Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

MOST LAW
RECEIVED
JUN 05 2017
BY: TIME: 11:45 AM

JONATHAN A. DELA CRUZ,
Complainant-Appellant,

-versus-

MARLON GARCIA,
ELIE MORENO,
NEIL BANIGUED,
MAURICIO HERRERA,
ROUIE PEÑALBA,
NELSON HERRERA and
FRANCES MAE GONZALES,
Respondents-Appellees.

OSEC-PR-MNL-2-111116-001
NPS Docket No. XV-07-INV-16E-02592
For: Violation of Section 4(a)(l) and (4) of R.A. No. 10175

Promulgated:
02 JUN 2017

x----------x

RESOLUTION

This resolves the petition for review of the resolution of the City Prosecutor of Manila in the above-entitled case dismissing the complaint for violation of Sections 4(a)(1), (3) and (4) of R.A. No. 10175 against respondents Marlon Garcia, Elie Moreno, Neil Baniqued, Rouie Peñalba Mauricio Herrera, Nelson Herrera and Frances Mae Gonzales for violation of Section 4(a)(l) and (4) of R.A. No. 10175.

The facts of the case as culled in the record are as follows:

Under R.A. No. 8436, as amended by R.A. No. 9636, COMELEC entered into several contracts with SMARTMATIC for the

different aspects of the Automated Election System (AES, for brevity) such as but not limited to, the lease of optical reader (OMR) machines, creation of the source codes for the Election Management System (EMS), Vote Counting Machines (VCM) and Consolidation and Canvassing System (CCS), as well as providing of Electronic Results Transmissions Services (ERTS).

Complainant cited the pertinent provisions of above cited laws that should be observed in ensuring free, orderly, honest, peaceful, credible and informed elections. Despite the rules and precautions, respondents allegedly committed a security breach in the AES, particularly the transparency server, thereby compromising the integrity and credibility of the 2016 elections, in addition to the confidentiality, integrity and availability of computer data and systems.

To prove their allegations, complainant cited the following:

From the reports above cited, it was gathered that:

a.) Smartmatic, through its Technical Support Team, was able to gain access to the script of the transparency server and change the same because of the private access code given by COMELEC IT personnel;

b.) The COMELEC En Banc was not notified of the issue about such change and did not authorize Smartmatic to tweak the script of the transparency server;

c.) The change was only announced to persons inside the Transparency Server Room after it was made;

d.) Non-matching of the hash codes was only discovered after about 24 hours since it was made;

e.) When the personnel of the Smartmatic Technical Support Team were confronted by representatives of different political parties and the PPCRV, the script was changed, again without

notice to and authorization from the COMELEC En Banc for the purpose of demonstrating the hash codes will match for the next result file.

Allegedly, the act of "tweaking' the script of the transparency server caused widespread anxiety and concern all over the nation. The lapses in protocol have undermined the credibility and integrity of the 2016 Elections including the confidentiality, integrity and availability afforded to computer data and systems.

As a consequence thereof, the herein complainant charged the following respondents Marlon Garcia, Elie Moreno, Neil Baniqued, Rouie Peñalba Mauricio Herrera, Nelson Herrera and Frances Mae Gonzales for violation of the following provisions of law:

1) Section 4 (a) (1) of R.A. No. 101751 by accessing a computer system, without right;

2) Section 4 (a) (3) by intentionally or recklessly altering computer data, without right; and

3) Section 4 (a) (4) by intentionally altering or recklessly hindering interfering with the functioning of a computer and computer network by inputting, deleting; and altering computer data and program, without right or authority.

Respondent Elie Moreno of Smartmatic alleged among others that he is an engineer by profession, and currently serves as the General Manager and Project Director of Smartmatic. His duties and responsibilities, among others are: (1) representing Smartmatic with respect to contract negotiations with the COMELEC for the purpose of automating the 2016 national and Local elections; (2) exercising direct supervision and control over all project managers and area managers in the country; (3) coordinating directly with COMELEC with respect to any operational issues in the automation of the 2016 National and Local Elections, in accordance with among others, the procedure

as stated in the Protocol of Escalation in the contract/s between Smartmatic and COMELEC.

He has been involved in at least two (2) National and Local elections in the Philippines the 2010 and the 2013 National and Local Elections. He was likewise involved in the pilot automation of elections in the Autonomous Region of Muslim Mindanao in 2008. For the 2016 National and Local elections, Smartmatic won the bid for the lease of optical Mark Readers that was used in the conduct of the automated elections.

In the hierarchy of the Protocol of Escalation, he was listed as one of the authorities to whom contingencies should be escalated to only when the contingency is at least of medium severity with level 3 intensity or high severity with level 3 intensity.

On May 9, 2016, the Philippine National and Local Elections were held. On that day, he oversaw their operations and helped ensure the smooth conduct of elections with respect to its automation by making sure that the equipment provided by Smartmatic to the COMELEC were fully operational and that technical support was available at all times where it is needed, in accordance with the Contracts entered into by and between Smartmatic and COMELEC.

On Election Day, he was stationed at the National Technical Support Center in Quezon City, where he was remotely monitoring the field activities, and controlling their operations all over the country. While he was in constant communication with the Smartmatic personnel stationed at the Transparency Server at Pope Pius Center, nothing of an urgent nature was reported to him which warranted the need for an escalation of issues with COMELEC officials. The reports which he received then were more in the nature of regular reports with few minor issues such as delay in updates in public results website. He actually learned of the issue for the first time when media reports regarding an alleged "change in the hash code of the Transparency Server" came about the day after the elections. Upon learning about the

issue, he conducted an inquiry. After conducting the investigation, it was clear that the change made was purely cosmetic and did not require escalation to a higher Smartmatic or COMELEC authority, pursuant to the Protocol of Escalation under Annex "W" of the Contracts. Since the correction of the script error identified by Mr. Peñalba was a minor issue, the same did not have to be escalated to him or to the designated COMELEC authority. Instead it remained and was solved at the level where it was found. Smartmatic personnel stationed in the Transparency Server merely acted under the direct supervision and authority of the COMELEC, through Mr. Peñalba. They fulfilled the contractual obligations which Smarmatic was bound to perform and deliver to COMELEC. All the acts of Smartmatic's personnel including those of respondent Moreno, Mr. Garcia and Mr. Baniqued, were executed within the scope of authority and responsibility of the people involved and as explained previously were under the direct supervision and authority of Mr. Peñalba. Smartmatic, furthermore completely acted in good faith and in performance of its contractual duties to the COMELEC. The fact that they were being accused of wrongdoing is truly unfortunate as they have partnered with COMELEC in two previous elections and have endeavored to maintain good relations with the Philippine government.

Respondent Moreno claimed that:

1. There is no probable cause to charge him with Violation Republic Act No. 10175 otherwise known as the Cybercrime Prevention Act of 2012.

In this case, the allegations in the complaint and the documents attached thereto do not support any finding of probable cause against him. On the contrary, the very facts and circumstances alleged therein show that he did not commit any crime or perpetrate any wrongdoing, as in fact none has been committed.

As can be gleaned from the Complaint-Affidavit, there is no particular act ascribed to him. In fact, the complainant does not

seem to be aware that he was not even present at the Pope Pius Center on May 9, 2016, and therefore could not have done any of the alleged illegal acts. Neither does complainant specify the manner by which he was alleged to have committed the acts. For this alone, the complaint against him should be dismissed.

In their fifteen-page Complaint-Affidavit dated May 24, 2016, nowhere has complainant pointed to any overt act that he committed the alleged crime.

On Election Day, he was stationed at the National Technical Support Center in Quezon City, where he was remotely monitoring the field activities, and controlling their operations all over the country.

Complainants impleaded him in their Complaint- Affidavit not because he participated in the commission of the alleged crime or on account of any personal and/or overt act, but solely as an afterthought by reason of his position in Smartmatic as General Manager and Project Director.

Accordingly, the fact alone that he is the General Manager and Project Director of Smartmatic is not sufficient justification to hold him answerable, much less criminally liable, for the offenses of illegal Access, Data Interference and System Interference allegedly committed by him and his co-respondents

2. There was no change done to the AES. Thus there can be no breach to the integrity, confidentiality, and availability of computer data and system.

The AES was never altered, modified, or changed. The AES is made up of several components, namely, the Election Management System ("EMS"), the Vote Counting Machine (previously referred to as the "VCM"), The Consolidation and Canvassing system (previously referred to as the "CCS"). Each component is operated by its corresponding software, which was certified by SLI Global Solutions. These components are

independent of each other and the processes involved in one component do not affect the processes in the other components.

Once the election in a particular precinct is closed, the VCMs compute the results which are then electronically transmitted to the respective Board of Canvassers, the COMELEC Central Server and the Transparency Server. The Canvassing server, Central Server, and the Transparency Server are separate, and there is no cross-over of information or processes from one server to another.

The Transparency Server also does not affect the VCMS because the only function of the Transparency server, insofar as the VCMs are concerned, is to receive one-way data from the VCMs, which are transmitted election result. In other words, the Transparency server cannot transmit information telethon results back to the VCMs. It must be noted that there is actually no way for results to be tampered with just by accessing parts of the Transparency Server, because, aside from the data which is transmitted to the CCS, there are also a total of thirty (30) copies of election returns distributed to different groups. All of the data reflected in these various media should, as they actually did, tally. Once the election results from the VCMs are transmitted to the Transparency Server, a resource file is generated and sent to the laptops of political parties, media and PPCRV in the PPCRV Data Center. The generated resource file is not affected and does not affect the AES. Thus, the data received from and transmitted by the VCMs to the CCS and, the Transparency Server, remain intact.

The change in the hash codes of the resource file (which resulted after the change was made in the script to fix the "?'" problem) did not result in any change in the hash codes of any of the components of the AES. Any resource file, data, or program, whether an integral part of the AES or merely generated therefrom, will contain a hash code, which serves as its unique identifier. In short, a hash, code is unique to the data it identifies and serves like its "fingerprint" to distinguish it from others, and also for easy detection of alteration, revision or modification. Therefore, any alteration, revision or modification of data on ANY

file or component will generate an altered, revised, or modified hash code.

The hash codes of each component of the AES remained as they were even after the correction of "'?" problem in the resource file. What changed merely was the hash code of the resource file that reflected the correction in the script. This does not affect any component of the AES. This is corroborated by the findings of PPCRV's Information Technology Director, Mr. Yu, in his Report dated May 11, 2016.

In fact, this problem was unique to the data packages generated from the Transparency Server alone. No similar problem/issue was ever reported with respect to the data in the other components of the AES. The VCMs, election returns, generated COCs and even the ballots, all correctly reflect the symbol ñ. Thus, the correction to the generated file from the TS was clearly a minor cosmetic change intended only to make the data entries in the components of the AES uniform.

3. He did not commit any act that would make him liable for Illegal Access under Section 4 (A) (1) of R.A. No. 10175.

The crime of Illegal Access pertains to the access to the whole or any part of a computer system without right. The access to fix the script of the resource file is not access to the AES; and the access was authorized by Mr. Peñalba of COMELEC. The following elements must concur in order for there to be Illegal Access:

a. That there is access to the whole or any part of any computer system;

b. That the access was without authority; and

c. That the access affected the confidentiality, integrity and availability of computer data systems.

The foregoing elements of Illegal Access are not present here. First, it cannot be said that there is "illegal access to the whole or any part of the system without right" because the resource file is not part of the AES system, which Complainant claims to have been compromised. The resource file where the change was made does not affect, and is beyond the scope of, the AES system, whose integrity and confidentiality remained intact. Second, the access was made not without right as COMELEC's representative did not object and even ratified the same. Third, the mere cosmetic change in the resource file which was done to fix the special character "?" to "ñ" in the names of some candidates did not in any manner threaten or attack the Transparency Server, let alone the AES system. Nor did the change cause impediments to the legitimate users of the system or data, or cause alteration or destruction with high costs for reconstruction.

4. He did not commit any act that would make him liable for Data Interference and System Interference under R. A. No. 10175.

Data interference is defined as the intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document or electronic data message, without right, including the introduction or transmission of viruses. The following elements must concur in order for there to be Data Interference: (a) That there must be intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document or electronic data message; (b) That the interference was Committed without right, and (c) That the interference affected the confidentiality, integrity and availability of computer data systems. The foregoing elements are not present in the instant case, first, there was no alteration, deletion, deterioration or damaging of any computer data electronic document.

Even assuming the cosmetic change could be considered an alteration, it still does not constitute Data Interference, as it was not made with recklessness or intent to cause damage, in fact, the change was merely made to address a report made by the client:

COMELEC. Second, the cosmetic change was made with right. The process was fully transparent and was known to all. In fact, before the change took effect, Mr. Peñalba, the COMELEC representative, announced the proposed change to all the stakeholders at the Data Center. Assent and authority are conveyed not merely by direct statements, but also by actions and, in this case, by the lack of objections, comments or concerns from any party, including the COMELEC representatives, after Mr. Peñalba announced that a change will be made. Indeed, Mr. Peñalba's act of announcing the change was constitutive of express consent and authority from the party authorized to give the same. Third, the act of changing the script of the resource file was not an intentional infliction of damage, and by no means, affected the integrity of proper functioning or use of stored computer data of computer program of the AES. As mentioned, the change was made on a resource file generated from the Transparency Server, and not on the AES itself.

System Interference refers to the intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering of suppressing computer data or program, electronic document, or electronic data message, without right of authority, including the introduction or transmission of viruses." The following elements must concur in order for there to be System Interference:

a) That there was intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic data message;

b) That the act was done without right; and

c) That the act affected the confidentiality, integrity and availability of computes data systems.

The foregoing elements of System Interference are not present here. First, there was no intentional hindering of interference with the functioning of a computer of computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, or electronic data message. Second, the cosmetic change was done with right as there was no objection whatsoever from COMELEC's representative, Mr. Peñalba, while Mr. Garcia made the change in the workstation in the full view and supervision of Mr. Peñalba. Third, the act of changing the script was not an intentional infliction of damage, and by no means affected the integrity or proper functioning or use of stored computer data or computer program of the AES.

The resource file and script are outside of, and thus could not possibly interfere with, the AES. More importantly, none of the acts alleged affected the confidentiality, integrity, and availability of the AES, which is the state policy enshrined under the R.A. No. 10175. In fact, nowhere in the complaint was it alleged that the official results of the elections were affected by the cosmetic change and at no point was the FS ever put at risk.

5. Smartmatic acted at all times under the authority given by the COMELEC through its officers.

As clearly discernible from the facts stated above, Mr. Garcia, Mr. Baniqued and Mr. Mauricio Herrera all acted within the full view and observation of COMELEC, through the person of Mr. Peñalba. When Mr. Peñalba told Mr. Garcia about the issue of special characters appearing in the names of some candidates, Mr. Garcia told him that he would verify the same and formulate a proposed solution to the problem. Upon verifying that indeed a "?" appears on some names of candidates, Mr. Garcia told Mr. Peñalba that he could make the change and asked if he could announce the same to the representatives of political parties and the media at the Transparency Server. When Mr. Peñalba made the announcement, no one raised any opposition, objection,

comment or concern. Mr. Garcia clearly understood that the announcement signified Mr. Peñalba's agreement that the minor change could be effected. Clearly, there was authority given by Mr. Peñalba, who was acting for and on behalf of COMELEC.

6. The minor change to correct the '"?" to "n" need not be elevated to the COMELEC EN BANC. The problem could be settled without having to elevate the same under the Protocol of Escalation.

Complainant is mistaken to assume that there is a need for the matter to be escalated to the COMELEC en banc. The Protocol of Escalation, which is Annex "W" of the contracts between SMARTMATIC and COMELEC, provides basis for authorized personnel from COMELEC and Smartmatic to classify the issue of special character appearing in the names of some candidates as not being severe enough to warrant escalation. Nowhere in the Protocol of Escalation was it provided that certain instances are subject of an escalation to the COMELEC en banc.

It is also evident that the cosmetic change effected to solve the problem of special characters appearing in some candidates' names does not qualify as either medium or high risk because none of the events that qualify or increase the severity of a problem to medium or high risk were present. In fact, the issue of special characters in some candidates' names could not even qualify as low severity issue since operations are not impaired and there are absolutely no risks to the milestones of the contracts.

7. The crimes charged and defined under R.A. 10175 are not mala prohibita but are mala in se. While R.A. 10175 is a special penal law, the crimes defined thereunder require criminal intent.

In interpreting the relevant provisions of the Act, reference should be made to the construction, definition, intention and interpretation of the Budapest Convention as they are laid out in the Explanatory Report to the Convention on cybercrime. Thus, complainant's position is incorrect. The explanatory Report on the

law states that: 1) the intention of the person in committing the acts; and 2) the effect or injury caused by the act, are both important elements in constituting the offenses under Section 4 (a) (1), (3) and (4) of the Act. Otherwise stated, there must be criminal intent before a person can be considered to have violated R.A. 10175. The Budapest Convention intended that the offenses of Illegal Access, Data interference and system interference, must be committed intentionally, and that the effect or injury caused by the act is an important element of the offense.

8. The records of Senate Deliberations in the enactment of the Cybercrime prevention Act likewise do not characterize the crime charged as mala prohibita. Hence, the offenses of Illegal Access, Data Interference Act must be committed with criminal intent.

The very definitions of "Data Interference" and "System Interference" conspicuously hew the word "intentional". It is clear therefore, that the intent of the legislature was to consider the acts punishable under the Cybercrime Prevention Act as mala in se, rather than *mala prohibita*. As such criminal intent is required, which is lacking in this case.

Respondent NEIL Q. BANIQUED alleged that he has been employed at Smartmatic-TIM Corporation since 14 March 2016 and currently the incoming "Technology Manager". He is being trained to manage Data Centers, the Consolidation and Canvassing System and the Election Management System. He observed the conduct of Mr. Marlon Garcia, who is the acting Technology Manager, for the management of the Parish Pastoral Council for Responsible Voting-Transparency Data Center. On the day of the 2016 National and local Elections, a similar minor change was once again effected by Smartmatic when the special character "?" appearing in the names of certain candidates was adjusted to the letter "ñ". On said date or specifically on 9 May 2016, he was present at the PPCRV Transparency Data Center; to provide technical support as part of his duties as incoming Technology Manager.

For the initialization process, COMELEC, through Mr. Peñalba and another COMELEC personnel, entered its part of the password. Afterwards, he saw Smartmatic personnel enter its part of the password. Afterwards he saw Smartmatic personnel enter its part of the password. To note, the two parts of the security password were held separately by COMELEC and Smartmatic, and thus, before Smartmatic may access the National and Local Elections AES Platform, COMELEC would have to give its consent and authorization by entering its part of the password. This protocol acknowledges the possibility that corrections or updates which carry no risk but are necessary may be implemented, but only with COMELEC's participation. To be sure, Smartmatic could not access or perform any activity in the 2016 NLE AES Platform without the knowledge and consent of the COMELEC through its representative entrusted with its part of the password. After the initialization of the computer system, they were on stand-by for COMELEC's instructions to provide technical assistance to all the parties in the PPCRV Transparency Data Center as and when needed. At 7:00 p.m., he saw a person, whom he later learned to be a representative of Rappler, approach Mr. Peñalba and thereafter approached him and informed him that there was a problem, specifically that the special character ("?') was appearing in the resource file. While Mr. Peñalba and him were discussing, Mr. Garcia came into the main room. Based on the review of the records and the CCTV Footage of the incident, it was 7:24 p.m. when Mr. Peñalba relayed the problem to Mr. Garcia in his presence. Mr. Peñalba explained to Mr. Garcia that there was a problem with a special character "?" appearing in some candidates' names. Mr. Garcia told Mr. Peñalba that he will verify what the problem was. Thereafter, he saw that Mr. Garcia, together with Mr. Mauricio Herrera, verified in the computer if there was a problem, and Mr. Garcia confirmed that the letter "ñ" was not properly displayed and what appeared was a "?" in the names of some candidates. He heard Mr. Garcia informed Mr. Peñalba that he would verify if the change could be implemented. A few minutes later, he saw Mr. Garcia and Mr. Peñalba discuss again. Based on the review of the records and the CCTV footage, it was

at 7:37 p.m. when Mr. Peñalba went to the representatives of the PPCRV, the political parties, and the media present in the room, and announced that a minor change from "?" to "ñ" will be implemented. He did not hear any objection, comment or question from the representatives of the PPCRV political parties and the media, or from any other party present, after Mr. Peñalba had spoken. Thereafter, the minor change took effect and the special character "?" in the text file was appropriately adjusted to "ñ". After such implementation of the minor change, he likewise did not hear any objection, comment or question from the stakeholders present, including the representatives of the COMELEC, the PPCRV, political parties and the media, about the said minor change. In fact, it was only days later that he learned that somebody was making an issue of the minor change made in connection with the special character.

For his part, Respondent Baniqued alleged the following defenses:

1. There is no probable cause to charge him and/or his co-respondents with violation of Sections 4 (a) (1), (3) of R.A. No. 10175 or the Cybercrime Prevention.

Nowhere is it indicated that Complainant personally involved or connected Respondent to the subject matter of his complaint. Likewise, the Statement of the Ultimate Facts in the complaint clearly points to his lack of personal knowledge of the matters and circumstances therein. Complainant is not competent to testify as to the allegations in the complaint His lack of personal knowledge is characterized by his constant reference to documents which he had no participation in the preparation of the reports, etc. which he mentioned in the complaint. Verily, complainant does not appear to be the author or to have participated in the preparation of the report, memorandum, letter and news articles mentioned in the complaint. In other words, his allegations are purely based on unreliable, second-hand information and therefore, deserve no credence or consideration.

2. There is neither allegation nor proof of his supposed participation in the alleged violation of RA. No. 10175.

He had no participation whatsoever in the acts complained of and alleged to be in violation of R.A. No 10175. To recall, he was merely apprised by Mr. Peñalba of a minor concern involving the special character appearing in some of the candidates' names. Thereafter, he simply observed when the minor changes to the special character "?" was implemented to adjust it to the proper letter "ñ". Aside from the sweeping allegation that he violated provisions of R.A. No. 10175, complainant fails to allege or specify any act that he committed in violation of said law or even allege any conspiracy among him and his correspondents to justify his inclusion in this case.

3. The acts alleged in the complaint did not, in any manner breach the Automated Election System (AES) or compromise the confidentiality of the computer data and systems thereof because the AES is systematically separate from the transparency server. Hence, there could not have been any illegal access, data interference or system interference to the AES as is alleged in the complaint.

The hash codes of each component of the AES remained as they were even after the correction of the "?" problem in the resource file. What changed was merely the hash code of the resource file that reflected the correction in the script. This does not affect any component of the AES. This is corroborated by the findings of PPCRV's Information Technology Director, Mr. William Yu in his Report dated May 11, 2016.

Therefore, the charge that he, along with his co-respondents, committed Illegal Access, Data Interference and System Interference that breached the AES which 'violated the confidentiality, integrity and availability of the computer data and systems thereof' is untrue.

Smartmatic at all times, acted within the authority given by them by the COMELEC through its authorized officers.

Every action undertaken by Smartmatic was done with the proper authority, contrary to the allegations in the complaint that they accessed a computer system, altered computer data and interfered with the functioning of a computer without right or authority.

The complainant harps on the alleged failure to notify the COMELEC en banc of the minor change performed by the Smartmatic personnel. Such requirement for a COMELEC en banc authority, however finds no basis in law and jurisprudence, as well as in the Contract executed between the owner of the AES, the COMELEC and Smartmatic. On the contrary, the Protocol of Escalation provided in Annexes "W" of the Contracts between Smartmatic and COMELEC in fact categorically and unequivocally allows Smartmatic to implement minor changes without the need to escalate the same to the COMELEC en banc.

It is clear that the cosmetic change effected to solve the problem of special characters appearing in some candidates' names does not qualify as either medium or high risk. In fact, the issue of special characters in some candidates' names could arguably not even qualify as low severity issues since operations are not impaired and there are absolutely no risks to the milestones of the contracts. Hence, the circumstances did not qualify to warrant escalation in the first place. It was only in the interest of prudence that Marlon Garcia, as Project Manager, stepped in to address the issue.

The offenses of Illegal Access, Data Interference and System Interference of the cybercrime Prevention Act are mala in se and must be committed with malicious intent, as borne by the records or Senate deliberations in the enactment of the Cybercrime Prevention Act.

Baniqued reiterated that the Canvassing Server and Central Server, which for part of the CCS of the AES, are systematically separate from the Transparency Server and that there is no cross-over of information or processes from one server to another. The purpose of the Transparency Server is only to receive data and forward the same to the media and the stakeholders inside the Transparency Data Center, and that by no means would the minor change on the file script of the resource file generated from the Transparency Server affect the scripts/ commands for the AES.

Therefore, since the offenses imputed to him and his co-respondents are characterized as mala in se, he was advised that criminal intent is essential. Aside from the lack of any criminal act which may be specifically ascribed to him, there was no malicious and criminal intent attendant to the act of adjusting the special character "?" appearing in some of the candidates' names to the appropriate letter "ñ". As previously mentioned, it was the owner of the AES itself, the COMELEC through Mr. Peñalba, which requested the simple rectification of a minor issue that was solved in the presence of the representatives of, not only the COMELEC, but as well as these of PPCRV, the political parties, and the media. Further, such minor change was merely for convenience and cosmetic purpose only. The change in the script in the resource file generated from the Transparency Server is distinct from the scripts/commands in the AES, and thus, at no point was the official results of the national elections ever at risk for modifications or alteration.

R.A. No. 10175 or the CYBERCRIME PREVENTION ACT OF 2012 was lifted from the Budapest Convention on Cybercrime and therefore, the Explanatory Report to the Convention on cybercrime that the perpetrator must have acted "intentionally" should be the guiding if not controlling, interpretation, of Section 4 (a) (1), (3) and (4), thereof.

Hence, in interpreting the relevant provisions of the Cybercrime Prevention Act, reference should be made to the construction, definition, intention and interpretation of the

Budapest Convention as they are laid out in the Explanatory Report to the Convention on Cybercrime. In this regard, it can be readily seen that the Complainant's position is contrary to the spirit and intent of R.A. No 10175 which he invokes.

From the foregoing, it can be readily seen that the Budapest Convention intended that the offenses of Illegal Access, Data Interference and System Interference, must be committed intentionally, and that the effect or injury caused by the act is an important element of the offense.

The allegations in the complaint failed to show that all the elements of the offenses of Illegal Access, Data Interference and System Interference are present sufficient to constitute a violation of the Cybercrime Prevention Act.

The simple act of changing the file script in the Transparency Server of the PPCRV could not have given rise to the offenses alleged by complainant. Hence, there is no probable cause to charge him of violating the Cybercrime Prevention Act as the complaint fails to allege the essential elements of the offenses charged under the said act, and with reference to the Budapest Convention and its Explanatory Report.

Respondent Mauricio Herrera alleged that he is an Information Technology expert by profession. He has been a Software Senior Developer of Smartmatic, Inc. since 2009. He has been involved in work regarding automation of elections since 2010. In the Philippines, he was part of support Level 3 of the Consolidation and Canvassing System of Smartmatic-TIM stationed at the National Support Center for the 2013 Local Elections. He also served as an Applications specialist in the 2015 Tabago, Mexico Regional Elections and in the 2010 Venezuelan Congressional and Legislative Elections.

For the 2016 National and Local Elections in the Philippines, he became part of the field Technical support personnel and reported directly to Marlon Garcia, the Project Manager and Acting

Technology Manager for Smartmatic. On May 9, 2016, he was assigned to be present at the Parish Pastoral Council for Responsible Voting Transparency Data Center at the Pope Pius XII Catholic Center Building, U.N. Avenue, Manila to provide technical support regarding the software provided by Smartmatic to the Commission on Elections. The Transparency Data Server is one of the components of the Automated Election System (AES), whose main purpose was for the media and political parties to receive information on election results even before official canvassing began.

He arrived at the Pope Pius Center at around 1:00 p.m. of Election Day. Among those present that day at the Pope Pius Center were Mr. Rouie Peñalba of the COMELEC, Messrs. Marlon Garcia and Neil Baniqued of Smartmatic, and representatives from media and political parties who had their own stations and computers in the premises. COMELEC Commissioner Christian Robert Lim was also in the Pope Pius Center at some time in the afternoon of Election Day. At around 3:00 p.m., he instructed the COMELEC and Smartmatic representatives to initialize the system in preparation for the transmission of votes. In connection with this, the COMELEC and Smartmatic representatives, who each had their separate passwords, had to input the same in order to access the computer system. He recalled that after the components of the password were inputted, they were no longer withdrawn by the COMELEC representative, which he understood to mean his consent to access to the computer system until and unless he said otherwise. In any event, all the actions undertaken by Smartmatic were always done in the presence and with knowledge of the COMELEC through Mr. Peñalba.

At around 7:15 p.m., he saw Mr. Peñalba having a conversation with someone inside the main room of the Pope Pius Center where all the media and political parties had their workstations. He later learned that said person was a representative of the media organization "Rappler". Immediately after the said conversation, Mr. Peñalba informed Mr. Baniqued about a certain issue about special characters appearing in the

names of certain candidates in the data files received by the media. Mr. Garcia came into the main room. Based on the review of the records and the CCTV Footage of the incident, it was 7:24 p.m. when Mr. Peñalba relayed the problem to Mr. Garcia in his presence. Mr. Peñalba explained to Mr. Garcia that there was a problem with a special character "?" appearing in some candidates' names. Mr. Garcia told Mr. Peñalba that he will verify what the problem was. Thereafter, he and Mr. Garcia verified in the computer if there was a problem, and Mr. Garcia confirmed that the letter "ñ" was not properly displayed and what appeared was a "?" in the names of some candidates. He heard Mr. Garcia informed Mr. Peñalba that he would verify if the change could be implemented. A few minutes later, he saw Mr. Garcia and Mr. Peñalba discuss again. Based on the review of the records and the CCTV footage, it was at 7:37 p.m. when Mr. Peñalba went to the representatives of the PPCRV, the political parties, and the media present in the room, and announced that a minor change will be implemented. He was informed that there was no objection, comment or question from the representatives of the PPCRV, political parties and the media, or from any other party present, after Mr. Peñalba had spoken. Thereafter, the minor change took effect and the special character "?" in the text file was appropriately adjusted to "ñ". After such implementation of the minor change, he was likewise informed that no objection, comment or question from the stakeholders present, including the representative of the COMELEC, the PPRCV, political parties and the media, about the said minor change.

Respondent raised the same defenses as that of his co-respondents Elie Moreno and Neil Baniqued.

Respondent Marlon Garcia is the Project Manager and Acting Technology Manager of Smartmatic-TIM Corporation and part of its Field Technical support personnel for the 2016 National and Local Elections. He is an Information Technology expert by profession. He has been an employee at Smartmatic Inc. since 2007. He was hired as an Applications Specialist and was tasked to configure applications, servers and vote-counting machines. Since

then he was involved in three elections, one regional election and two referenda in Venezuela as Applications Deployment Engineer of Smartmatic in which around 30,000 voting machines were configured to accommodate the votes of almost 17,000,000 voters in each event. He was also assigned as a Technology Manager in Bolivia in 2009 as part of the team that handled the biometrics project implementation to enroll 5 million citizens in 75 days. From 2013 to 2014, he has also extensive participation in the conduct of automated elections in Bulgaria and Ecuador, and in a biometrics project implementation in Haiti.

In 2008, he came to the Philippines to be part of the Pre-Sales Team of Smartmatic tasked to do demonstrations in preparation for the implementation of the Automated Elections System. In 2010, he supported the Implementation Team of Smartmatic as one of the Application Specialists. He was among those who were assigned in the configuration of the servers, the Consolidation and Canvassing Systems, laptops and the vote-counting machines.

In the Philippines, he has participated in the 2010 National Elections, 2010 Special Elections, 2013 Local elections and the 2016 National and Local Elections as part of the Technology Team deployed by Smartmatic. In the 2010 National Elections, he served as an Applications Specialist. In the 2010 Special Elections and 2013 Local elections, he was the Technology Manager. He has also participated in the recently concluded 2016 National and Local Elections as Project manager and Acting Technology Manager.

As Project Manager and Acting Technology Manager for the 2016 National and Local elections, his duties and responsibilities included among others, overseeing the overall project implementation, setting up of the infrastructure, installation, configuration and administration of servers, platforms, network equipment and administration of systems platforms.

As Technology Manager, he is familiar with the contracts and other documents defining the relationship between the COMELEC

and Smartmatic and governing the procedures to be undertaken leading to, and on, the National and Local Elections. These documents define the parameters of the relationship between Smartmatic and COMELEC to ensure the accuracy and integrity of the voting process and in particular the requirement to extend technical support.

Respondent Garcia raised the same arguments/defenses as those of his co-respondents.

In his counter-affidavit, respondent ROUIE PEÑALBA of COMELEC refuted the charges against him. He averred that the complainant has no personal knowledge of the incident and based his complaint on second-hand reports and unverified press releases.

He further alleged that the complaint does not contain any averment of the specific acts he committed which constitute the offense charged. He was just mentioned as one of the COMELEC IT personnel assigned at PPRCV at the time of the alleged incident.

The charges against him for Illegal Access under section 4 (a) (1); Data Interference under section 4 (a) (3) and System Interference under section 4 (a) (3) of R.A. No.10175, have a common element that he has done said acts "without right". He alleged that like his co-respondents, it cannot be said that they have acted "without authority". They have the passwords which were imputed during the initialization of process on May 9, 2016. With said passwords, they were granted legitimate access, in one form of another, to the data in the transparency server. In correcting the special character "?" to correctly reflect the "ñ" in some of the names of the candidate's name, they were neither "without authority" to access the data in the transparency server nor in excess of the authority granted to them. There is no showing that when the "?" of the transparency server was changed, it altered the election results.

While respondents Nelson Herrera and Frances Mae Gonzales jointly averred that in the compliant, there were no allegations against them or specific at which would constitute a crime. They were just named as COMELEC IT personnel assigned to the PPCRV Center at the time of the alleged incident. They further adopt all the arguments raised by respondent Rouie Peñalba.

In the Consolidated Reply Affidavit of complainant, he raised the following:

1. The allegation in the Complaint-affidavit and the documents attached thereto are sufficient to support a finding of probable cause against respondents for violations of Sec. 4 (a) (1), (3) and (4) of R.A. No. 10175.

Indisputably, violations of the provisions of R.A. No. 10175 are in the nature of public offenses which enable the complainant, a nominee of the ABAKADA party-list, a participant in the 2016 automated elections, to file a complaint against respondents for purposes of preliminary investigation.

Verily, in order to establish probable cause for purposes of preliminary investigation, he attached documents and news articles containing reports of how the script of the Transparency Server was changed and statements issued thereafter by the pertinent individuals.

The documents and news articles attached in the Complaint-Affidavit are publicly available and should be admitted by the courts on grounds of relevance, trustworthiness, and necessity. Also, when certain facts are within judicial notice of the Court, newspaper accounts only buttressed these facts as facts

Moreover, the individuals who issued statements to the media after the change in the script include respondent Garcia and Commission on Elections Commissioners Rowena Guanzon and

Christian Robert Lim. Indeed, these COMELEC Commissioners are credible and are expected to provide reliable information.

Aside from Dr. William Yu, PPCRV information Technology Director, Mr. Peñalba and Mr. Moreno, the authors of the reports complainant attached in the complaint are in fact respondents herein.

Accordingly, the allegations in the Complaint-Affidavit as well as the evidence in support thereof should be deemed sufficient for the filing of the Information.

2. The violations of Sec. 4(a) (1), (3) and (4) of R.A. No. 10175 are *mala prohibita*.

Criminal intent is not necessary where the acts are prohibited for reasons of public policy.

The Records of the Senate deliberations with respect to the Cybercrime Prevention Act were mischievously taken out of context by respondents. Evidently, the suggestion of Senate President Juan Ponce Enrile was worded as if the latter intended that the definitions of cybercrime offenses expressly provide that they are *mala prohibita*. Surely, despite the acceptance by Senator Angara, the measure's sponsor, of Senate President Enrile's suggestions and the lack of objections thereto, nowhere can it be found in the enacted version of the law that cybercrime offenses are characterized as *mala prohibita*.

Pursuant thereto, a perusal of various special laws will not produce any express statement that the crimes defined therein are characterized as *mala prohibita*. Indeed, respondents and their counsel disregarded the rule that crimes punishable by special laws are generally considered as *mala prohibita*.

A perusal of the records of the Senate deliberations will show that Senate President Enrile proposed to remove the word "intentional" in the definition of the cybercrime offenses of Illegal

Access and Illegal Interception, Data interference and system interference. Senate President Enrile pro-pounded that it is enough that such acts are made without right or justifiable reason.

Consequently, the enacted law illustrates that the word "intentional" was deleted for the cybercrime offenses of Illegal Access and Illegal Interception as compared to the terms of the draft measure and Budapest Convention. As for the cyber crime offenses of Data Interference and system Interference, it can be inferred that the word 'intentional" was not deleted as both cover acts done recklessly or without intent

Furthermore, as a mala in se felony cannot absorb *mala prohibita* crimes, the fact that a prosecution under R.A. No. 10175 shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, further strengthens the argument.

Therefore, it is respectfully submitted that the violations of Sec. 4 (a) (1), (3) and (4) of R.A. No. 10175 be classified as *mala prohibita*, and thus, removes as element thereof, the fact that the access/interference affected the confidentiality, integrity and availability of compute data and systems.

3. The elements of Illegal Access, Data Interference and System Interference under Section 4(a), (3) and (4) of R.A. No. 10175, respectively, are present.

In illegal Access, the access to the whole or any part of a computer system must be without right in Data Interference the intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document or electronic data in age including the introduction of transmission of viruses must be without right.

In System Interference, the intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting damaging, deleting,

deteriorating, altering of suppressing computer data or program, electronic document, of electronic data message must be without right or authority.

The changing of the script of the Transparency Server entails acts constituting access of or interference with a computer data or system.

It is submitted, therefore, that the unauthorized change in the script of the Transparency server be deemed as constituting the elements of access or interference as prescribed by the provisions of Sec. 4(a) (1), (3) and (4) of R.A. No. 10175.

The changing of the script of the Transparency Server was without right or authority.

First, assuming, arguendo, that the Orientation meeting actually took place, the same was presided by Commissioner Lim. Also, instructions/requests were directly made by the latter.

Second, it cannot be presumed that the duty to monitor systems, databases, application servers and scheduled tasks necessarily include the authority to make changes in the script of the Transparency Server.

Third, respondent Peñalba, in his Urgent Memorandum dated 11 May 2016 submitted to the COMELEC En Banc on 12 May 2016, denied that he instructed respondent Garcia to change the script as he does not have the authority to do so. In such declaration, respondent Peñalba is estopped from denying that the Smartmatic personnel were without authority when they changed the said script.

Fourth, the allegation that none of the representatives of the political parties and the media expressed their objections to the changes made in the script of the Transparency Server when it was announced at around 7:30 p.m. of May 9, 2016 is misleading. The change in the script was in the nature of a highly technical

matter that requires meticulous analysis to determine its far-reaching consequences. Nevertheless, the discrepancy in the hash codes were discovered within 24 hours, and immediately raised by the representatives of the political parties before the Smartmatic and COMELEC personnel present in the server room.

Fifth, respondents merely focused on the severity levels in the Protocol of Escalation (e.g. Low, Medium or High), but omitted to explain how the levels of intensity are determined (eg. Level 1, Level 2. Level 3 or Level 4. However, it can certainly be deduced from the Protocol of Escalation that levels of intensity are also characterized by the scope of responsibility attributed to the Smartmatic official and the corresponding COMELEC counterpart personnel designated to undertake decisions. If taken together with the statement of Commissioner Lim as reported in the news article dated 12 March 2016 that he should have been informed of the intended change, the intensity of the contingency should be at least Level 3.

Sixth, respondents cannot deny that no issue is required to be escalated to the COMELEC En Banc as respondent Garcia himself admitted in a press conference held on May 13, 2016 that there are just certain matters that need to be escalated [En banc].

Seventh, Commissioner Guanzon, as reported in the news article dated 14 May 2016, expressed that Smartmatic should have asked permission from the [En banc] first".

The respondents are all liable for participating in the commission of the acts in violation of Sec. 4(a) (1), (3) and (4) of R.A. No. 10175.

As for respondents Garcia, M. Herrera and Baniqued, Smartmatic personnel stationed within the FTC RV, they should be held liable due to the following circumstances:

Clearly, respondent Garcia made the changes in the script of the Transparency Server. Prior to effecting the change thereto,

respondent M. Herrera admitted in his Counter-Affidavit that he was the one who gave advice to respondent Garcia and certainly emboldened the latter.

In essence, his act falls under aiding and abetting in the commission of a cybercrime by which he should be held liable. Meanwhile, respondent Baniqued cannot deny participation by alleging that he was a mere observer. It is appalling that a personnel of Smartmatic was allowed to loiter within the premises of the PPCRV for mere observation and training purposes.

Nonetheless, the presence of respondents Garcia, M. Herrera and Baniqued directly diverges from the plain provision of COMELEC Resolution 10105A, stating that "only personnel from the COMELEC ITD shall be allowed in the restricted area where the actual server and hardware equipment are located."

Respondent Moreno's allegation that he was stationed at the National Technical Support Center in Quezon City should be taken with a grain of salt.

As a matter of fact, respondent Moreno himself admitted that he was the one remotely monitoring the field activities and controlling the operations of Smartmatic all over the country. Moreover, his participation, knowledge and acquiescence to the change in the script of the Transparency Server can be inferred from the fact that he was in constant communication with the Smartmatic personnel assigned to the PPCRV Center and was responsible for making the report in behalf of his staff.

Without a doubt, the acts were knowingly committed and approved on behalf of Smartmatic, which falls within the scope of respondent Moreno's authority. Sec. 9 of RA 10175 appropriately states that: the liability imposed on a juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

Respondent Peñalba, N. Herrera and Gonzales, likewise, cannot deny participation as they comprise the COMELEC ITD personnel assigned to the PPCRV server room and supposedly the only individuals allowed in the restricted area where the actual server and hardware equipment are located.

Respondent Peñalba was the one who actually instigated the change in the script. Respondent Peñalba did not object to such change and even announced it to the representatives of the political parties. Remarkably, respondent Peñalba failed, in the scheme of things, to inform the COMELEC or at least Commissioner Lim, of the proposed change and seek their authorization.

Unmistakably, respondent Peñalba exceeded his authority in allowing the Smartmatic personnel to effect such change. Respondents N. Herrera and Gonzales, being his subordinates and without raising any objection thereto, should also be held liable. Yet again, their act falls under aiding and abetting in the commission of a cybercrime.

In their joint rejoinder-affidavit, respondents Marlon Garcia, Elie Moreno and Neil Baniqued reiterated their arguments and defenses as alleged in their Counter-Affidavit. Respondents in addition, wish to correct an erroneous statement in the Reply-Affidavit. Complainant misquoted Mr. Garcia as allegedly having stated that "there are just certain matters that need to be escalated [en banc]," as Mr. Garcia made no statement to that effect to the media. A reading of the whole paragraph from where the quote was lifted will reveal that Mr. Garcia's statement was misquoted by the newspaper article, as the statement evidently should have been stated in the negative, thus:
"Garcia said they did not raise the issue to the en banc because the changes that had been made did not require any financial disbursements. He said: There are just certain matters that need to be escalated to en banc.

We now resolve.

As regards the liability of Respondents-Appellees, we may only discuss the same on their actual participation of the acts as provided in the allegations.

Contrary to the findings of the City Prosecutor of Manila, this Office may only absolve Elie Moreno (stationed at the NTSC in Quezon City) for the lack of any allegation attributing any act of participation constituting a violation of the provisions of the Cybercrime Prevention Act.

Marlon Garcia, himself, admitted that he made the change in the script of the transparency server as advised by Mauricio Herrera. Notably, it was Rouie Peñalba who notified the Smartmatic personnel. However, this Office cannot absolve him for his inconsistent statements of having instructed Marlon Garcia to change the script because he (Peñalba) had no authority to do so, but belatedly acknowledged that Smartmatic personnel had authority to access the system. Rouie Peñalba, along with Frances Mae Gonzales and Nelson Herrera, as COMELEC representatives assigned to the PPCRV Center and holding ½ of the password to access the system, acquiesced to the access or interference effected by the Smartmatic personnel, beyond their authority.

The elements constituting violations of the aforesaid provisions of the Cybercrime Prevention Act are as follows:

Sec.4(a)(1) - Illegal Access

1. That there be access to the whole or any part of a computer system; and

2. That said access is without right.

Sec. 4(a)(3) –Data Interference

1. That there be intentional or reckless act/s of alteration, damaging, deletion or deterioration of computer data,

electronic document or electronic data message including transmission or introduction of virus; and

2. That said act/s are done without right.

Sec. 4(a)(4) –System Interference

1. That there beact/s of intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message; and

2. That said act/s are done without right or authority.

Prior to discussing whether or not the elements of the violations of the aforesaid sections of the Cybercrime Prevention Act, a special law, are present, we deem it right to rule that the same should be classified as crimes *mala prohibita*. The language of the law is clear that any illegal access to the computer or any part thereof without right is a violation of the Cybercrime Act. Aside from the clarion clear wordings of the law, it is worthy to note that the real intention of the legislative body as exemplified by the records of the Senate deliberation wherein the proposal of Senator Enrile was accepted by the sponsor of the law to remove the word "intentional" in the definition of the Cybercrime offenses only proves that violation of the cybercrime law is intended to be mala prohibita. Thus, criminal intent is not necessary where the acts are prohibited by reason of public policy, the mere perpetration thereof, constitute an offense against the confidentiality, integrity, and availability of computer data and systems. As a consequence, proof of good faith or damage is immaterial. When the doing of the act is prohibited by law, it is considered injurious to public welfare, and the doing of the prohibited act is the crime itself.[1]

---

[1] Dungo v. People, G.R. No. 209464, July 1, 2015.

Nonetheless, as cited by Complainant-Appellant, the Supreme Court clarified said matters as should be raised in the trial court and threshed out in a judicial proceeding, to wit:

> The other issues raised by the COMELEC – whether the offenses punished under Section 27(b) of R.A. No. 6646, a special law, are *mala prohibita* or *mala in se* and whether damage is an element of the offenses are likewise matters which are properly raised in the trial court and threshed out in a judicial proceeding, being necessarily interconnected with the defense raised by respondents.

Record shows that there was access made to, and there were acts of interference done on the whole or part of a computer system, data, electronic document or electronic data message, computer or computer network. The Transparency Server, its resource files, the script thereof, etc. fall under the definition of a computer, computer data, computer program or computer system as provided under the Cybercrime Prevention Act.

Thus, this Office is merely confined to determining whether or not said acts of access or interference were done without right or authority.

The following reasons were contended by respondents-appellees and acceded to by the City Prosecutor of Manila to prove that their acts were with right or authority:

Being the project manager of Smartmatic, Marlon Garcia was given the right to access the AES, after the system was initialized upon instruction of COMELEC Commissioner Christian Robert Lim. The entering of the COMELEC's password was the operative act that conferred the right or authority upon Smartmatic from that time to access the computer. It would be absurd to expect Smartmatic to provide election automation service if it has no right to access the AES which is the automation system that runs the election. It is not only Smartmatic's right to access the AES but

also its duty to do so. Marlon Garcia had previously effected a change on the script upon the request of COMELEC Commissioner Lim and by the political parties present during an orientation meeting held on April 29, 2016.

The change effected on the script was within the competence of Marlon Garcia, the project manager to deal with, which means that prior authority from the COMELEC was not necessary. It was alleged that the issue was only of low or medium severity level as per the Protocol of Escalation. Thus, not all incidents related to the operation of the AES require a notice to the COMELEC En Banc.

We do not agree.

Smartmatic personnel cannot conclude that when COMELEC entered its ½ of the password to initialize the system, it then gave to the former access to make changes thereon. Effecting a change on the script in the transparency server as requested by the COMELEC and by the political parties prior to the day of elections is different from effecting a change thereon on the day of elections without any request or any authority given by the COMELEC. In fact, Smartmatic personnel should have followed the protocol of escalation.

As regards the Protocol of Escalation, this Office finds the need to incorporate the whole document to clarify the purpose thereof:

ANNEX "W"
PROTOCOL OF ESCALATION

This Annex involves contingency matters for escalation to higher authorities to report, secure agreements or approvals, and directions/guidance on subsequent actions steps. Authorized personnel from both parties are likewise indicated to identify the counterpart personnel that shall undertake such decision/s.

Contact Names, Email Addresses, and Telephone Numbers of these personnel are indicated in this Annex to enable reproduction of copies for the functions that may be involved in such escalation processes.

The particulars of this document shall be updatable during the contract period to enable further inclusions or deletions.

LEVEL	SMARTMATIC JV	COMELEC	SEVERITY	BEFORE ELECTION DAY	ON ELECTION DAY
1	Area Manager Email address: 2016nle@smartmatic Office Phone: TBD Mobile Phone: TBD	Area Director Email address: TBD Office Phone: TBD Mobile Phone: TBD	LOW	The officer in-charge has 12-hours after receipt of the incident report to offer resolution(s).	The officer in-charge has 30 minutes, after receipt of the incident report to offer resolution(s) .
1	Area Manager Email address: 2016nle@smartmatic Office Phone: TBD Mobile Phone: TBD	Area Director Email address: TBD Office Phone: TBD Mobile Phone: TBD	MEDIUM	The officer in-charge has 6 hours after receipt of the incident report to offer resolution(s).	The officer in-charge has 20 minutes after receipt of the incident report to offer resolution(s) .
1	Area Manager Email address: 2016nle@smartmatic Office Phone: TBD	Area Director Email address: TBD Office Phone: TBD Mobile Phone: TBD	HIGH	The officer in-charge has 1 hour after receipt of the incident report to offer resolution(s).	The officer in-charge has 10 minutes, after receipt of the incident report to offer resolution(s) .
LEVEL	**SMARTMATIC JV**	**COMELEC**	**SEVERITY**	**BEFORE ELECTION DAY**	**ON ELECTION DAY**
2	Project Manager **Marlon Garcia** Email address: marlon.garcia@smart	Project Director: **TBD** Email address:		The officer in-charge has 12 hours after receipt of the	The officer in-charge has 30 minutes

	matic.com Office Phone: 02-74512694 Mobile Phone: 0917-8784619	TBD Office Phone: TBD Mobile Phone: TBD	LOW	incident report to offer resolution(s).	after receipt of the incident report to offer resolution(s) .
2	Project Manager **Marlon Garcia** Email address: marlon.garcia@smart matic.com Office Phone: 02-74512694 Mobile Phone: 0917-8784619	Project Director Email address: TBD Office Phone: TBD Mobile Phone: TBD	MEDIUM	The officer in-charge has 6 hours after receipt of the incident report to offer resolution(s).	The officer in-charge has 20 minutes, after receipt of the incident report to offer resolution(s) .
2	Project Manager **Marlon Garcia** Email address: marlon.garcia@smart matic.com Office Phone: 02-74512694 Mobile Phone: 0917-8784619	Area Director Email address: TBD Office Phone: TBD Mobile Phone: TBD	HIGH	The officer in-charge has 1 hour after receipt of the incident report to offer resolution(s).	The officer in-charge has 10 minutes, after receipt of the incident report to offer resolution(s) .
LEVEL	**SMARTMATIC JV**	**COMELEC**	**SEVERITY**	**BEFORE ELECTION DAY**	**ON ELECTION DAY**
3	G.S. Director for APAC **Elie Moreno** Email address: emoreno@smartmatic .com Office Phone: 02-7451264 Mobile Phone: 0917-8723446	Chairman of Steering Committee: **Comm. Robert Christian Lim** Email address: TBD Office Phone: TBD Mobile Phone: TBD	MEDIUM	The officer in-charge has 6 hours after receipt of the incident report to offer resolution(s).	The officer in-charge has 20 minutes after receipt of the incident report to offer resolution(s) .
3	G.S. Director for APAC **Elie Moreno** Email address: emoreno@smartmatic .com Office Phone: 02-7451264	Chairman of Steering Committee: **Comm. Robert Christian Lim** Email address:	HIGH	The officer in-charge has 1 hour after receipt of the incident report to offer resolution(s).	The officer in-charge has 10 minutes, after receipt of the incident

	Mobile Phone: 0917-8723446	TBD Office Phone: TBD Mobile Phone: TBD			report to offer resolution(s).
3	VP for Global Services **Nick Sandoval** Email address: Nick.sandoval@smartmatic.com Mobile Phone: +15612129780	COMELEC Chairman: **Hon. J. Andres Bautista** Email address: chairman@comelec.gov Office Phone: TBD Mobile Phone: TBD	HIGH	The officer in-charge has 1 hour after receipt of the incident report to offer resolution(s).	The officer in-charge has 10 minutes, after receipt of the incident report to offer resolution(s).

Levels indicated above refer to the intensity of the contingency where Level 1 is the lowest and Level 4 being the highest. The differentiation is the length of time the impact of a contingency event hampers the operation during or before the Election Day. Since Election Day is a critical event and lasts only for approximately half a day, the time element between escalation is designed to be very short.

The severity levels are defined as follows:

LOW

- The project timelines, budget and quality will be slightly affected or will not be affected at all by the matter subject to escalation.
- Impaired operations of some components, but allows the users to continue using the system.
- Milestone completion are at minimal risk.

MEDIUM

- The project timelines, budget and quality will be considerably affected by the matter subject to escalation.
- A major functionality or service is severely impaired.

- Operations can continue in a restricted fashion, although long-term productivity might be adversely affected.
- A major milestone is at risk. Ongoing and succeeding activities are affected.
- A temporary workaround is available.

HIGH

- The project timelines, budget and quality will be severely affected by the matter subject to escalation.
- Production platforms or other mission critical system(s) are down and no workaround is immediately available.
- All or a substantial portion of the mission critical data or service is at a significant risk of loss or corruption.
- There has been a substantial loss of service.
- The operations have been severely disrupted.

Let it be emphasized, it is explicitly stated that the Annex involves contingency matters for escalation to higher authorities to report, secure agreements or approvals and directions/ guidance on subsequent action steps. Authorized personnel from both parties are likewise indicated to identify the counterpart personnel that shall undertake such decision/s.

A perusal of said document indicates that there are 6 columns. The first column with the heading, LEVEL, indicates the level of intensity (1,2,3, and 4) of the contingency depending on the length of time the impact of a contingency event hampers the operation during or before Election Day. The second column with the heading, SMARTMATIC JV, and the third column with the heading, COMELEC, shows the Smartmatic personnel assigned to report any issue to, and seek approval of any contingency measure from a COMELEC personnel assigned to undertake a decision thereon. The third column with the heading SEVERITY, shows how an issue under different levels of intensity (1,2,3, and 4)are classified under different levels of severity (low, medium, and high). The fourth and fifth columns, with the headings BEFORE ELECTION DAY and ON ELECTION DAY, respectively,

provide that the officer-in-charge (COMELEC personnel or official) shall have a certain period of time to offer resolution(s).

From the foregoing, it cannot be concluded that any issue classified under any level of severity (low, medium, or high)pertaining to any level of intensity (1, 2, 3, or 4) can be decided alone by a Smartmatic personnel or official, particularly in this case, Marlon Garcia. Indeed, the protocol of escalation requires any Smartmatic personnel to report on any issue regardless of level (severity or intensity) to a COMELEC personnel or official. It is only the designated COMELEC personnel or official which may undertake any decision thereon.

Moreover, it was established that respondents was able to access the transparency server to change the same without notifying the COMELEC en banc. It must be noted that the COMELEC IT Personnel assigned at the PPCRV center had no authority to allow any Smartmatic personnel to tweak the script of the transparency server. As a result thereof, the hash codes failed to match. However, despite the said alteration, said fact was not announced until after the lapse of 24 hours when the parties were alerted of said fact.

Nonetheless, the failure of the respondent to secure the authorization of the COMELEC en banc before they made a change on the script of the transparency server is against the protocol. And not only that said act is an offense under Sections 4(a) (1), (3) and (4) of the Cybercrime Act.

The issues involved herein, notwithstanding their connection to the conduct of elections, require technical knowledge of computers, programs, data, systems, etc. To reiterate, whether or not the change effected caused material damage is immaterial as the perpetration of the acts, without right or authority, constitute an offense against the confidentiality, integrity, and availability of computer data and systems. In any case, it is deemed best for said issues to be resolved and threshed out at the trial proper.

WHEREFORE, premises considered, the Petition for Review is hereby **PARTIALLY GRANTED** and the Resolution dated September 28, 2016 of the City Prosecutor of Manila is **MODIFIED**. The Office of the City Prosecutor of Manila is directed to file the necessary Information for violations of Sec. 4(a)(1), (3) and (4) of the Cybercrime Prevention Act against respondents Marlon Garcia, Neil Baniqued, Mauricio Herrera, Rouie Peñalba, Nelson Herrera and Frances Mae Gonzales before the appropriate court/s and to report the action taken within ten (10) days from receipt hereof, while the dismissal of the complaint against Ellie Moreno is hereby affirmed.

SO ORDERED.

Manila, Philippines.

For the Secretary of Justice:

DEO L. MARCO
Undersecretary

Copy furnished:

THE CITY PROSECUTOR
Manila

ATTY. ANNA LIZA G. LOGAN
ATTY. ADRIAN F. AUMENTADO
Counsels for the Complainant-Appellant
MOSTLAW
(Formerly Marcos Ochoa Serapio and Tan Law Office)
30th Floor, Tycoon Centre
Pearl Drive, Ortigas Center, Pasig City

ANGARA ABELLO CONCEPCION REGALA & CRUZ
Counsel for Respondent Marlon Garcia and Smartmatic Respondents
22nd Floor, ACCRALAW Tower
2nd Avenue corner 30th Street
Crescent Park West, Bonifacio Global City
Taguig City

DIME & EVIOTA LAW FIRM
Counsel for COMELEC Respondents
Unit 201 Midway Court Building
241 EDSA Mandaluyong City