved may have been designed and built specifically for the *Comelec*. In theory at least, the only computer capable of understanding the leaked biometric data is with the *Comelec*. Without access to that apparatus, no one can replicate the biometric data or use it for identity fraud.

---

[48] *Bangko Sentral warns against identity theft in wake of 'Comeleak'*, GMA News, April 25, 2016. Source:http://www.gmanetwork.com/news/story/563991/scitech/technology/bangko-sentral-warns-against-identity-theft-in-wake-of-comeleak

[49] *Banks warned vs identity theft 'Comeleak' website taken down*, Lawrence Agcaoili, April 23, 2016. Source:http://www.philstar.com/headlines/2016/04/23/1575917/banks-warned-vs-identity-theft-comeleak-website-taken-down.

[50] *Bangko Sentral warns against identity theft in wake of 'Comeleak'*, GMA News, April 25, 2016. Source:http://www.gmanetwork.com/news/story/563991/scitech/technology/bangko-sentral-warns-against-identity-theft-in-wake-of-comeleak

[51] *Philippines elections hack 'leaks voter data'*, Leisha Chi, April 11, 2016. Source: http://www.bbc.com/news/technology-36013713

[52] *Comelec data leak puts Filipino voters 'at risk' – Trend Micro*, Michael Bueza, April 8, 2016. Source: http://www.rappler.com/nation/politics/elections/2016/128716-comelec-data-leak-filipino-voters-risk-trend-micro

[53] *Breaches in Turkey, Philippines Expose 100 Million Citizens' Personal Data*, Jeff Goldman, April 11, 2016. Source:http://www.esecurityplanet.com/hackers/breaches-in-turkey-philippines-expose-100-million-citizens-personal-data.html

[54] *Breaches in Turkey, Philippines Expose 100 Million Citizens' Personal Data*, Jeff Goldman, April 11, 2016. Source:http://www.esecurityplanet.com/hackers/breaches-in-turkey-philippines-expose-100-million-citizens-personal-data.html

[55] *The Philippines election hack is 'freaking huge'*, James Temperton, April 14, 2016. Source: http://www.wired.co.uk/news/archive/2016-04/14/philippines-data-breach-fingerprint-data

The local IT community also had their say on the matter. Lito Averia, IT consultant for the National Citizens' Movement for Free Elections, was very vocal about his reservations about the purported libertarian motivations behind the hacking. Speaking to the media, he said that while it is possible for some voters to be "targeted" by individuals with criminal intent using the data from the breach, the public should also be wary when attempting to access the leaked database. Hacker groups like *Anonymous* and *Lulzsec* sometimes like to project a positive image, but there is no proper way to confirm this. Any file they release could contain malware that may potentially harm the computer devices it ends up infecting.[56] Averia advised the *Comelec* to look into the incident and adopt all measures necessary to resolve it.[57]

Another IT expert agreed in that, in extreme cases, voters' personal information could be used to commit identity theft. A person can use them to open a bank account or obtain a driver's license. This explains why datasets are often sold in underground markets around the world. He scored the *Comelec* for its inability to secure the large amount of information in its possession. He also observed that even if the system for the website is truly independent of or different from that used during the elections, the damage has already been done. Many people will always associate the equate the *Comelec*'s credibility and competence to the incident.[58]

For groups like the *Bankers Marketing Association of the Philippines*, however, it was important not to let the incident blow things out of proportion. Allan Tumbaga, director for industry relations of the organization, pointed out that customer verification today already go beyond birth dates, addresses, and the maiden name of bank customers' mothers.[59] Banks already ask about account numbers, credit card numbers, and other details about their clients. Nonetheless, some bankers did not want to leave things to chance. For instance, a *Banco de Oro* executive claimed that the incident prompted his company to look into its verification process in order to prevent any of the leaked information from being misused.[60] One option they were looking at was the use of biometrics in customer identity verification.

What Other People Said

Former *Kabataan* Partylist Representative Terry Ridon said that the leak put the integrity of the May 9, 2016 elections at risk by exposing the same to fraud. In a press release,[61] he called on the *Comelec* to make an immediate assessment of the potential impact of the breach on the 2016 elections, including its other possible harms. He asked the Commission to inform all affected voters of the leak, including the dangers it poses, and, at the same time, hold accountable all officials or employees who may have allowed the breach to occur as a result of their malfeasance or nonfeasance.

Senator Vicente "Tito" Sotto III, on the other hand, stated then that the Senate would require a full briefing on the matter from the government agencies involved in the investigation—including IT professionals from the private sector—in order to properly assess the need for additional remedial legislation to prevent a repeat of the incident.[62]

---

[56] *IT expert warns public in accessing leaked COMELEC database*, March 29, 2016.
Source:http://ptvnews.ph/bottom-news-life2/11-11-nation-submenu/49132-it-expert-warns-public-in-accessing-leaked-comelec-database.

[57] *Experts fear identity theft, scams due to Comelecleak*, Michael Bueza and Wayne Manuel, April 1, 2016.
Source: http://www.rappler.com/newsbreak/in-depth/127870-comelec-leak-identity-theft-scams-experts

[58] Ibid.

[59] *Banks warned vs identity theft 'Comeleak' website taken down*, Lawrence Agcaoili, April 23, 2016.
Source:http://www.philstar.com/headlines/2016/04/23/1575917/banks-warned-vs-identity-theft-comeleak-website-taken-down.

[60] Ibid.

[61] *Massive voter data leak poses serious threats to integrity of upcoming polls*, April 12, 2016.
Source:http://kabataanpartylist.com/blog/2016/04/12/massive-voter-data-leak-poses-serious-threats-to-integrity-of-upcoming-polls/

[62] *Aquino blamed for Comelec data breach*, Butch Fernandez, April 22, 2016.
Source: http://www.businessmirror.com.ph/aquino-blamed-for-comelec-data-breach

Former Justice Secretary (now Senator) Leila De Lima asked the concerned agencies to focus on protecting voters' personal data and on preventing identity theft by developing the necessary guidelines.[63] De Lima said that pointing fingers at the *Comelec* is no longer productive. Nevertheless, she was not prepared to consider the Commission free of liability and called on the NBI and the Office of the Ombudsman to investigate. She shared the opinion that a mishandling of the situation could have affected the public's perception of the integrity of the elections.

Meanwhile, Senator Ralph Recto believed that the data leak exposed the absence of a designated State guardian of the country's ICT infrastructure. He then used the incident to consolidate support for the passage of a bill (now a law) seeking the establishment of the Department of Information and Communications Technology (DICT), a Cybercrime Investigation and Coordination Center, and the National Computer Emergency Response Team (CERT). Recto also suggested hiring so-called white hat hackers to guard government IT infrastructures and repel future cyber-attacks.[64]

Susan Ople, advocate for overseas Filipino workers (OFWs) and head of a non-profit organization assisting OFWs, urged the Senate to conduct its own investigation of the hacking.[65] She cited the dangers that Filipinos working overseas are now exposed to because of the breach. She also urged the *Comelec* to share with the public its efforts to safeguard its digital infrastructure.[66]

The legal community was also awash with opinions regarding the incident. *Philippine Internet Freedom Alliance* member Marlon Anthony Tonson, for one, discussed in various fora how the *Comelec* and its officials may be held criminally liable under the country's data privacy law for their failure to protect the voters' personal information. Tonson asserted that the culpability of *Comelec* officials may be traced to the Commission having neglected to implement measures that could have prevented the unsanctioned access. He added that criminal cases may also be brought up for perceived violations of the Voters Registration Act and the Cybercrime Prevention Act. Tonson also suggested filing a *habeas data* petition as another legal option. On the part of the government, Tonson suggested that the Cybersecurity Inter-Agency Committee could be directed to handle the matter and coordinate with the proper authorities in order to prevent similar incidents in the future.[67]

For Eric Maranon III, an election lawyer who worked previously for the *Comelec*, it was important to determine first the nature of the stolen data before looking into its potential harm, and the possible liability of the *Comelec*. If only basic information (i.e., voter's name, precinct number, and barangay) were disclosed, he did not see any liability attaching to the Commission since such types of data are accessible to the public anyway. However, if sensitive information (e.g., photos, signatures, and fingerprints) were compromised, there may be an inquiry as to how the leak could have been prevented. If an investigation confirms criminal negligence on the part of the Commission, prosecutors will be confronted with the challenge of proving its existence. What is clear, however, is that liability will arise from an anti-graft or anti-crime legislation outside of the Omnibus Election Code. Maranon said the Code could not have not contemplated many of the concepts that come into play in this incident (e.g., automated voters' list, digital theft or even computers).[68]

NBI's Vic Lorenzo was of the opinion that without any criminal intent on the part of the *Comelec* personnel involved, they could not be subjected to criminal, civil, or administrative liability. He

---

[63] *After 'Comeleak,' De Lima Urges Guidelines vs Identity Theft*, Yuji Vincent Gonzales, April 28, 2016.
Source: http://newsinfo.inquirer.net/782160/after-comeleak-de-lima-calls-for-govt-guidelines-vs-identity-theft.

[64] *Comelec data breach prompts suggestion to hire 'white hats', Bautista's resignation*, Joel R. San Juan and Butch Fernandez April 24, 2016.
Source:
http://www.businessmirror.com.ph/comelec-data-breach-prompts-suggestion-to-hire-white-hats-bautistas-resignation

[65] *Ople worried over identity thefts after hacking of Comelec website*, April 13, 2016.
Source: http://www.mb.com.ph/ople-worried-over-identity-thefts-after-hacking-of-comelec-website

[66] *Claiming good leads, NBI sees arrests soon on Comelec hacking, data dump,* Jet Villa, April 12, 2016.
Source: http://interaksyon.com/article/126361/claiming-good-leads-nbi-sees-arrests-soon-on-comelec-hacking-data-dump

[67] *Is Comelec liable for website data leak?*, Michael Bueza, April 11, 2016.
Source: http://www.rappler.com/newsbreak/in-depth/127465-comelec-hackers-liability-website-hacking-data-leak.
See also: *Comelec to sue hackers 'in next few days'*, Paterno Esmaquel II, April 12, 2016.
Source: http://www.rappler.com/nation/politics/elections/2016/129203-comelec-sue-hackers-website-data-leak

[68] Ibid.

believed that the Commission was a mere victim and to hold it liable for failing to protect the voters' data was "too absolute" and "unfair".[69]

Kristoffer James Purisima, a private practitioner, also came out stating that the hackers may be charged with any or all of the following offenses: (a) violation of Sec. 4, RA 10175 (illegal access); (b) violation of Sec. 29, RA 10173 (unauthorized access or intentional breach), committed in large scale (Sec. 35); and (c) violation of Sec. 33, RA 8792 (hacking or cracking). Meanwhile, on the part of the *Comelec*, Purisima lists the following offenses: (a) violation of Sec. 26, RA 10173 (accessing personal information and sensitive personal information due to negligence), committed in large scale (Sec. 35), and by a public officer (Sec. 36); (b) violation of Sec. 7(c), RA 6713; (c) violation of Sec. 3(e), RA 3019; and (d) violation of the 1987 Constitution.[70]

Finally, former Assistant Secretary and head of the Presidential Communications Strategic Planning Office Reginald Tongol had his own take on the subject. In a forum he attended with Purisima, he stated that the Comelec may be charged with the following offenses: (a) violation of Section 26(a) and/or (b) of RA 10173 (Accessing Personal Information and Sensitive Personal Information Due to Negligence), committed in large scale and quite possibly through a combination or series of acts; (b) violation of Section 30, RA 10173 (concealment of security breach), committed in large scale and quite possibly through a combination or series of acts; (b) violation of Sec. 7(c), RA 6713; and (d) violation of the 1987 Constitution. Meanwhile, the hackers may be charged with having committed the following crimes: (a) Sec. 29 of RA 10173 (unauthorized access or intentional breach),committed in large scale and quite possibly through a combination or series of acts; (b) violation of Sec. 4(a)(1), RA 10175; (c) violation of Sec. 32, RA 10173 (Unauthorized Disclosure). He agreed that a Petition for a Writ of Habeas Data may also filed against the Office of the President for its "unauthorized processing of the leaked data through its website", and the *Comelec*, "in order to require it to disclose the steps or actions he (sic) has taken to ensure the security, confidentiality, and accuracy of the information."[71]

What Were the Lessons Learned and Where are Things Headed Now

It's been more than two years since the breach. Public outcry has died down, and so have the initial outbursts demanding full accountability on the part of the *Comelec*, and the government in general. Bautista is no longer with the Commission and has not returned from abroad because of a supposed illness. Meanwhile, the country is once again bracing itself for another set of elections. What important lessons should have been learned from this entire episode? Given the way things have turned out, can one perceive an ideal way forward? Here are a number of important points to take away:

- ***Filipinos need to take data privacy seriously***. The DPA has been around since 2012, but it took a disastrous data breach on the part of the Philippine government to actually put it on the map. Anyone asked to look for a silver lining in this controversy would likely point to this fact. If one recalls, the law lay dormant for more than three years, languishing in legislative limbo, before being thrust abruptly into the center of public consciousness.

  Now basking in the attention it deserves, the challenge is about sustaining public interest in the subject—enough for people and organizations to fully appreciate the need to adopt and embed data privacy measures in their respective sectors and industries. Otherwise, all that free publicity will have been for naught. Breaches and questionable data processing practices will continue, with their impact bound to get worse. The most recent scandal involving *Facebook* and *Cambridge Analytica* should be sufficient proof of this. And yet, nobody is any the wiser.

---

[69] Ibid.
[70] *Legal Implications of #COMELEAK* [PowerPoint slides], Kristoffer James E. Purisima, April 23, 2016. Source: https://drive.google.com/open?id=0B3Cl7p3wuem2YTNfRVZfeHFueFk
[71] *Legal Remedies for Data Leakage* [PowerPoint slides], Regie Tongol, April 23, 2016. Source: https://drive.google.com/open?id=0B3Cl7p3wuem2WVNQRkRCbTNmSG8

- ***There has to be a competent, well-resourced, and independent National Privacy Commission***. The breach was the first major test for the NPC, which was just a few weeks old when this extraordinary case fell on its lap. Lacking in funds and staff support, it relied on the good graces of sister units under the Office of the President, and assistance from a small group of volunteers just to conduct its hearings, and even agency meetings—a remarkable initiation rite for a new organization.

  With the NPC ageing in stride with the case, its members are now well into the third and last year of their term (except perhaps for the newest Deputy Privacy Commissioner). It has to be asked: Is it now equipped to handle a similar case, given its existing resources? How about two such cases happening at the same time, or maybe more? Are all members of the organization—from the Commission proper down to the lawyers and IT personnel who make up the bulk of its operations staff—competent to handle this new and specialized field? Do they now have the requisite tools and equipment to carry out their functions?

  So far, the Commission appears preoccupied still with its information awareness efforts. It remains to be seen whether or not its capacity as an institution is mature enough to handle the more substantial and more formidable aspects of its mandate.

  There is also the issue of the NPC's independence. If it is to perform well akin to its peers in other jurisdictions, the Commission should be able to set itself apart from other government units, including the DICT, its parent agency. Its credibility as a regulator—even of fellow offices in government—depends on it. Otherwise, the NPC will unnecessarily compromise the impartial nature of its regulatory and investigative work if perceptions of having close ties to other agencies will persist. What if the DICT becomes the next government agency to suffer a major data breach? How about the Office of the President?

- ***Additional data protection policies are urgently needed to help government agencies and the private sector comply with the DPA***. Critics and proponents alike acknowledge that the DPA offers plenty of policy gaps that both the NPC and Congress need to address through their respective policy-making powers.

  In the case of the Commission, it should continue to issue subsidiary policies that provide minimum standards for data protection constantly being requested by its regulated sectors. It should issue clear rules that prescribe administrative sanctions and penalties against erring persons and/or organizations. These would temper the perceptibly harsh treatment by the DPA of data protection violations, while promoting compliance among organizations and empowerment among the people. Advisories and opinions regarding the more complicated aspects of the DPA ought to be regularly issued, as well. They are extremely important guide posts for the implementation of an admittedly imperfect piece of legislation.

- ***State capacity in other areas such as cybersecurity and cybercrime investigations should also improve***. Data privacy cuts across several fields. Its effectiveness is therefore contingent on these other areas going through similar positive changes and developments. In terms of its anti-cybercrime efforts, the government's readiness (or lack thereof) was in full display when the "I Love You" virus wreaked havoc at the turn of the previous millennium. No one was held accountable then for lack of any law penalizing the development and spreading of a computer virus. Now, there is the Cybercrime Prevention Act, and a slew of other statutes concerning various IT and internet-related offenses. Unfortunately, like the DPA, they also suffer from defects and a significant number of implementation woes. The NBI, for instance, has long lamented the difficulties it encounters when fighting cybercrimes in the country.[72] As recent as last year, it would appear that things have not improved much.[73] Meanwhile, in the

[72] *Fighting cybercrime difficult in PH – NBI*, Pia Ranada, March 7, 2014.
Source: https://www.rappler.com/nation/52454-fighting-cybercrime-philippines-nbi
[73] *NBI admits difficulty handling cybercrime cases*, Hanna Camella Talabucon, October 11, 2017.
Source: http://palawan-news.com/nbi-admits-difficulty-handling-cybercrime-cases/

private sector and among the general public, difficulties in comprehending basic concepts and principles relating to modern technologies also remain widespread. This has to change. The government has to have a plan to build its capacity in handling all these new challenges, a corresponding strategy, and the willingness to dedicate resources towards its realization. Notably, last year, on 2 May 2017, the DICT officially unveiled the country's National Cybersecurity Plan 2022. It remains to be seen, though, whether its implementation is anywhere near the level it is supposed to be.

- ***Extreme caution is necessary when dealing with data-intensive systems***. Governments everywhere are made up of agencies and offices like the *Comelec* whose work involve the collection and processing of sizable amounts of personal data. It's no different with the private sector where so-called data-driven methods and technologies are constants among tech companies and big businesses.

  The *Comelec* breach has made it apparent that a responsible approach to technological advancements is imperative. Integrating them into existing data processing systems are always welcome, and perhaps even inevitable, but there has to be sufficient foresight and careful planning involved. Today, it is worth noting that, despite the hacking incident, the Philippine government is still keen on establishing other data-hungry systems like a mandatory SIM card registration regime and a national ID system. If its approach to these new programs remains the same, the government best prepare for the worst as it would only be a matter of time before it will have to deal with another catastrophic breach, and the reputational stain that go along with it.

  Here, the role of the NPC cannot be overstated. As the primary enforcer of the country's data protection law, its advice regarding the use of these new systems should punctuate and amplify the calls for restraint and reason by privacy advocates and civil society.

- ***Civil society needs to continue promoting the adoption of privacy and data protection measures by government and the private sector***. It shouldn't be lost on anyone that civil society and the public at large will have to continue playing a significant role in this burgeoning story of data privacy in the country. They must remain vigilant and keep a close watch on the efforts both government and the private sector are taking to integrate data protection into their respective systems and organizations. They need to call out those who refuse to heed the clamor for better handling and security of personal data, while giving due credit to those who do. Opportunities for collaborations must always be explored, too, for it is only by working together that stakeholders can hope to ensure an effective and lasting data protection regime in the country.