EN BANC

G.R. No. 224027 – AL S. VITANGCOL III, Petitioner, **v. COMMISSION ON ELECTIONS, represented by its Chairperson, HON. ANDRES D. BAUTISTA,** Respondent.

G.R. No. 224116 – AL C. ARGOSINO, Petitioner, **v. COMMISSION ON ELECTIONS, represented by its Chairperson, HON. ANDRES D. BAUTISTA,** Respondent.

Promulgated:

October 11, 2016

x---x

SEPARATE OPINION

LEONEN, *J.*:

I concur in the result. Petitioners seek to determine whether the data received by the Commission on Elections during the transmission of election results originated from the devices recognized by the Commission on Elections. However, the transmission of election results to the Commission on Elections central server has been terminated. The May 9, 2016 Elections have been carried out. It is in this sense that the issues raised have become moot and academic.

Nevertheless, the issues that petitioners raise are susceptible to repetition. In a few years, the electorate will again cast their votes through the automated election system. Rather than this Court again having to deal with belatedly filed petitions as in the past, we should take cognizance of this case for the early guidance of the bench, the bar, and the public.

I

The Commission on Elections, as early as 1992, identified the modernization of the electoral process as a vital part of its six (6)-year modernization program under Operation Modex (Modernization and Excellence).[1] The passage of Republic Act No. 8436[2] in 1997 authorized the

[1] Filipinas Heritage Library, *A History of Automated Elections in the Philippines*, <http://www.filipinaslibrary.org.ph/features/275-a-history-of-automated-elections-in-thephilippines> (last visited September 14, 2016).

[2] An Act Authorizing the Commission on Elections to Use an Automated Election System in the May 11, 1998 National or Local Elections and in Subsequent National and Local Electoral Exercises, Providing Funds Therefor and for Other Purposes (1997).

use of an automated system for the May 1998 Elections and subsequent national and local elections. On January 23, 2007, Republic Act No. 9369[3] was passed amending several provisions of Republic Act No. 8436. Section 1 of Republic Act No. 8436 now reads:

> SECTION 1. **Declaration of Policy**. – It is the policy of the State to *ensure free, orderly, honest, peaceful, credible and informed elections*, plebiscites, referenda, recall, and other similar electoral exercises by improving on the election process and adopting systems, *which shall involve the use of an automated election system that will ensure the secrecy and sanctity of the ballot and all election, consolidation and transmission documents in order that the process shall be transparent and credible and that the results shall be fast, accurate and reflective of the genuine will of the people*. (Emphasis supplied)

However, it was only on May 10, 2010 that the automated election system was implemented nationwide.[4]

The use of the automated election system during the 2010 National Elections—though attended with numerous issues concerning its viability—was regarded as a big step forward in terms of our democratic process.[5] In a span of 11 hours after the polls closed, about 78.55 percent of votes for the national elective positions had already been released.[6] In the 2013 Elections, within 21 hours after the polls closed, about 68.68 percent of the votes had been transmitted.[7]

The May 9, 2016 Elections set a record for the largest electronic vote count and speed of tally.[8] About 86% of the votes were transmitted during election night, thus giving the public a fairly accurate idea of who the new set of public officials was.[9]

[3] An Act Amending Republic Act No. 8436, entitled "An Act Authorizing the Commission on Elections to Use an Automated Election System in the May 11, 1998 National or Local Elections and in Subsequent National and Local Electoral Exercises, to Encourage Transparensy, Credibility, Fairness and Accuracy of Elections, Amending for the Purpose Batas Pambansa Blg. 881, As Amended, Republic Act No. 7166 and Other Related Election Laws, Providing Funds Therefor and for Other Purposes (2007).

[4] Filipinas Heritage Library, *A History of Automated Elections in the Philippines* <http://www.filipinaslibrary.org.ph/features/275-a-history-of-automated-elections-in-thephilippines> (visited September 14, 2016).

[5] Christian S. Monsod, *The 2010 automated elections – An assessment* <http://www.philstar.com/opinion/629285/2010-automated-elections-assessment> (visited September 27, 2016).

[6] GMA News Online, *Transmission of poll results much slower in 2013 than in 2010* <http://www.gmanetwork.com/news/story/308541/news/nation/transmission-of-poll-results-much-slower-in-2013-than-in-2010> (visited September 20, 2016).

[7] Id.

[8] Philippine Daily Inquirer, *Smartmatic: PH now world reference point for automated elections* <http://newsinfo.inquirer.net/785083/smartmatic-ph-now-world-reference-point-for-automated-elections> (visited September 19, 2016).

[9] Id.

Indeed, the automated election system has its advantages, speed of results being primary. Automation is seen as a way to reduce electoral fraud by minimizing human intervention. However, the automated election system is still vulnerable to other forms of interference.

Petitioners Al S. Vitangcol III and Al C. Argosino allege in their Petitions for Mandamus[10] that the automated election system may be compromised through various forms of hacking.[11] To prevent this, petitioners seek to compel the Commission on Elections to submit an inventory of the Media Access Control (MAC) and Internet Protocol (IP) addresses, as well as the International Mobile Subscriber Identity (IMSI) of all the Subscriber Identity Module (SIM) Cards and International Mobile Equipment Identity (IMEI), of all vote-counting machines, servers, computers, broadband global area networks, and other communication devices to be used for the 2016 Elections.[12]

II

For a clearer grasp of the issues, a definition of some technical terms is necessary.

A Media Access Control (MAC) address refers to the unique hardware or physical address of a network device.[13] MAC addresses are composed of six (6) two-digit hexadecimal numbers[14] written in MM:MM:MM:SS:SS:SS format.[15] The first three (3) bytes are known as the Organizational Unique Identifier, which identifies the manufacturer of the device. The last three (3) bytes identify the type of device and its serial number.[16] MAC addresses are permanent and do not change regardless of where the device is.[17]

An Internet Protocol (IP) address is a unique address that allows a network device to communicate with another network device.[18] An IP address can either be static or dynamic. As its qualifier suggests, a static IP address is permanent.[19] It contains information that can reveal the exact

[10] *Rollo* (G.R. No. 224027), pp. 6–20.
[11] Id. at 10–16.
[12] Id. at 16.
[13] IP Location, *What is a MAC Address?* <https://www.iplocation.net/mac-address> (visited September 27, 2016).
[14] Techterms, *MAC Address* <http://techterms.com/definition/macaddress> (visited September 27, 2016).
[15] IP Location, *What is a MAC Address?* <https://www.iplocation.net/mac-address> (visited September 27, 2016).
[16] Webopedia, *What is a MAC Address?* <http://www.webopedia.com/quick_ref/what_is_a_mac_address.asp> (visited September 27, 2016).
[17] Technomag, *How IP and MAC Addresses Work Together During Data Transmission* <http://www.technomag.co.zw/2016/06/15/techexchange-ip-mac-addresses-work-together-data-transmission/#sthash.rQp2eOjO.dpbs> (visited September 27, 2016).
[18] *What is an IP Address?* <http://whatismyipaddress.com/ip-address> (visited September 27, 2016).
[19] Id.

location and internet service provider of the device.[20] In contrast, a dynamic IP address is only temporary and is assigned each time the device connects to the internet.[21]

MAC and IP addresses work together so that network devices can communicate with one another.[22] Simply put, a MAC address is akin to a person's full name, while an IP address is akin to a person's address.[23]

A Subscriber Identity Module (SIM) Card contains a unique and permanent ID called the International Mobile Subscriber Identity (IMSI). The IMSI number is used to identify a device connected to a particular network.[24] A database used by internet service providers, known as the Home Location Register, contains each IMSI connected to the network.[25] The Home Location Register is updated every time a device transfers to another location. This allows the network to determine recent location information of the device.[26]

An International Mobile Equipment Identity (IMEI) number is a unique ID hardcoded in mobile devices, usually located in the battery compartment.[27] The purpose of an IMEI number is to identify mobile devices connected to a network.[28] Mobile carriers can also use the IMEI number to blacklist a stolen mobile phone and block the device from connecting to the network.[29]

III

The primary mode of transmitting election data from vote-counting machines and other election-related devices to the servers is through electronic transmission. For this purpose, a virtual private network is created. A virtual private network allows users to "securely access a private network and share data remotely through public networks."[30] Devices

[20] Id.

[21] Id.

[22] Technomag, *How IP and MAC Addresses Work Together During Data Transmission* <http://www.technomag.co.zw/2016/06/15/techexchange-ip-mac-addresses-work-together-data-transmission/#sthash.rQp2eOjO.dpbs> (visited September 27, 2016).

[23] Id.

[24] Tech-FAQ, *IMSI (Internet Mobile Subscriber Identity)* <http://www.tech-faq.com/imsi.html> (visited September 20, 2016).

[25] HLR Check, *What is HLR?* <https://www.hlrcheck.com/overview> (visited September 20, 2016).

[26] Techopedia, *Home Location Register* <https://www.techopedia.com/definition/7580/home-location-register-hlr> (visited September 19, 2016).

[27] Know Your Mobile, *IMEI number* <http://www.knowyourmobile.com/glossary/imei-number> (visited October 4, 2016).

[28] Make Tech Easier, *Everything You Should Know About Your IMEI Number* <https://www.maketecheasier.com/imei-number> (visited October 4, 2016).

[29] Id.

[30] Gizmodo, *VPNs: What They Do, How They Work and Why You're Dumb for Not Using One* <http://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one> (visited October 4, 2016).

connected to the network are identified by their corresponding MAC and IP addresses.[31]

There are four (4) levels of transmission involved in the automated election system. The first level of transmission takes place when the vote-counting machines transmit the election returns to the municipal board of canvassers.[32] The municipal board of canvassers then transmits the election returns to the provincial board of canvassers. Finally, the provincial board of canvassers transmits the election returns to the national board of canvassers and to the central server.[33]

The second level of transmission takes place when the vote-counting machines transmit the election returns directly to the Commission on Elections' central server.[34] The third and fourth levels of transmission takes place when vote-counting machines transmit the election returns to the transparency server[35] and to another server at the Joint Congressional Canvassing.[36]

Electronic transmission within the virtual private network involves the use of cellular data or mobile data network. For areas without cellular cites, a broadband global area network is used.[37] To connect to a cellular network, vote-counting machines are equipped with the SIM cards[38] of Globe Telecom Inc:, Smart Communications Inc., and Digitel Mobile Philippines Inc., otherwise known as Sun Cellular.[39]

Although the transmission process occurs within a virtual private network, there is a possibility that the data may be intercepted at the weakest link of the network through various forms of hacking.[40]

[31] *Rollo* (G.R. No. 224027), p. 15.

[32] JC Gotinga, CNN Philippines, *How electronic vote transmission works* <http://cnnphilippines.com/news/2015/11/04/how-electronic-vote-transmission-works.html1> (visited September 19, 2016).

[33] Id.

[34] Id.

[35] Id.

[36] *Rollo* (G.R. No. 224027), p. 15.

[37] Roel Pareño, Philippine Star, *Election data transmission prone to jamming* <http://www.philstar.com/nation/2016/02/25/1556667/election-data-transmission-prone-signal-jamming> (visited September 19, 2016).

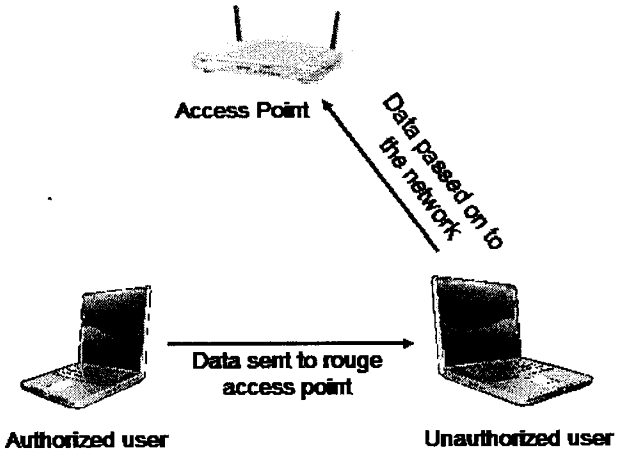
[38] Leslie Ann Aquino, Manila Bulletin, *Comelec to conduct nationwide election results transmission tests* <http://www.mb.com.ph/comelec-to-conduct-nationwide-election-results-transmission-tests> (visited September 19, 2016).

[39] Roel Pareño, Philippine Star, *Election data transmission prone to jamming* <http://www.philstar.com/nation/2016/02/25/1556667/election-data-transmission-prone-signal-jamming> (visited September 19, 2016).

[40] *Rollo* (G.R. No. 224027), pp. 15–16.

IV

For instance, a Man-In-The-Middle (MITM) attack is a form of confidentiality attack[41] where a third party actively monitors, captures, and controls data sent by one device to another.[42] An MITM attack allows a third party to re-route data exchange,[43] as illustrated below:[44]


Access Point
Data passed on to the network
Data sent to rouge access point
Authorized user
Unauthorized user

In an MITM attack, the authorized user is forced to connect to an unauthorized user. Through the process of "sniffing,"[45] the unauthorized user can capture data, alter it, and transmit the altered data to the access point.[46]

Another form of interception is a Denial of Service (DoS). The purpose of a DoS attack is to make a portion of the network unreachable to prevent an authorized user from gaining access.[47] One type of DoS attack is an authentication flood. In an authentication flood, "thousands of authentications are sent from random Media Access Control (MAC) addresses"[48] to the access point.[49] This floods the access point's authentication table, thereby making it difficult for an authorized user to gain access to the network.[50]

[41] *Wireless Hacking Tools* <http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking> (visited October 4, 2016).

[42] Microsoft, *Common Types of Network Attacks* <https://technet.microsoft.com/en-us/library/cc959354.aspx> (visited October 4, 2016).

[43] Id.

[44] *Wireless Hacking Tools* <http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking> (visited October 4, 2016).

[45] A sniffer is an application that can capture "network data exchanges." *See* <https://technet.microsoft.com/en-us/library/cc959354.aspx> (visited October 4, 2016).

[46] *Wireless Hacking Tools* <http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking> (visited October 4, 2016).

[47] Id.

[48] Id.

[49] Id.

[50] Id.

The Commission on Elections' consolidation and canvassing system was designed to accept only one (1) transmission from a precinct.[51] Through a combination of hacking techniques, it is possible to prevent the vote-counting machines from transmitting legitimate election results to the servers. This is a vulnerability of the automated election system that needs to be addressed.

Petitioners assert that the transmissions may be verified and authenticated by examining the transmission logs of public telecommunications networks. The MAC and IP addresses reflected in the transmission logs should match the MAC and IP addresses of election-related devices.[52] The Commission on Elections can undertake the verification and authentication of transmission logs if it has a record or inventory of the MAC and IP addresses and the IMSI and IMEI numbers of all election-related devices. Presently, the election returns, at most, only reflect the vote-counting machines' IDs.[53]

However, it is as important for the public to be able to assess the integrity of the entire automated election system.

V

A petition for mandamus may be given due course if the party instituting it is "aggrieved by the . . . inaction of a tribunal, corporation, board, or person, which unlawfully excludes [the] party from the enjoyment of a legal right."[54] For mandamus to lie, the plaintiff must possess a clear legal right to the act demanded and a direct interest in the duty to be performed.[55]

When the subject of the petition for mandamus relates to a public right such as the right to information on matters of public concern, and when the object of the petition is to compel the performance of a public duty, the petitioner need not show that its interest on the result is exclusive.[56] It may be shared by the public in general. In *Legaspi v. Commission on Civil Service*:[57]

[51] *Rollo* (G.R. No. 224027), p. 16.

[52] Id. at 14.

[53] Michael Bueza, *#PHVoteWatch: What election returns, other poll documents look like* <http://www.rappler.com/nation/politics/elections/2016/131815-samples-election-returns-poll-documents-comelec> (visited on October 4, 2016).

[54] *Guingona v. Commission on Elections*, 634 Phil 516, 527 (2010) [Per J. Carpio, En Banc].

[55] *Legaspi v. Commission on Civil Service*, 234 Phil 521, 535 (1987) [Per J. Cortes, En Banc].

[56] *Tañada v. Tuvera*, 220 Phil 422, 430 (1985) [Per J. Escolin, En Banc].

[57] 234 Phil 521 (1987) [Per J. Cortes, En Banc].

> But what is clear upon the face of the Petition is *that the petitioner has firmly anchored his case upon the right of the people to information on matters of public concern, which, by its very nature, is a public right.*
>
> . . . .
>
> From the foregoing, it becomes apparent that *when a Mandamus proceeding involves the assertion of a public right, the requirement of personal interest is satisfied by the mere fact that the petitioner is a citizen, and therefore, part of the general "public" which possesses the right.*[58] (Emphasis supplied).

This principle was reiterated in *Guingona v. Commission on Elections*:[59]

> In order that a petition for mandamus may be given due course, it must be instituted by a party aggrieved by the alleged inaction of any tribunal, corporation, board, or person, which unlawfully excludes said party from the enjoyment of a legal right. *However, if the petition is anchored on the people's right to information on matters of public concern, any citizen can be the real party in interest. The requirement of personal interest is satisfied by the mere fact that the petitioner is a citizen, and therefore, part of the general public which possesses the right. There is no need to show any special interest in the result. It is sufficient that petitioners are citizens and, as such, are interested in the faithful execution of the laws.*[60] (Emphasis supplied, citations omitted)

The People's right to information on matters of public concern is enshrined in Article III, Section 7 of the Constitution:

> ARTICLE III
> Bill of Rights
>
> . . . .
>
> SECTION 7. The right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents, and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law.

For every person's fundamental right, there is a corresponding duty on the part of government to recognize and protect it.[61] In *Valmonte v. Belmonte*:[62]

[58] Id. at 530.

[59] 634 Phil. 516 (2010) [Per J. Carpio, En Banc].

[60] Id. at 527.

[61] *Legaspi v. Civil Service Commission*, 234 Phil. 521, 531 (1987) [Per J. Cortes, En Banc].

[62] 252 Phil. 264 (1989) [Per J. Cortes, En Banc].

> The right to information goes hand-in-hand with the constitutional policies of full public disclosure and honesty in the public service. It is meant to enhance the widening role of the citizenry in governmental decision-making as well in checking abuse in government.[63]

The policy of full public disclosure is enshrined in Article II, Section 28 of the Constitution:

> ARTICLE II
>
> . . . .
>
> State Policies
>
> . . . .
>
> SECTION 28. Subject to reasonable conditions prescribed by law, the State adopts and implements a policy of full public disclosure of all its transactions involving public interest.

Like other constitutional guarantees, the right to information and the policy of full public disclosure are not absolute.[64] The People's right to information is limited by the nature and classification of the information sought.[65] The information should involve "matters of public concern"[66] and should not be excluded by law from the operation of the guarantee.[67] In the same manner, the policy of full public disclosure is limited to transactions involving public interest and is subject to reasonable conditions prescribed by law.[68] In *Legaspi*:

> "Public concern" like "public interest" is a term that eludes exact definition. Both terms embrace a broad spectrum of subjects which the public may want to know, either because these directly affect their lives, or simply because such matters naturally arouse the interest of an ordinary citizen. In the final analysis, it is for the courts to determine in a case by case basis whether the matter at issue is of interest or importance, as it relates to or affects the public.[69]

Guided by this principle, this Court has granted petitions for mandamus anchored on the right to information as it found that the information sought was a matter of public concern.[70]

l

[63] Id. at 271–272.

[64] *Ba-Ra v. Commission on Elections,* 551 Phil. 1, 13 (2007) [Per J. Garcia, En Banc].

[65] Id.

[66] CONST., art. III, sec. 7.

[67] *Legaspi v. Civil Service Commission*, 234 Phil. 521, 529 (1987) [Per J. Cortes, En Banc].

[68] CONST., art. II, sec. 28.

[69] *Legaspi v. Civil Service Commission*, 234 Phil. 521, 535 (1987) [Per J. Cortes, En Banc].

[70] *See Subido v. Ozaeta,* 80 Phil. 383 (1948) [Per J. Tuason, En Banc]; *Tañada v. Tuvera,* 220 Phil. 422, (1985) [Per J. Escolin, En Banc]; *Legaspi v. Civil Service Commission*, 234 Phil. 521 (1987) [Per J. Cortes, En Banc]; and *Valmonte v. Belmonte,* 252 Phil. 264 (1989) [Per J. Cortes, En Banc].

In *Ba-Ra v. Commission on Elections*,[71] this Court ordered the Commission on Elections to disclose or publish the names of the nominees of party-list groups, sectors, or organizations accredited to participate in the 2007 Elections.[72] In *Guingona*, a case involving the automated election system, this Court ordered the Commission on Elections to disclose information pertaining to the conduct of the 2010 Elections.[73]

Without a doubt, information on the conduct of elections is a matter of public concern as it directly affects the lives of the People. The conduct of free, orderly, honest, peaceful, and credible elections is the primary mechanism by which the principles of a democratic and republican society can be achieved.[74] It is an exercise of direct sovereignty from which all government authority emanates. To borrow the words of Former Chief Justice Reynato S. Puno, elections lie at the very heart of our democratic process because it is through voting that consent to the government is secured.[75]

The issues raised by petitioners have far-reaching and serious implications. The claim that hackers can intercept, alter, and send the altered data to the Commission on Elections servers may cast doubt on the integrity of election results. Consequently, the legitimacy of the newly elected officials may be questioned. The electorate may find the automated election system unreliable, which may then deter them from casting their votes on election day.

The Commission on Elections may be compelled, through mandamus, to make an inventory of and disclose the MAC and IP addresses and IMSI and IMEI numbers of all electronic devices used during elections to the public. It is mandated to enforce and administer all laws and regulations relative to the conduct of an election.[76]

In relation to the state's policy to ensure the transparency of the election process and the credibility of the results,[77] the Commission on Elections must ensure that the automated election system meets the minimum system capabilities as listed in Section 6 of Republic Act No. 8436, thus:

[71] 551 Phil. 1 (2007) [Per J. Garcia, En Banc].

[72] Id. at 15–16.

[73] *Guingona v. Commission on Elections*, 634 Phil. 516, 536–539 (2010) [Per J. Carpio, En Banc].

[74] CONST., art. II, sec. 1.

[75] J. Puno, Dissenting Opinion in *Tolentino v. Commission on Elections*, 465 Phil 385, 417 (2004) [Per J. Carpio, En Banc].

[76] CONST., art. IX-C., sec. 2, par. (1).

[77] Rep. Act No. 8436 (1997), as amended by Rep. Act No. 9369 (2007), sec. 1, par. 1.

> SEC.6. *Minimum System Capabilities.* – The automated election system must at least have the following functional capabilities:
>
> (a) *Adequate security against unauthorized access*;
> (b) *Accuracy in recording and reading of votes as well as in the tabulation, consolidation/canvassing, electronic transmission, and storage of results*;
> (c) Error recovery in case of non-catastrophic failure of device;
> (d) System integrity which ensures physical stability and functioning of the vote recording and counting process;
> (e) Provision for voter verified paper audit trail;
> (f) *System auditability which provides supporting documentation for verifying the correctness of reported election results*;
> (g) An election management system for preparing ballots and programs for use in the casting and counting of votes and to consolidate, report and display election result in the shortest time possible;
> (h) Accessibility to illiterates and disabled voters;
> (i) Vote tabulating program for election, referendum or plebiscite;
> (j) Accurate ballot counters;
> (k) Data retention provision;
> (l) Provide for the safekeeping, storing and archiving of physical or paper resource used in the election process;
> (m) Utilize or generate official ballots as herein defined;
> (n) Provide the voter a system of verification to find out whether or not the machine has registered his choice; and
> (o) Configure access control for sensitive system data and functions. (Emphasis supplied)

Any form of doubt on the integrity of election results is detrimental to our democratic form of government. Clearly, then, transparency is imperative to dispel fears and mistrust.

The case may have been rendered moot and academic, but the Petitions should be granted for fuller guidance of the bench and bar as automated elections will definitely occur in the future.

ACCORDINGLY, the Petitions should be granted. The Media Access Control (MAC) and Internet Protocol (IP) addresses, as well as the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) numbers, of all election-related devices should be made public.

MARVIC M.V.F. LEONEN
Associate Justice