

G.R. No. 203335 - JOSE JESUS M. DISINI, JR., ET AL., *Petitioners*, v. THE SECRETARY OF JUSTICE, ET AL., *Respondents*; **G.R. No. 203299** - LUIS "BAROK" C. BIRAOGO, *Petitioner*, v. NATIONAL BUREAU OF INVESTIGATION, ET AL., *Respondents*; **G.R. No. 203306** - ALAB NG MAMAMAHAYAG (ALAM), ET AL., *Petitioners* v. OFFICE OF THE PRESIDENT, ET AL., *Respondents*; **G.R. No. 203359** - SENATOR TEOFISTO DL GUINGONA III, *Petitioner*, v. THE EXECUTIVE SECRETARY, ET AL., *Respondents*; **G.R. No. 203378** - ALEXANDER ADONIS, ET AL., *Petitioners*, v. THE EXECUTIVE SECRETARY, ET AL., *Respondents*; **G.R. No. 203391** - HON. RAYMOND V. PALATINO, *Petitioners*, v. HON. PAQUITO N. OCHOA, JR., ET AL., *Respondents*; **G.R. No. 203407** - BAGONG ALYANSANG MAKABAYAN SECRETARY GENERAL RENATO M. REYES, JR., ET AL., *Petitioners*, v. BENIGNO SIMEON C. AQUINO III, *Respondents*; **G.R. No. 203440** - MELENCIO S. STA. MARIA, ET AL., *Petitioners*, v. HON. PAQUITO OCHOA, ET AL., *Respondents*. **G.R. No. 203453** - NATIONAL UNION OF JOURNALISTS OF THE PHILIPPINES, ET AL., *Petitioners*, v. THE EXECUTIVE SECRETARY, ET AL., *Respondents*; **G.R. No. 203454** - PAUL CORNELIUS T. CASTILLO, ET AL., *Petitioners*, v. THE HON. SECRETARY OF JUSTICE, ET AL., *Respondents*; **G.R. No. 203469** - ANTHONY IAN M. CRUZ, ET AL., *Petitioners*, v. HIS EXCELLENCY BENIGNO S. AQUINO III, ET AL., *Respondents*; **G.R. No. 203501** - PHILIPPINE BAR ASSOCIATION, INC., *Petitioner* v. HIS EXCELLENCY BENIGNO S. AQUINO III, ET AL., *Respondents*; **G.R. No. 203509** - BAYAN MUNA REPRESENTATIVE NERI J. COLMENARES, *Petitioner*, v. THE EXECUTIVE SECRETARY PAQUITO OCHOA, JR., *Respondent*; **G.R. No. 203515** - NATIONAL PRESS CLUB OF THE PHILIPPINES, INC., ET AL., *Petitioners*, v. OFFICE OF THE PRESIDENT, PRESIDENT BENIGNO SIMEON AQUINO III, ET AL., *Respondents*; **G.R. No. 203518** - PHILIPPINE INTERNET FREEDOM ALLIANCE, ET AL., *Petitioners*, v. THE EXECUTIVE SECRETARY, ET AL., *Respondents*.

Promulgated:

FEBRUARY 18, 2014

X-----X

SEPARATE CONCURRING OPINION

BRION, J.:

A. Concurrences & Dissents

Technology and its continued rapid development in the 21st century have been pushing outward the boundaries of the law, compelling new responses and the redefinition of fundamental rights from their original

P

formulation; enlarging the need for, and the means of, governmental regulation; and more importantly, sharpening the collision between the individual's exercise of fundamental rights and governmental need for intervention.

In this kind of collision, the Court – as constitutionally designed – finds itself in the middle, balancing its duty to *protect individuals'* exercise of fundamental rights, with the *State's intervention* (through regulation and implementation) in the performance of its duty *to protect society*. It is from this vantage point that the Court, through the *ponencia*, closely examined the Cybercrime prevention Act (*Cybercrime Law*) and the validity of the various provisions the petitioners challenged.

I write this Separate Concurring Opinion to generally support the ponencia, although my vote may be qualified in some provisions or in dissent with respect to others. In line with the Court's "per provision" approach and for ease of reference, I have tabulated my votes and have attached the tabulation and explanation as Annex "A" of this Separate Opinion.

This Opinion likewise fully explains my vote with a full discussion of *my own reasons and qualifications* in the areas where I feel a full discussion is called for. I am taking this approach in Section 12 of the Cybercrime Law in my vote for its unconstitutionality. My qualifications come, among others, in terms of my alternative view that would balance cybercrime law enforcement with the protection of our citizenry's right to privacy.

I concur with the *ponencia's* finding that cyber-libel as defined in Section 4(c)(4) of the Cybercrime Law does not offend the Constitution. I do not agree, however, with the *ponencia's* ultimate conclusion that the validity is "*only with respect to the original author of the post*" and that cyber-libel is unconstitutional "*with respect to others who simply receive the post and react to it.*"

I believe that the constitutional status of cyber-libel hinges, not on Section 4(c)(4), but on the provisions that add to and qualify libel in its application to Internet communications. For example, as the *ponencia* does, I find that **Section 5¹ of the Cybercrime Law** (which penalizes aiding, abetting or attempting to commit a cybercrime) is unconstitutional for the reasons fully explained below, and should not apply to cyber-libel.

I likewise agree with Chief Justice Sereno's point on the unconstitutionality of applying **Section 6 of the Cybercrime Law** (which

¹ Section 5. Other Offenses. — The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of Cybercrime. — Any person who wilfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) Attempt in the Commission of Cybercrime. — Any person who wilfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

penalizes crimes committed through information communications technology) and impose on libel a penalty one degree higher.

Further, I join Justice Carpio's call to declare **Article 354 of the Revised Penal Code** unconstitutional when applied to libellous statements committed against public officers and figures, and to nullify the application of **Section 7 of the Cybercrime Law** to cyber-libel.

On the other content-related offenses in the Cybercrime Law, I concur with the *ponencia* in upholding the constitutionality of **Section 4(c)(1)** on cybersex and **Section 4(c)(2)** on child pornography committed through computer systems, and in striking down as unconstitutional **Section 4(c)(3)** for violating the freedom of speech.

I also agree that **Section 5² of the Cybercrime Law**, in so far as it punishes aiding, abetting or attempting to commit online commercial solicitation, cyber-libel and online child pornography, violates the Constitution.

Lastly, I partially support the *ponencia*'s position that **Section 19³** of the Cybercrime Law (which empowers the Secretary of the Department of Justice to restrict or block access to computer data found to be in violation of its provisions) is unconstitutional for violating the right to freedom of expression.

B. My Positions on Cyber-libel

B.1. The Core Meaning and Constitutionality of Section 4(c)(4)

Based on a *facial examination* of Section 4(c)(4) of the Cybercrime Law, I find no reason to declare cyber-libel or the application of Section 355 of the Revised Penal Code (that penalizes libel made in print and other forms of media, to Internet communications) unconstitutional.

Laws penalizing libel normally pit two competing values against each other – the fundamental right to freedom of speech on one hand, and the state interest's to protect persons against the harmful conduct of others. The latter conduct pertains to scurrilous speech that damages the reputation of the person it addresses. Jurisprudence has long settled this apparent conflict

² Section 5. Other Offenses. — The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of Cybercrime. — Any person who wilfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) Attempt in the Commission of Cybercrime. — Any person who wilfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

³ Section 19. Restricting or Blocking Access to Computer Data. — When a computer data is *prima facie* found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data.

by excluding libelous speech outside the ambit of the constitutional protection.⁴ Thus, the question of whether a libelous speech may be penalized by law – criminally or civilly – has already been answered by jurisprudence in the affirmative.

Article 355 of the Revised Penal Code penalizes “libel⁵ committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means.” Section 4(c)(4) of the Cybercrime Law merely extends the application of Article 355 to “communications committed through a computer system, or any other similar means which may be devised in the future.” It does not, by itself, redefine libel or create a new crime – it merely adds a medium through which libel may be committed and penalized. Parenthetically, this medium – under the statutory construction principle of *ejusdem generis* – could already be included under Article 355 through the phrase “any similar means.”

Thus, I fully support the constitutionality of **Section 4(c)(4)** as it stands by itself; its intended effect is merely to erase any doubt that libel may be committed through Internet communications.⁶ However, my support stops there in light of the qualifications under the law’s succeeding provisions.

B.2. Sections 5, 6 & 7 of the Cybercrime Law

In the process of declaring internet defamatory statements within the reach of our libel law, the Cybercrime Law also makes the consequences of cyber-libel far graver than libelous speech in the real world. These consequences result from the application of other provisions in the Cybercrime Law that Congress, in the exercise of its policy-making power, chose to impose upon cybercrimes.

Thus, the law, through **Section 5**, opts to penalize the acts of aiding, abetting, and attempting to commit a cybercrime; increases the penalty for crimes committed by, through and with the use of information and communications technologies in **Section 6**; and clarifies that a prosecution

⁴ *Guinguin v. Court of Appeals*, 508 Phil. 193, 197 – 198 (2005).

See: Joaquin Bernas, *The 1987 Constitution of the Republic of the Philippines: A Commentary*, 2003 Edition, p. 272;

In as early as 1909, our jurisprudence in *US v. Sedano* has recognized the constitutionality of libel, noting that “the provisions of the Constitution of the United States guaranteeing the liberty of the press, from which the provisions of the Philippine Bill were adopted, have never been held to secure immunity to the person responsible for the publication of libelous defamatory matter in a newspaper.”

⁵ Libel, as defined by Article 353 of the Revised Penal Code as a public and malicious imputation of a crime, or of a vice or defect, real or imaginary, or any act, omission, condition, status, or circumstance tending to cause the dishonor, discredit, or contempt of a natural or juridical person, or to blacken the memory of one who is dead.

⁶ During the interpellations of the cybercrime bill before the Senate, Senator Edgardo J. Angara, the bill’s principal sponsor, pointed out that cyberspace is just a new avenue for publicizing or communicating a libellous statement which is subject to prosecution and punishment as defined by the Revised Penal Code. Senate Journal, December 12, 2011, available at <http://www.gov.ph/2012/10/03/for-the-record-public-records-of-senate-deliberations-on-the-cybercrime-prevention-bill/>

under the Cybercrime Law does not *ipso facto* bar a prosecution under the Revised Penal Code and other special laws in **Section 7**.

In my view, the application of these provisions to cyber-libel unduly increases the prohibitive effect of libel law on online speech, and can have the effect of imposing self-censorship in the Internet and of curtailing an otherwise robust avenue for debate and discussion on public issues. In other words, **Section 5, 6 and 7** should not apply to cyber-libel, as they open the door to application and overreach into matters other than libelous and can thus prevent protected speech from being uttered.

Neither do I believe that there is sufficient distinction between libelous speech committed online and speech uttered in the real, physical world to warrant increasing the prohibitive impact of penal law in cyberspace communications.

The rationale for penalizing defamatory statements is the same regardless of the medium used to communicate it. It springs from the state's interest and duty to protect a person's enjoyment of his private reputation.⁷ The law recognizes the value of private reputation and imposes upon him who attacks it – by slanderous words or libelous publications – the liability to fully compensate for the damages suffered by the wronged party.⁸

I submit that this rationale did not change when libel was made to apply to Internet communications. Thus, cyber-libel should be considered as the State's attempt to broaden the protection for a person's private reputation, and its recognition that a reputation can be slandered through the Internet in the same way that it can be damaged in the real world.⁹

A key characteristic of online speech is its potential to reach a wider number of people than speech uttered in the real world. The Internet

⁷ American Jurisprudence (Vol. 33, p. 292) explains that "Under the common-law theory, which is embodied in some of the statutory provisions on the subject, the criminality of a defamatory statement consist in the tendency thereof to provoke a breach of the peace," but, it adds, **"many of the modern enactments, ... ignore this aspect altogether and make a libelous publication criminal if its tendency is to injure the person defamed, regardless of its effect upon the public."**

The present Philippine law on libel conforms to this modern tendency. For a little digression on the present law of libel or defamation, let it be noted that the Revised Penal Code has absorbed libel under Act No. 277 and calumny and insult under the old Penal Code. (Commentaries on the Revised Penal Code, Guevarra, p. 764.) The new Penal Code includes "All kinds of attacks against honor and reputation, thereby eliminating once and for all the idle distinction between calumny, insult and libel." (Idem, p. 765.) *People v. del Rosario*, 86 Phil. 163, 165 – 166 (1950).

⁸ *Worcester v. Ocampo*, 22 Phil. 42, 73 – 74 (1912).

⁹ During the senate's deliberations on the cybercrime bill, Senator Sotto asked Senator Angara if the bill also addresses internet libel or internet defamation. Senator Angara answered that the bill includes it as a crime, an actionable offense, because one can be defamed through Twitter or social media.

To the comment that one's reputation can easily be ruined and damaged by posts and comments in social network sites, Senator Angara stated that under the proposed law, the offended party can sue the person responsible for posting such comments. Senate Journal, December 12, 2011, available at <http://www.gov.ph/2012/10/03/for-the-record-public-records-of-senate-deliberations-on-the-cybercrime-prevention-bill/>

empowers persons, both public and private, to reach a wider audience – a phenomenon some legal scholars pertain to as “cyber-reach.”¹⁰ Cyber-reach increases the number of people who would have knowledge of a defamatory statement – a post published by a person living in the Philippines, for instance, can reach millions of people living in the United States, and *vice versa*. It could thus be argued that an increase in the audience of a libelous statement made online justifies the inhibitive effect of Section 5, 6, and 7 on online speech.

I find this proposition to be flawed. Online speech has varying characteristics, depending on the platform of communications used in the Internet. It does not necessarily mean, for instance, that a libelous speech has reached the public or a wider audience just because it was communicated through the Internet. A libelous statement could have been published through an e-mail, or through a private online group, or through a public website – each with varying degrees in the number of people reached.

I also find it notable that the publicity element of libel in the Revised Penal Code does not take into consideration the amount of audience reached by the defamatory statement. For libel prosecution purposes, a defamatory statement is considered published when a third person, other than the speaker or the person defamed, is informed of it.¹¹ Libelous speech may be penalized when, for instance, it reaches a third person by mail,¹² or through a television program,¹³ or through a newspaper article published nationwide.¹⁴ All these defamatory imputations are punishable with the same penalty of *prision correccional* in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos or both.¹⁵

Penalizing libelous speech committed through the Internet with graver penalties and repercussions because it allegedly reaches a wider audience creates an unreasonable classification between communications made through the Internet and in the real, physical world, to the detriment of online speech. I find no basis to treat online speech and speech in the real

¹⁰ One of the most striking aspects of cyberspace is that it "provides an easy and inexpensive way for a speaker to reach a large audience, potentially of millions." n1 This characteristic sharply contrasts with traditional forms of mass communication, such as television, radio, newspapers, and magazines, which require significant start-up and operating costs and therefore tend to concentrate communications power in a limited number of hands. Anyone with access to the Internet, however, can communicate and interact with a vast and rapidly expanding cyberspace audience. n2 As the Supreme Court opined in its recent landmark decision, *Reno v. ACLU*, n3 the Internet enables any person with a phone line to "become a pamphleteer" or "a town crier with a voice that resonates farther than it could from any soapbox." n4 Indeed, the Internet is "a unique and wholly new medium of worldwide human communication" n5 that contains content "as diverse as human thought." n6

The term "cyber-reach" can be used to describe cyberspace's ability to extend the reach of an individual's voice. Cyber-reach makes the Internet unique, accounts for much of its explosive growth and popularity, and perhaps holds the promise of a true and meaningful "free trade in ideas" that Justice Holmes imagined eighty years ago. Bill Mcswain, *Developments in the Law - The Long Arm of Cyber-reach*, 112 Harv. L. Rev. 1610 (1998).

¹¹ *Alcantara v. Ponce*, 545 Phil. 678, 683 (2007).

¹² *US v. Grino*, 36 Phil. 738 (1917); *People v. Silvela*, 103 Phil. 773 (1958).

¹³ *People v. Casten*, CA-G.R. No. 07924-CR, December 13, 1974.

¹⁴ *Fermin v. People of the Philippines*, 573 Phil. 12 (2008).

¹⁵ Article 355 of the Revised Penal Code

world differently on account of the former's cyber-reach because Article 355 of the Revised Penal Code does not treat libel committed through various forms of media differently on account of the varying numbers of people they reach.

In other words, since Article 355 of the Revised Penal Code does not distinguish among the means of communications by which libel is published, the Cybercrime Law, which merely adds a medium of communications by which libel may be committed, should also not distinguish and command a different treatment than libel in the real world.

Notably, the enumeration of media in Article 355 of the Revised Penal Code have for their common characteristic, not the audience a libelous statement reaches, but their permanent nature as a means of publication.¹⁶ Thus, cyber-libel's addition of communications through the Internet in the enumeration of media by which libel may be committed is a recognition that it shares this common characteristic of the media enumerated in Article 355 of the RPC, and that its nature as a permanent means of publication injures private reputation in the same manner as the enumeration in Article 355 does.

Neither should the ease of publishing a libelous material in the Internet be a consideration in increasing the penalty for cyber-libel. The ease by which a libelous material may be published in the Internet, to me, is counterbalanced by the ease through which a defamed person may defend his reputation in the various platforms provided by the Internet - a means not normally given in other forms of media.

Thus, I agree with the *ponencia* that **Section 5¹⁷ of the Cybercrime Law**, which penalizes aiding, abetting, or attempting to commit any of the cybercrimes enumerated therein, is unconstitutional in so far as it applies to the crime of cyber-libel. As the *ponente* does, I believe that the provision, when applied to cyber-libel, is *vague* and can have a chilling effect on otherwise legitimately free speech in cyberspace.

I further agree with the Chief Justice's argument that it would be constitutionally improper to apply the higher penalty that **Section 6** imposes to libel.

Section 6¹⁸ qualifies the crimes under the Revised Penal Code and special laws when committed by, through and with the use of information

¹⁶ *People v. Santiago*, G.R. No. L-17663, May 30, 1962, 5 SCRA 231, 233 – 234.

¹⁷ Section 5. Other Offenses. — The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of Cybercrime. – Any person who wilfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) Attempt in the Commission of Cybercrime. — Any person who wilfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

¹⁸ Section 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be

and communications technologies, and considers ICT use as an aggravating circumstance that raises the appropriate penalties one degree higher. As Chief Justice Sereno points out, Section 6 not only considers ICT use to be a qualifying aggravating circumstance, but also has the following effects: *first*, it increases the accessory penalties of libel; *second*, it disqualifies the offender from availing of the privilege of probation; *third*, it increases the prescriptive period for the crime of libel from one year to fifteen years, and the prescriptive period for its penalty from ten years to fifteen years; and *fourth*, its impact cannot be offset by mitigating circumstances.

These effects, taken together, unduly burden the freedom of speech because the inhibiting effect of the crime of libel is magnified beyond what is necessary to prevent its commission.

I also agree with Justice Carpio that the application of **Section 7** to cyberlibel should be declared unconstitutional. By adopting the definition of libel in the Revised Penal Code, Section 4(c)(4)'s definition of cyberlibel penalizes the same crime, except that it is committed through another medium enumerated in Article 355. Thus, Section 7 exposes a person accused of uttering a defamatory statement to multiple prosecutions under the Cybercrime Law and the Revised Penal Code for the same utterance. This creates a significant chill on online speech, because the gravity of the penalties involved could possibly compel Internet users towards self-censorship, and deter otherwise lawful speech.

B.3. Article 354 of the Revised Penal Code

Lastly, I join in Justice Carpio's call for the Court to declare Article 354 of the Revised Penal Code as unconstitutional in so far as it applies to public officers and figures.

The petitions against the Cybercrime Law provide us with the opportunity to clarify, once and for all, the prevailing doctrine on libel committed against public officers and figures. The possibility of applying the presumed malice rule against this kind of libel hangs like a Damocles sword against the actual malice rule that jurisprudence established for the prosecution of libel committed against public officers and figures.

The presumed malice rule embodied in Article 354¹⁹ of the Revised Penal Code provides a presumption of malice in every defamatory

covered by the relevant provisions of this Act: Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

¹⁹ Art. 354. Requirement for publicity. — Every defamatory imputation is presumed to be malicious, even if it be true, if no good intention and justifiable motive for making it is shown, except in the following cases:

1. A private communication made by any person to another in the performance of any legal, moral or social duty; and
2. A fair and true report, made in good faith, without any comments or remarks, of any judicial, legislative or other official proceedings which are not of confidential nature, or of any statement, report or speech

imputation, except under certain instances. Under this rule, the defamatory statement would still be considered as malicious even if it were true, unless the accused proves that it was made with good and justifiable intentions.

Recognizing the importance of freedom of speech in a democratic republic, our jurisprudence has carved out another exception to Article 354 of the Revised Penal Code. Through cases such as *Guinguing v. Court of Appeals*²⁰ and *Borjal v. Court of Appeals*,²¹ the Court has applied the actual malice rule in libel committed against public officers and figures. This means that *malice in fact is necessary* for libel committed against public officers and figures to prosper, *i.e.*, it must be proven that the offender made the defamatory statement with the knowledge that it is false or *with reckless disregard of whether it is false or not*. As the Court held in *Guinguing*, adopting the words in *New York Times v. Sullivan*.²²: “[w]e have adopted the principle that debate on public issues should be uninhibited, robust, and wide open and that it may well include vehement, caustic and sometimes unpleasantly sharp attacks on government and public officials.”

I agree with Justice Carpio’s point regarding the necessity of a concrete declaration from the Court regarding Article 354’s unconstitutional application to libelous speech against public officers and officials. To neglect our duty to clarify what the law would amount to and leave a gap in the implementation of our laws on libel, in the words of Justice Carpio, would “leave[s] fundamental rights of citizens to freedom of expression to the mercy of the Executive’s prosecutorial arm whose decision to press charges depends on its own interpretation of the penal provision’s adherence to the Bill of Rights.”

This need for a clear signal from the Court has become even more pronounced given the current nature of the Internet – now a vibrant avenue for dialogue and discussion on matters involving governance and other public issues, with the capacity to allow ordinary citizens to voice out their concerns to both the government and to the public in general.

B.4. Summation of Constitutionality of Section 4(c)(4)

With the four provisions – *i.e.*, **Section 5**, **Section 6** and **Section 7** of the **Cybercrime Law** and **Article 354 of the Revised Penal Code**, *removed* from cyber-libel, Section 4(c)(4) would present a proper balance between encouraging freedom of expression and preventing the damage to the reputation of members of society. Conversely, the presence of either one of these three provisions could tilt this delicate balance against freedom of expression, and unduly burden the exercise of our fundamental right. Thus, *hand in hand with the recognition of the constitutionality of Section*

delivered in said proceedings, or of any other act performed by public officers in the exercise of their functions.

²⁰ 508 Phil. 193 (2005).

²¹ 361 Phil. 3 (1999).

²² 376 US 254.

4(c)(4) of the Cybercrime Law under a facial challenge, the four mentioned provisions should likewise be struck down as unconstitutional.

C. My Positions on Section 12 of the Cybercrime Law

In agreeing with the *ponencia*'s conclusion regarding the unconstitutionality of Section 12, I begin by emphasizing the point that no ***all-encompassing constitutional right to privacy exists in traffic data***. I stress the need to be sensitive and discerning in appreciating traffic data as we cannot gloss over the distinctions between content data and traffic data, if only because of the importance of these distinctions for law enforcement purposes.

The right to privacy over the ***content*** of internet communications is a given, as recognized in many jurisdictions.²³ ***Traffic data*** should likewise be recognized for what they are – information necessary for computer and communication use and, in this sense, are practically ***open and freely-disclosed information that law enforcers may examine***.

²³ 209. The type of data that can be collected is of two types: traffic data and content data. 'Traffic data' is defined in Article 1 d to mean any computer data relating to a communication made by means of a computer system, which is generated by the computer system and which formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size and duration or the type of service. 'Content data' is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).

210. In many States, a distinction is made between the real-time interception of content data and real-time collection of traffic data in terms of both the legal prerequisites required to authorize such investigative measure and the offences in respect of which this measure can be employed. ***While recognizing that both types of data may have associated privacy interests, many States consider that the privacy interests in respect of content data are greater due to the nature of the communication content or message.*** Greater limitations may be imposed with respect to the real-time collection of content data than traffic data. To assist in recognizing this distinction for these States, the Convention, while operationally acknowledging that the data is collected or recorded in both situations, refers normatively in the titles of the articles to the collection of traffic data as 'real-time collection' and the collection of content data as 'real-time interception'.

xxx

215. The conditions and safeguards regarding the powers and procedures related to real-time interception of content data and real-time collection of traffic data are subject to Articles 14 and 15. ***As interception of content data is a very intrusive measure on private life, stringent safeguards are required to ensure an appropriate balance between the interests of justice and the fundamental rights of the individual.*** In the area of interception, the present Convention itself does not set out specific safeguards other than limiting authorisation of interception of content data to investigations into serious criminal offences as defined in domestic law. Nevertheless, the following important conditions and safeguards in this area, applied in domestic laws, are: judicial or other independent supervision; specificity as to the communications or persons to be intercepted; necessity, subsidiarity and proportionality (e.g. legal predicates justifying the taking of the measure; other less intrusive measures not effective); limitation on the duration of interception; right of redress. Many of these safeguards reflect the European Convention on Human Rights and its subsequent case-law (see judgements in Klass (5), Kruslin (6), Huvig (7), Malone (8), Halford (9), Lambert (10) cases). Some of these safeguards are applicable also to the collection of traffic data in real-time.

Explanatory Report on the Budapest Convention on Cybercrime, [2001] COETSER 8 (November 23, 2001), available at <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

But beyond all these are *information generated from raw traffic data* on people's activities in the Internet, that are collected through real-time extended surveillance and which may be as private and confidential as content data. To my mind, the grant to law enforcement agents of the authority to access these data require a very close and discerning examination to determine the grant's constitutionality.

I justify my position on the unconstitutionality of Section 12 as it *patently lacks proper standards* guaranteeing the protection of data that should be constitutionally-protected. In more concrete terms, *Section 12 should not be allowed – based solely on law enforcement agents' finding of 'due cause' – to serve as authority for the warrantless real-time collection and recording of traffic data.*

Lastly, I clarify that the nullification of Section 12 does not absolutely bar the real-time collection of traffic data, as such collection can be undertaken upon proper application for a judicial warrant. Neither should my recommended approach in finding the unconstitutionality of Section 12 prevent Congress, by subsequent legislation, from authorizing the conduct of warrantless real-time collection of traffic data provided that proper constitutional safeguards are in place for the protection of affected constitutional rights.

C.1 *The constitutional right to privacy in Internet communications data*

The right to privacy essentially means the right to be let alone and to be free from unwarranted government intrusion.²⁴ To determine whether a violation of this right exists, a first requirement is to ascertain the existence of a reasonable expectation of privacy that the government violates. The *reasonable expectation of privacy* can be made through a two-pronged test that asks: (1) whether, by his conduct, the individual has exhibited an expectation of privacy; and (2) whether this expectation is one that society recognizes as reasonable. Customs, community norms, and practices may, therefore, limit or extend an individual's "reasonable expectation of privacy."²⁵ The awareness of the need for privacy or confidentiality is the critical point that should dictate whether privacy rights exist.

The finding that privacy rights exist, however, is not a recognition that the data shall be considered absolutely private;²⁶ the recognition must yield

²⁴ *Morfe v. Mutuc*, 130 Phil. 415, 436 (1968).

²⁵ *Ople v. Torres*, 354 Phil. 948, 970 (1998).

²⁶ See, for instance, the following cases where the Court upheld the governmental action over the right to privacy: *Kilusang Mayo Uno v. NEDA*, 521 Phil. 732 (2006) (regarding the validity of Executive Order No. 420, which established the unified multi-purpose identification (ID) system for government); *Standard Chartered Bank v. Senate Committee on Banks*, 565 Phil. 744 (2007) (regarding the Senate's resolution compelling petitioners who are officers of petitioner SCB-Philippines to attend and testify before any further hearing to be conducted by the Senate); *Gamboa v. Chan*, G.R. No. 193636, July 24, 2012, 677

when faced with a compelling and fully demonstrated state interest that must be given primacy. In this exceptional situation, the balance undeniably tilts in favor of government access or intrusion into private information. Even then, however, established jurisprudence still requires safeguards to protect privacy rights: the law or rule allowing access or intrusion must be so narrowly drawn to ensure that other constitutionally-protected rights outside the ambit of the overriding state interests are fully protected.²⁷

The majority of the Court in *Ople v. Torres*,²⁸ for instance, found the repercussions and possibilities of using biometrics and computer technologies in establishing a National Computerized Identification Reference System to be too invasive to allow Section 4 of Administrative No. 308 (the assailed regulation which established the ID system) to pass constitutional muster. According to the majority, the lack of sufficient standards in Section 4 renders it vague and overly broad, and in so doing, was not narrowly fitted to accomplish the state's objective. Thus, it was unconstitutional for failing to ensure the protection of other constitutionally-protected privacy rights.

Other governmental actions that had been declared to be constitutionally infirm for failing the compelling state interest test discussed above include the city ordinance barring the operation of motels and inns within the Ermita-Malate area in *City of Manila v. Laguio Jr.*,²⁹ and the city ordinance prohibiting motels and inns from offering short-time admission and pro-rated or "wash up" rates in *White Light Corporation v. City of Manila*.³⁰ In both cases, the Court found that the city ordinance overreached and violated the right to privacy of motel patrons, both single and married.

C.2 *Traffic and Content Data*

The Internet serves as a useful technology as it facilitates communication between people through the application programs they use. More precisely, the Internet is "*an electronic communications network that connects computer networks and organizational computer facilities around the world.*"³¹ These connections result in various activities online, such as

SCRA 385, 395 – 399 (regarding the Regional Trial Court of Laoag's decision denying the petitioner's petition for the privilege of the writ of habeas data).

²⁷ See, for instance, the following cases where the Court nullified governmental actions and upheld the right to privacy: *City of Manila v. Laguio Jr.*, 495 Phil. 289, 317 – 319 (2005) (regarding a city ordinance barring the operation of motels and inns, among other establishments, within the Ermita-Malate area); *Social Justice Society v. Dangerous Drugs Board*, 591 Phil. 393, 413 – 417 (2008) (regarding mandatory drug-testing for of candidates for public office and persons charged with a crime having an impossible penalty of imprisonment of not less than six (6) years and one (1) day before the prosecutor's office); *White Light Corporation v. City of Manila*, 596 Phil. 444, 464 – 467 (2009) (regarding a city ordinance prohibiting motels and inns from offering short-time admission, as well as pro-rated or "wash up" rates).

²⁸ *Ople v. Torres*, 354 Phil. 948, 970 (1998).

²⁹ *City of Manila v. Laguio Jr.*, 495 Phil. 289 (2005).

³⁰ *White Light Corporation v. City of Manila*, 596 Phil. 444 (2009).

³¹ Internet definition, Merriam Webster Online Dictionary, <http://www.merriam-webster.com/dictionary/internet>

simple e-mails between people, watching and downloading of videos, making and taking phone calls, and other similar activities, done through the medium of various devices such as computers, laptops, tablets and mobile phones.³²

Traffic data refer to the computer data generated by computers in communicating to each other to indicate a communication's origin, destination, route, time, date, size, duration or type of underlying service.³³ These data should be distinguished from **content data** which contain the body or message of the communications sent.³⁴ Traffic data do not usually indicate on their face the actual identity of the sender of the communication; the content data, on the other hand, usually contain the identity of sender and recipient and the actual communication between them.

It must also be appreciated that as the technology now exists, data (both traffic and content) are usually sent through the Internet through a packet-switching network. The system first breaks down the materials sent into tiny **packets of data** which then pass *through different networks* until they reach their destination where they are reassembled into the **original** data sent.

These tiny packets of data generally contain a header and a payload. The **header** contains the overhead information about the packet, the service and other transmission-related information. It includes the source and destination of the data, the sequence number of the packets, and the type of service, among others. The **payload**, on the other hand, contains the actual data carried by the packet.³⁵ Traffic data may be monitored, recorded and collected from the headers of packets.³⁶

I hold the view, based on the above distinctions and as the *ponencia* did, that no reasonable expectation of privacy exists in traffic data *as they appear in the header*, as these are data generated in the course of communications between or among the participating computers or devices and intermediary networks. The absence of any expectation is based on the

³² As the technology exists now, data is usually sent through the Internet through a packet-switching network. Under this system, data sent through the Internet is first broken down into tiny packets of data which pass through different networks until it reaches its destination, where it is reassembled into the data sent. These tiny packets of data generally contain a header and a payload. The header keeps overhead information about the packet, the service and other transmission-related information. This includes the source and destination of the data, the sequence number of the packets, and the type of service, among others. The payload, on the other hand, is the actual data carried by the packet. Traffic data may be monitored, recorded and collected from the headers of packets.

³³ Chapter 1, Article 1 (d) of the Cybercrime Convention; see also Section 3 (p) of Republic Act No. 10175.

³⁴ Chapter 1, Article 1 (b) of the Cybercrime Convention

³⁵ *What is a packet?*, HowStuffWorks.com (Dec. 01, 2000) <http://computer.howstuffworks.com/question525.htm> See also: *Structure of the Internet: Packet switching*, in A-level Computing/AQA, http://en.wikibooks.org/wiki/A-level_Computing/AQA/Computer_Components_The_Stored_Program_Concept_and_the_Internet/Structure_of_the_Internet/Packet_switching; and *What is Packet Switching?*, Teach-ICT.com, http://www.teach-ict.com/technology_explained/packet_switching/packet_switching.html.

³⁶ Edward J. Wegman and David J. Marchette, *On Some Techniques for Streaming Data: A Case Study of Internet Packet Headers*, p.7, <http://www.dmarchette.com/Papers/VisPacketHeadersRev1.pdf>.

reality that the traffic data: are open as they pass through different unknown networks;³⁷ cannot be expected to be private as they transit on the way to their intended destination; and are necessarily identified as they pass from network to network. In contrast, the content data they contain remain closed and undisclosed, and do not have to be opened at all in order to be transmitted. The unauthorized opening of the content data is in fact a crime penalized under the Cybercrime Law.³⁸

For a clearer analogy, traffic data can be likened to the address that a person sending an ordinary mail would provide in the mailing envelope, while the size of the communication may be compared to the size of the envelope or package mailed through the post office. There can be no reasonable expectation of the privacy in the address appearing in the envelope and in the size of the package as it is sent through a public network of intermediary post offices; they must necessarily be read in these intermediary locations for the mail to reach its destination.

A closer comparison can be drawn from the number dialed in using a telephone, a situation that the US Supreme Court had the opportunity to pass upon in *Smith v. Maryland*³⁹ when it considered the constitutionality of the Pen Register Act.⁴⁰ The US Court held that the Act does not violate the Fourth Amendment (the right to privacy) because no search is involved; there could be no reasonable expectation of privacy in the telephone numbers that a person dials. All telephone users realize that they must “convey” phone numbers to the telephone company whose switching equipment serve as medium for the completion of telephone calls.

As in the case of the regular mail and the use of numbers in communicating by telephone, privacy cannot be reasonably expected from traffic data *per se*, because their basic nature – data generated in the course

³⁷ 167. Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination. Explanatory Report on the Budapest Convention on Cybercrime, [2001] COETSER 8 (Nov. 23, 2001), available at <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

³⁸ A law enforcement agent’s unauthorized access to content data may constitute illegal interception, which is penalized by Section 4, paragraph 2 of the Cybercrime Law:

(2) Illegal Interception. – The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

³⁹ 442 U.S. 735 (1979).

⁴⁰ In *Smith v. Maryland* 442 U.S. 735 (1979), the petitioner had been charged with robbery, and prior to his trial, moved that the evidence acquired by the police through the installation of a pen register at a telephone company’s central offices. This allowed the police to record the numbers dialed from the telephone at the petitioner’s home. The US Supreme Court eventually held that this act did not violate the petitioner’s right to privacy, as it does not constitute a search. The petitioner did not entertain an actual, legitimate and reasonable expectation of privacy to the phone numbers he dialed.

of sending communications from a computer as communications pass through a public network of intermediate computers.

To complete the comparison between transfer data and content data, an individual sending an e-mail through the Internet would expect at least the same level of privacy in his email's content as that enjoyed by the mail sent through the post office or in what is said during a telephone conversation. Expectations regarding the confidentiality of emails may in fact be higher since their actual recipients are not identified by their actual names but by their email addresses, in contrast with regular mails where the addresses in the envelopes identify the actual intended recipients and are open to the intermediary post offices through which they pass.

At the same level of privacy are the information that an Internet subscriber furnishes the Internet provider. These are also private data that current data privacy laws⁴¹ require to be accurate under the guarantee that the provider would keep them secure, protected, and for use only for the purpose for which they have been collected.

For instance, a customer buying goods from a website used as a medium for purchase or exchange, can expect that the personal information he/she provides the website would only be used for facilitating the sales transaction.⁴² The service provider needs the customer's consent before it can disclose the provided information to others; otherwise, criminal and civil liability can result.⁴³ This should be a reminder to service providers and

⁴¹ In the Philippines, data privacy is governed by Republic Act 10173 or The Data Privacy Act of 2012. RA 10173 established the country's data privacy framework. It recognizes the individual's rights to his personal information and sensitive information, and fines the unlawful processing of these kinds of information and the violation of the rights of a data subject.

⁴² Section 16 of the Data Privacy Act provides:

Section 16. Rights of the Data Subject. – The data subject is entitled to:

(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;

xxxx

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

⁴³ Section 31 and 32 of the Data Privacy Act provide:

Section 31. Malicious Disclosure. – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

Section 32. Unauthorized Disclosure. – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject

their staff who sell telephone numbers and addresses to commercial companies for their advertising mailing lists.

Notably, social networking websites allow its subscribers to determine who would view the information the subscribers provide, *i.e.*, whether the information may be viewed by the public in general, or by a particular group of persons, or only by the subscriber.⁴⁴ Like the contents of Internet communications, the user and the public in general expect these information to be private and confidential.

In the context of the present case where the right to privacy is pitted against government intrusion made in the name of public interest, the intrinsic nature of traffic data should be fully understood and appreciated because a miscalibration may carry profound impact on one or the other.

In concrete terms, casting a net of protection wider than what is necessary to protect the right to privacy in the Internet can unduly hinder law enforcement efforts in combating cybercrime. Raw traffic data raise no expectation of privacy and should not be beyond the reach of law enforcers. At the opposite end, constitutionally allowing the unregulated inspection of Section 12 may unwittingly allow government access or intrusion into data greater than what the public recognizes or would allow, resulting in the violation of privacy rights.

A miscalibration may immediately affect congressional action addressing the balancing between the privacy rights of individuals and investigative police action. The recognition of the right to privacy over raw traffic data may curtail congressional action by practically requiring Congress to increase the required governmental interest not only for the real-time surveillance and collection of traffic data, but also for simple police investigative work. The effect would of course be most felt at the level of field law enforcement where officers would be required to secure a higher level of compelling governmental interest simply to look at raw traffic data even on a non-surveillance situation. Using the above email analogy, it may amount to requiring probable cause to authorize law enforcement to look at an address in a mailing envelope coursed through the public post office.

to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

⁴⁴ Mindi McDowell, *Staying Safe on Social Network Sites*, US-CERT, (Feb. 6, 2013) <http://www.us-cert.gov/ncas/tips/ST06-003>; See Adam Tanner, *Users more savvy about social media privacy than thought, poll says*, Forbes Magazine, (Nov. 11, 2013) <http://www.forbes.com/sites/adamtanner/2013/11/13/users-more-savvy-about-social-media-privacy-than-thought-poll-finds/>.

Not to be forgotten is the reality that information and communication technology – particularly on the transmission, monitoring and encryption of data – is continuously evolving with no foreseeable end in sight. In the words of Justice Scalia in *Kyllo v. United States*,⁴⁵ a case pitting the right to privacy with the law enforcement’s use of thermal imaging devices: “the rule we adopt must take account of more sophisticated systems that are already in use or in development.”⁴⁶

This Court, made aware of this reality, must similarly proceed with caution in exercising its duty to examine whether a law involving the regulation of computers and cyber communications transgresses the Constitution. If we must err, we should do so in favor of slow and carefully calibrated steps, keeping in mind the possible and foreseeable impact of our decisions on future technology scenarios and on our jurisprudence. After all, our constitutionally-designed role is merely to interpret policy as expressed in the law and rules, not to create policy.

***C.3 Data collected from Online Activities –
the midway point between traffic data
and content data.***

While traffic data can practically be considered as disclosed (and consequently, open and non-confidential) data, they can – ***once collected and recorded over a period of time, or when used with other technologies*** – reveal information that the sender and even the general public expect to be private and confidential.

This potential use of raw traffic data serves as the limit for the analogy between traffic data and the addresses found in envelopes of regular mails. Mailed letters exist in the physical world and, unless coursed through one central post office, can hardly be monitored for a recognizable pattern of activities that can yield significant data about the writer or the recipient.

In contrast, the Internet allows the real-time sending and receiving of information at any given time, to multiple recipients who may be sending and receiving their own information as well. This capability and the large amount of traffic that ensues in real time open wide windows of opportunity for analysis of the ensuing traffic for trends and patterns that reveal information beyond the originally collected and recorded raw traffic data. For example, the analysis may provide leads or even specifically disclose the actual geographical location of the sender or recipient of the information, his online activity, the websites he is currently browsing, and even possibly the content of the information itself.

⁴⁵ 533 U.S. 27 (2001).

⁴⁶ 533 U.S. 27, 37 (2001).

It is at this point that the originally raw traffic data mass cross over and partake of the nature of content data that both the individual and the public expect to be private. Evidently, privacy interests arise, not from the raw data themselves, but from the resulting conclusions that their collection and recording yield. Thus, violation of any existing constitutional right starts at this point. From the point of view of effective constitutional protection, the trigger is not at the point of the private information end result, but at the point of real-time collection and recording of data that, over time and with analysis, yield private and confidential end result. In other words, it is at the earliest point that safeguards must be in place.

That this aspect of Internet use may no longer simply be an awaited potential but is already a reality now with us, can be discerned from what computer pundits say about the application of proper traffic analysis techniques to the traffic data of phone calls conducted through the Internet (also known as Voice Over Internet Protocol or VOIP). They claim that this analysis can reveal the language spoken and the identity of the speaker, and may even be used to reconstruct the actual words spoken during the phone conversation.⁴⁷ Others, on the other hand, have tested the possibility of inferring a person's online activities for short periods of time through traffic data analysis.⁴⁸

Recent developments in the Internet, such as the rise of Big Data⁴⁹ and the Internet of Things,⁵⁰ also serve as evidence of the realization of these possibilities, as people share more and more information on how they conduct their daily activities in the Internet and on how these information are used to perform other tasks. Right now, wireless signal strength in multiple monitoring locations may be used to accurately estimate a user's location and motion behind walls.⁵¹ With the advent of the Internet of

⁴⁷ Riccardo Bettatti, *Traffic Analysis and its Capabilities*, (Sept. 10, 2008) http://usacac.army.mil/cac2/cew/repository/papers/Modern_Traffic_Analysis_and_its_Capabilities.pdf; Fan Zhang, Wenbo He, Xue Liu and Patrick Bridges, *Inferring Users' Online Activities Through Traffic Analysis* (June 2011) <http://www.math.unipd.it/~conti/teaching/CNS1213/atpapers/Profiling/profiling.pdf> citing C.V. Wright, L. Ballard, F. Monrose, and G. M. Masson, *Language identification of encrypted VoIP traffic: Alejandra y roberto or alice and bob* in Proceedings of USENIX Security Symposium, 2007 and C.V. Wright, L. Ballard, S. E. Coull, F. Monrose, and G. M. Masson, *Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations*, In Proceedings of IEEE Symposium on Security and Privacy, 2008.

⁴⁸ Fan Zhang, Wenbo He, Xue Liu and Patrick Bridges, *Inferring Users' Online Activities Through Traffic Analysis* (June 2011) <http://www.math.unipd.it/~conti/teaching/CNS1213/atpapers/Profiling/profiling.pdf>.

⁴⁹ See: James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers, *Big data: The next frontier for innovation, competition, and productivity*, Mckinsey Global Institute, (May 2011) http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

⁵⁰ More objects are becoming embedded with sensors and gaining the ability to communicate. The resulting information networks promise to create new business models, improve business processes, and reduce costs and risks. Michael Chui, Markus Löffler, and Roger Roberts, *The Internet of Things*, Mckinsey Global Institute, (March 2010) http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things.

⁵¹ Fan Zhang, Wenbo He, Xue Liu and Patrick Bridges, *Inferring Users' Online Activities Through Traffic Analysis* (June 2011) <http://www.math.unipd.it/~conti/teaching/CNS1213/atpapers/Profiling/profiling.pdf> citing T. Jiang, H.J. Wang, and Y. Hu. *Preserving location privacy in wireless LANs* In Proceedings of MobiSys, pages 246–257, 2007 and J. Wilson and N. Patwari, *See through walls: Motion tracking using variance-based radio tomography networks*, IEEE Transactions on Mobile Computing, 2010.

Things, which equips devices with sensors that allow the direct gathering of information in the physical world for transmission to the Internet, even seemingly innocuous traffic data, when collected, may possibly reveal even personal and intimate details about a person and his activities.

Thus, I believe it indisputable that information gathered from purposively collected and analyzed raw traffic data, now disclose information that the Internet user *never intended to reveal when he used the Internet*. These include the language used in a phone conversation in the Internet, the identity of the speaker, the content of the actual conversation, as well as a person's exact location inside his home. From this perspective, these data, as collected and/or analyzed from online activities, are no different from content data and should likewise be protected by the right to privacy.

C.4 Deficiencies of Section 12

Section 12 of the Cybercrime Law authorizes law enforcement agents to collect and record in real-time traffic data associated with specified communications, under the following terms:

Section 12. Real-Time Collection of Traffic Data. — Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

Traffic data refer only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.

All other data to be collected or seized or disclosed will require a court warrant.

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed; (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

I have no doubt that the state interest that this section seeks to protect is a compelling one. This can be gleaned from Section 2 of the Cybercrime Law which clearly sets out the law's objective – to equip the State with

sufficient powers to prevent and combat cybercrime. The means or tools to this objective, Section 12 among them, would enable our law enforcers to investigate incidences of cybercrime, and apprehend and prosecute cybercriminals. According to the Department of Justice, nearly nine out of ten Filipino Internet users had been victims of crimes and malicious activities committed online. Contrast this to the mere 2,778 cases of computer crimes referred to the Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group (CIDG) of the Philippine National Police (PNP) from 2003 to 2012,⁵² to get a picture of just how vulnerable the citizenry is to computer-related crimes.

But bad might the situation be and as already mentioned in passing above, a demonstrated and compelling state interest effectively serves only as starting point and basis for the authority to grant collection and recording authority to state agents faced with clearly established right to privacy. In addition to and as equally important as the invoked compelling state interest, is the requirement that the authorizing law or rule must provide safeguards to ensure that no unwarranted intrusion would take place to lay open the information or activities not covered by the state interest involved; the law or rule must be narrowly drawn to confine access to what the proven state interests require.

I submit that, on its face, Section 12 fails to satisfy this latter constitutional requirement. In Section 12 terms, its “due cause” requirement does not suffice as the safeguard that the Constitution requires.

My examination of Section 12 shows that it properly deals with the various types of data that computer communication generates, *i.e.*, with traffic data *per se*, with data other than the defined traffic data (thus, of content data), and with the real-time collection of these data over time. The law, however, is wanting on the required safeguards when private data are accessed.

True, traffic data *per se* does not require any safeguard or measure stricter than the “due cause” that the law already requires, while content data can be accessed only on the basis of a judicial warrant. The real time collection and recording of traffic data and its “due cause” basis, however, suffer from fatal flaws.

The law’s “due cause” standard is vague in terms of the substance of what is “due cause” and the procedure to be followed in determining the required “cause”. The law is likewise overly broad so that real-time monitoring of traffic data can effectively overreach its allowable coverage and encroach into the realm of constitutionally-protected activities of Internet users, specifically, data that a cybercrime may not even address.

⁵² Department of Justice Primer on Cybercrime, available at <http://www.upm.edu.ph/downloads/announcement/DOJ%20Primer%20on%20Cybercrime%20Law.pdf>; see also “Quashing Cybercrime,” Senator Edgardo Angara’s sponsorship speech on the Cybercrime Prevention Act (May 11, 2011) http://www.senate.gov.ph/press_release/2011/0511_angara3.asp

Consider, in this regard, that as worded, law enforcement agents, *i.e.*, members of the National Bureau Investigation (NBI) and the Philippine National Police (PNP),⁵³ practically have *carte blanche* authority to conduct the real-time collection and recording of traffic data at anytime and on any Internet user, given that the law does not specifically define or give the parameters of the purpose for which law enforcement authorities are authorized to conduct these intrusive activities. Without sufficient guiding standards, the “due cause” basis in effect allows law enforcement agents to monitor all traffic data. This approach, to my mind, may even allow law enforcement to conduct constitutionally-prohibited fishing expeditions for violations and their supporting evidence.

Additionally, while Section 2 empowers the State to adopt sufficient powers to conduct *the detection, investigation and prosecution* of cybercrime as an expressed policy, Section 12, however, does not provide a standard sufficient to render enforcement rules certain or determinable; it also fails to provide guiding particulars on the real-time monitoring of traffic data. Assuming that the Cybercrime Law contemplates that real-time collection of traffic data would assist in criminal investigations, the provision does not provide any specified or determinable trigger for this activity -- should collection and recording be connected with criminal investigation in general? Is it necessary that a cybercrime has already been committed, or could it be used to prevent its commission? Would it only apply to investigations on cybercrime, or would it include investigations on crimes in the physical world whose aspects have seeped into the Internet?

In the absence of standards, guidelines or clean definitions, the ‘due cause’ requirement of Section 12 fatally opens itself to being vague as it does not even provide the context in which it should be used. It merely provides that the real-time monitoring would be related to ‘specified communications’ without mentioning as to what these communications pertain to, how these communications will be specified, and as well as the extent of the specificity of the communications.

Section 12 likewise does not provide for the extent and depth of the real-time collection and recording of traffic data. It does not limit the length of time law enforcement agents may conduct real-time monitoring and recording of traffic data, as well as the allowable contours by which a specified communication may be monitored and recorded. In other words, it does not state how long the monitoring and recording of the traffic data connected to a specified communication could take place, how specific a specified communication should be, as well as the extent of the association allowable.

⁵³ Section 10 of the Cybercrime Law provides:

Section 10. Law Enforcement Authorities. — The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

The absolute lack of standards in the collection and recording of traffic data under Section 12 in effect negates the safeguards under Section 13 of the Cybercrime Law. Section 13 obligates internet service providers to collect and store traffic data for six months, which data law enforcement agents can only access based on a judicial order under Section 14. Properly understood, Section 13 is a recognition that traffic data once collected in depth and for a considerable period of time, would produce information that are private. But because Section 12 does not specify the length and extent of the real-time collection, monitoring and storage of traffic data, it in effect skirts the judicial warrant requirement before any data may be viewed under Section 13. The limitation in this section also does not also apply if the law enforcement agency has its own collection and recording facilities, a possibility that in these days is not farfetched.

Neither does Section 12 as worded sufficiently limit the information that would be collected and recorded in real-time only to traffic data. The lack of standards in Section 12 regarding the extent and conduct of the real-time collection and recording of traffic data effectively allows for its collection in bulk, which, as earlier pointed out, reveals information that are private. The lack of standards also does not prevent the possibility of using technologies that translates traffic data collected in real-time to content data or disclose a person's online activities.

Significantly, the Cybercrime Law's omissions in limiting the scope and conduct of the real-time collection and recording of traffic data cannot be saved by statutory construction; neither could it be filled-in by implementing rules and regulations. We can only construe what the law provides, harmonize its provisions and interpret its language. We cannot, no matter how noble the cause, add to what is not provided in the law.

The same limitation applies to law enforcement agents in the implementation of a law – assuming they have been delegated to provide for its rules and regulations. They cannot, in fixing the details of a law's implementation, legislate and add to the law that they seek to implement.

Given the importance of Section 12 in cybercrime prevention and its possible impact on the right to privacy, we cannot, in interpreting a law, usurp what is rightfully the Congress's duty and prerogative to ensure that the real-time collection of traffic data does not overreach into constitutionally-protected activities. In other words, it is Congress, through law, which should draw the limits of traffic data collection. Our duty in the Court comes only in determining whether these limits suffice to meet the principles enshrined in the Constitution.

In sum, as worded, the authorization for a warrantless real-time collection and recording of traffic data is not narrowly drawn to ensure that it would not encroach upon the privacy of Internet users online. Like A.O. No. 308 in *Ople v. Torres*, Section 12 of the Cybercrime threatens the right to privacy of our people, and should thus be struck down as unconstitutional.

**D. *Implications for law enforcement of
the unconstitutionality of Sec. 12***

The Court has, in addition to its constitutional duty to decide cases and correct jurisdictional errors, the duty to provide guidance to the bench and bar.⁵⁴ It is in consideration of this duty, as well as the pressing need for balance between the investigation and prosecution of cybercrimes and the right to privacy, that I discuss the repercussions of my proposed ruling on law enforcement.

The declaration of the unconstitutionality of Section 12 in the manner framed by the Court, should not tie the hands of Congress in enacting a replacement provision empowering the conduct of warrantless real-time collection of traffic data by law enforcement agents. This grant of power should of course avoid the infirmities of the present unconstitutional provision by providing for standards and safeguards to protect private data and activities from unwarranted intrusion.

I clarify as well that the unconstitutionality of Section 12 does not remove from the police the authority to undertake real-time collection and recording of traffic data as an investigation tool that law enforcement agents may avail of in the investigation and prosecution of criminal offenses, both for offenses involving cybercrime and ordinary crimes. Law enforcement agencies may still conduct these activities under their general powers, but with a prior judicial authorization in light of the nature of the data to be collected. To cite an example in today's current crime situation, this tool may effectively be *used against the drug menace* whose leadership has so far evaded arrest and whose operations continue despite police interdiction efforts.

Notably, Section 24 of Republic Act No. 6975 empowers the Philippine National Police to enforce all laws and ordinances relative to the protection of lives and properties; maintain peace and order and take all necessary steps to ensure public safety; investigate and prevent crimes, effect the arrest of criminal offenders, bring offenders to justice and assist in their prosecution; and to exercise the general powers to make arrest, search and seizure in accordance with the Constitution and pertinent laws.

Section 1 of Republic Act No. 157 as amended, on the other hand, mandates the National Bureau of Investigation to investigate crimes and other offenses against Philippine laws, assist, upon request, in the investigation or detection of crimes, and to establish and maintain an up-to-date scientific crime laboratory and to conduct researches in furtherance of scientific knowledge in criminal investigation.

⁵⁴ See for instance, *Fernandez v. Comelec*, 579 Phil. 235, 240 (2008) and *Villanueva v. Adre*, 254 Phil. 882, 887 (1989), where the Court declared a petition moot and academic, but proceeded to rule on the issue of jurisdiction for the guidance of the bench and the bar; or *Altres v. Empleo*, 594 Phil. 246, 261 – 262 (2008), where the Court restated in capsule form the jurisprudential pronouncements on forum-shopping; or *Republic v. CA and Molina*, 335 Phil. 664, 676 – 680 (1997), where the Court formulated guidelines in the interpretation and application of Art. 36 of the Family Code.

These laws sufficiently empower the PNP and the NBI to make use of up-to-date equipment in the investigation of crimes and in the apprehension and prosecution of criminals, including cybercriminals. The PNP is particularly empowered to undertake search and seizure under RA 6975. The need for a judicial warrant does not need be a stumbling block in these efforts in the sensitive area of Internet data, as the grant of warrant is merely a question of the existence of a probable cause, proven of course according to the requirements of the Constitution.

E. *The role of the courts in cybercrime prevention and prosecution*

Internet has significantly changed the way crimes are committed, and has paved the way for the emergence of new crimes committed in a totally different plane: from the previous real, physical world, to the abstract, borderless plane of interconnected computers linked through the Internet.

In the same manner that technology unleashed these new threats to security and peace, it also devised new means to detect, apprehend and prosecute those who threaten society. The Cybercrime Law is notable in its aim to penalize these new threats, and in giving clear signals and actually empowering our law enforcement agents in the investigation of these cybercrimes, in the apprehension of cybercriminals, and in the prosecution of cases against them.

In the same manner likewise that our laws and law enforcement have been adapting to the threats posed by cybercrime, we in the judiciary must also rise up to the challenge of competently performing our adjudicative functions in the cyber world.

The judicial steps in cybercrime prosecution start as early as the investigation of cybercrimes, through the issuance of warrants necessary for real-time collection of traffic data, as well as the issuance of the orders for the disclosure of data retained by internet service providers.⁵⁵ After these,

⁵⁵ Section 14 and 16 of the Cybercrime Law provides:

Section 14. Disclosure of Computer Data. — Law enforcement authorities, *upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control* within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

Section 16. Custody of Computer Data. — *All computer data, including content and traffic data, examined under a proper warrant* shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data. The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court. The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or then contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

courts also determine the probable cause for the arrest of suspects accused of committing cybercrimes. The suspect's arrest would then lead to a trial that, depending on the suspect's conviction or acquittal, could then go through the judiciary appellate process. During trial, pieces of evidence would be presented and testimonies heard, and trial courts would then exercise their constitutional duty to adjudicate the cases brought before them.

Judicial involvement in all these processes requires the handling members of the Judiciary to be computer literate, at the very least. We cannot fully grasp the methodologies and intricacies of cybercrimes unless we have a basic understanding of how the world of computers operates. From the point of law, basic knowledge must be there to grasp how cybercrimes may be proven before us during trial, and what constitutes the evidentiary threshold that would allow us to determine, beyond reasonable doubt, that the person accused really did commit a cybercrime.

For instance, I agree with the Solicitor General's observation that time is of the utmost essence in cybercrime law enforcement, as the breadth and speed of technology make the commission of these crimes and the subsequent destruction of its evidence faster and easier. To my mind, our current rules of procedure for the issuance of search warrants might not be responsive enough to effectively track down cybercriminals and obtain evidence of their crimes. Search warrants for instance, might be issued too late to seize evidence of the commission of a cybercrime, or may not properly describe what should be seized, among others.

Due to the highly-technical nature of investigating and prosecuting cybercrimes, as well as the apparent need to expedite our criminal procedure to make it more responsive to cybercrime law enforcement, ***I propose that special cybercrime courts be designated to specifically handle cases involving cybercrime. In addition, these cybercrime courts should have their own rules of procedure tailor-fitted to respond to the technical requirements of cybercrime prosecution and adjudication.***

The designation of special cybercrime courts of course is not outside our power to undertake: Section 21⁵⁶ of the Cybercrime Law grants the Regional Trial Courts jurisdiction over any violation of the Cybercrime Law, and provides that special cybercrime courts manned by specially trained judges should be designated. Section 5, Article VIII of the 1987 Constitution,⁵⁷ on the other hand, empowers this Court to promulgate rules on the pleading, practice, and procedure in all courts.

⁵⁶ Section 21 of the Cybercrime Law provides:


Section 21. Jurisdiction. — The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act, including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

⁵⁷ Article VIII, Section 5, paragraph 5 of the 1987 Constitution provides:

As with every petition involving the constitutionality of a law, we seek to find the proper balance between protecting a society where each individual may lawfully enjoy his or her fundamental freedoms, and where the safety and security of the members of society are assured through proper regulation and enforcement. In the present petition, I agree with the *ponencia* that the Cybercrime Law is improperly tilted towards strengthening law enforcement, to the detriment of our society's fundamental right to privacy. This is highlighted by the law's position under Section 12 which, as discussed, goes beyond what is constitutionally permissible. Beyond this finding, however, we need to provide – within the limits of our judicial power, remedies that will still allow effective law enforcement in the cyber world. It is in these lights that I urge my colleagues in this Court to consider the immediate training and designation of specialized cybercrime courts and the drafting of their own rules of procedure.

As I mentioned in the opening statements of this Concurring Opinion, I have prepared a table for easy reference to my votes. This table is attached as Annex "A" and is made an integral part this Opinion.


ARTURO D. BRION
Associate Justice

Section 5. The Supreme Court shall have the following powers:

xxx

5) Promulgate rules concerning the protection and enforcement of constitutional rights, pleading, practice, and procedure in all courts, the admission to the practice of law, the integrated bar, and legal assistance to the under-privileged. Such rules shall provide a simplified and inexpensive procedure for the speedy disposition of cases, shall be uniform for all courts of the same grade, and shall not diminish, increase, or modify substantive rights. Rules of procedure of special courts and quasi-judicial bodies shall remain effective unless disapproved by the Supreme Court.

**Annex A - Submitted Votes and Explanation on Cybercrime
J. Arturo D. Brion**

Cybercrime Law provision	J. Brion's Vote and Explanation
<p>Section 4(a)(1) penalizing illegal access as a cybercrime offense. Illegal access is defined as “[t]he access to the whole or any part of a computer system without a right.”</p>	<p>Constitutional – concur with the ponencia</p> <p>According to the petitioners, Section 4(a) (1) fails the strict scrutiny test because it is not narrowly fitted to exclude the ethical hacker, who hack computer systems to test its vulnerability to threats.</p> <p>What Section 4(a)(1) penalizes is harmful conduct in the Internet. It does not infringe upon the exercise of fundamental rights, and hence does not trigger a facial examination and the strict scrutiny of Section 4(a) (1).</p> <p>Even assuming that the strict scrutiny test applies, what the law punishes is the act of accessing a computer WITHOUT RIGHT; this excludes the ethical hacker who has been presumably contracted by the owner of the computer systems.</p>
<p>Section 4(a)(3) penalizes data interference which is defined as “[t]he 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.”</p>	<p>Constitutional – concur with the ponencia</p> <p>What Section 4(a)(3) penalizes is harmful conduct in the Internet. It does not infringe upon the exercise of fundamental rights, and hence does not trigger a facial examination and the strict scrutiny of Section 4(a)(3).</p> <p>Even if a facial examination of Section 4(a)(3) is warranted, the petitioners failed to show sufficient reason for the law’s unconstitutionality. Contrary to the petitioners’ claim, this provision does not suffer from overbreadth. As elucidated by the <i>ponencia</i>, all penal laws have an inherent chilling effect or the fear of possible prosecution. To prevent the state from legislating criminal laws because they instill this kind of fear is to render the state powerless to penalize a socially harmful conduct. Moreover, this provision clearly describes the evil that it seeks to punish.</p>
<p>Section 4(a)(6) punishes cyber-squatting which is defined as “[t]he acquisition of domain name over the internet in bad faith to profit, mislead, destroy the reputation, and deprive others from registering the same, if such a domain name is:</p> <p>(i) Similar, identical, or confusingly similar to an existing trademark</p>	<p>Constitutional – concur with the ponencia</p> <p>- Petitioners contend that Section 4(a)(6) violates the equal protection clause because a user using his real name will suffer the same fate as those who use aliases or take the name of another in satire, parody or any other literary device. The law would be punishing both a person who registers a name in satire and the person who uses this name as it is his real name.</p>

<p>registered with the appropriate government agency at the time of the domain name registration;</p> <p>(ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and</p> <p>(iii) Acquired without right or with intellectual property interests in it.”</p>	<p>Section 4(a)(6) does not violate the equal protection clause because it appears to exclude the situation that the petitioners fear. The law punishes the bad faith use of a domain name; there can be no bad faith if the person registering the domain name uses his own name.</p>
<p>Section 4(b)(3) which penalizes identity-theft, defined as “[t]he intentional acquisition, use, misuse, transfer, possession, alteration, or deletion of identifying information belonging to another, whether natural or juridical, without right.”</p>	<p>Constitutional - concur with the ponencia</p> <p>What Section 4(b)(3) penalizes is harmful conduct in the Internet. It does not infringe upon the exercise of fundamental rights, and hence does not trigger a facial examination and the strict scrutiny of Section 4(b) (3).</p> <p>Even assuming that a facial examination may be conducted, the petitioners failed to show how the government’s effort to curb this crime violates the right to privacy and correspondence, and the right to due process of law.</p> <p>According to the <i>ponencia</i>, the overbreadth doctrine does not apply because there is no restriction on the freedom of speech. What this provision regulates are specific actions: the acquisition, use, misuse or deletion of personal identifying data of another. Moreover, there is no fundamental right to acquire another’s personal data.</p> <p>This provision does not violate the freedom of the press. Journalists would not be prevented from accessing a person’s unrestricted user account in order to secure information about him. This is not the essence of identity theft that the law seeks to punish. The theft of identity information must be intended for an illegitimate purpose. Moreover, acquiring and disseminating information made public by the user himself cannot be regarded as a form of theft.</p>
<p>Section 4(c)(1) penalizing cybersex, i.e., “the willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration”.</p>	<p>Constitutional - concur with the ponencia</p> <p>Obscene speech is not protected speech, and thus does not trigger the strict scrutiny test for content-based regulations. Cybersex is defined as:</p> <p>(1) Cybersex. — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of</p>

	<p>a 'computer system, for favor or consideration.</p> <p>The qualification that the exhibition be 'lascivious' takes it outside the protective mantle of free speech.</p>
<p>Section 4(c)(2) penalizing child pornography as defined in Republic Act No. 9975 (<i>RA 9975</i>) or the Anti-Child Pornography Act of 2009 when committed through computer systems</p>	<p>Constitutional - concur with the <i>ponencia</i></p> <p>According to the <i>ponencia</i>, this provision merely expanded the scope of RA 9975 (The Anti-Child Pornography Act of 2009). The resulting penalty increase is the legislature's prerogative. Moreover, the potential for uncontrolled proliferation of a pornographic material when uploaded in the cyberspace is incalculable. There is thus a rational basis for a higher penalty.</p>
<p>Section 4(c)(3). Unsolicited commercial communications, punishes the act of transmitting commercial electronic communications which seek to advertise, sell or offer for sale products and services (SPAM)</p>	<p>Unconstitutional for infringing on commercial speech.</p> <p>According to the <i>ponencia</i>, SPAM is a legitimate form of expression, <i>i.e.</i>, commercial speech, which is still entitled to protection even if at a lower level. The government failed to present basis to hold that SPAM reduces the efficiency of computers, which is allegedly the reason for punishing the act of transmitting them.</p> <p>I do not agree with the <i>ponencia's</i> argument that Section 4(c)(3) should be declared unconstitutional because it denies a person the right to read his emails. Whether a person would be receiving SPAM is not a certainty; neither is it a right.</p>
<p>Section 4(c)(4) application of libel articles of Article 353, 354, 361 and 362 of the Revised Penal Code when committed through a computer system</p>	<p>Constitutional, but the other provisions of the Cybercrime Law that qualify cyber-libel should all be declared unconstitutional for unduly increasing the prohibitive effect of the libel law on speech. The prohibitive effect encourages self-censorship and creates a chilling effect on speech</p> <p>I concur with J. Carpio in declaring Article 354 of the Revised Penal Code unconstitutional in so far as it cyber-libel involving public officers and public figures. Section 7 of the Cybercrime Law is likewise unconstitutional insofar as it applies to cyber-libel.</p> <p>➤ The 'presumed malice' found in Article 354, in relation to Article 361 and 362 of the Revised Penal Code (which the Cybercrime Act adopted) is contrary to subsequent US rulings on freedom of speech which have been transplanted when the Philippines adopted the Bill of Rights under the 1935, 1973 and 1987 Constitutions. He noted that the RPC was enacted in 1930, before the adoption of a Bill of</p>

	<p>Rights under the 1935 Constitution. Since then, jurisprudence has developed to apply the ‘actual malice’ rule against public officials.</p> <ul style="list-style-type: none">➤ It is the duty of this Court to strike down Article 354, insofar as it applies the presumed malice rule to public officers and public figures.➤ Section 4(c)(4) of the Cybercrime Law, which adopted the definition of libel in the Revised Penal Code, and added only another means by which libel may be committed. Thus, for purposes of double jeopardy analysis, Section 4(c)(4) and Article 353 of the RPC define and penalize the same offense of libel➤ Further, Section 7 also offends the Free Speech clause by assuring multiple prosecutions of those who fall under the ambit of Section 4(c)(4). The spectre of multiple trials and sentencing, even after a conviction under the Cybercrime Law, creates a significant and not merely incidental chill on online speech. <p>- the application of Section 6 (which increases its penalty) of the Cybercrime Law to libel, should, as CJ Sereno pointed out, be declared unconstitutional (<i>discussed below</i>)</p> <p>- the application of Section 5, in so far as it applies to cyberlibel, should be declared as unconstitutional (<i>discussed below</i>)</p>
<p>Section 5 on aiding or abetting and attempt in the commission of cybercrimes</p>	<p>Unconstitutional - concur with the ponencia. It is unconstitutional in so far as it applies to unsolicited commercial communications, cyberlibel and child pornography committed online.</p> <p>According to the <i>ponencia</i>, Section 5 is unconstitutional in so far as it applies to unsolicited commercial communications, cyberlibel and child pornography committed online</p> <p>The law has not provided reasonably clear guidelines for the law enforcement authorities and the trier of facts to prevent their arbitrary and discriminatory enforcement. This vagueness in the law creates a chilling effect on free speech in cyberspace.</p> <p>For example, it is not clear from the wording of the law whether the act of ‘liking’ or ‘commenting’ on a libelous article shared through a social networking site constitutes aiding or abetting in cyberlibel.</p>

	<p>As regards aiding or abetting child pornography, the law is vague because it could also punish an internet service provider or plain user of a computer service who are not acting together with the author of the child pornography material online.</p>
<p>Section 6, which provides that all crimes penalized by the Revised Penal Code, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by RA 10175. It further states that the imposable penalty shall be one degree higher than that provided for by the Revised Penal Code, and special laws.</p>	<p>Unconstitutional – concurs with CJ Sereno, it is unconstitutional in so far as it increases the penalty for cyber-libel one degree higher.</p> <p>According to CJ Sereno, Section 6 creates an additional <i>in terrorem</i> effect on top of that already created by Article 355 of the RPC:</p> <ol style="list-style-type: none"> 1) The increase in penalty also results in the imposition of harsher accessory penalties 2) The increase in penalty neutralizes the full benefits of the Law on probation. Effectively threatening the public with the guaranteed imposition of imprisonment and its accessory penalties 3) It appears that Section 6 increases the prescription periods for the crime of cyberlibel and for its penalty to fifteen years 4) ICT as a qualifying aggravating circumstance cannot be offset by any mitigating circumstances <p>For providing that the use of ICT <i>per se</i>, even without malicious intent, aggravates the crime of libel, Section 6 is seriously flawed and burdens free speech.</p>
<p>Section 7, which provides that “[a] prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended or special laws.”</p>	<p>Unconstitutional – concur with the ponencia and Justice Carpio, unconstitutional insofar as it applies to cyberlibel and child pornography</p> <p>According to Justice Carpio, Section 7 is unconstitutional in so far as it applies to libel because it assures multiple prosecutions of those who fall under the ambit of Section 4(c)(4). The spectre of multiple trials and sentencing, even after a conviction under the Cybercrime Law, creates a significant and not merely incidental chill on online speech.</p> <p>Further, Section 4(c)(4) of the Cybercrime Law, which adopted the definition of libel in the Revised Penal Code, only added another means by which libel is committed. Thus, for purposes of double jeopardy analysis, Section 4(c)(4) and Article 353 of the RPC define and penalize the same offense of libel</p> <p>The same reasoning applies for striking down as</p>

	unconstitutional the application of Section 7 to Section 4(c)(2) or child pornography. It merely expands the Anti-Child Pornography Act’s scope to include identical activities in cyberspace.
Section 8 , which provides for penalties for the cybercrimes committed under the Cybercrime Law	Constitutional - concur with the ponencia According to the <i>ponencia</i> , it is the legislature’s prerogative to fix penalties for the commission of crimes. The penalties in Section 8 appear proportionate to the evil sought to be punished
Section 12 on the real time collection and recording of traffic data	Unconstitutional because it violates the right to privacy. While traffic data <i>per se</i> does not raise any reasonable expectation of privacy, the lack of standards in Section 12 in effect allows the real time collection and recording of traffic data of online activities and content data. Content data is indisputably private information. The collection of traffic data, over time, yields information that the internet user considers to be private. Thus, Section 12 suffers from vagueness and overbreadth that renders it unconstitutional. This ruling does not totally disallow the real-time collection and recording of traffic data. Until Congress enacts a law that provides sufficient standards for the warrantless real-time collection of traffic data, this may still be performed by law enforcement authorities, subject to a judicial warrant.
Section 13 , which requires Internet Service providers to retain traffic data and subscriber data for a period of 6 months; and for ISPs to retain content data upon order from law enforcement agents	Constitutional – concur with the ponencia The petitioners argued that Section 13 constitutes an undue deprivation of the right to property. The data preservation order is a form of garnishment of personal property in civil forfeiture proceedings, as it prevents internet users from accessing and disposing of traffic data that essentially belong to them. The <i>ponencia</i> maintained that there was no undue deprivation of property because the user has the obligation to keep a copy of his data, and the service provider has never assumed responsibility for the data’s loss or deletion while in its keep. Further, the data that service providers preserve are not made inaccessible to users by reason of the issuance of the preservation order. The process of preserving the data will not unduly hamper the normal transmission or use of these data.



<p>Section 14 on Disclosure of Computer Data, which provides that “[l]aw enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber’s information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.”</p>	<p>Constitutional – concur with the <i>ponencia</i></p> <p>The petitioners argued that it is beyond the law enforcement authorities’ power to issue subpoenas. They asserted that issuance of subpoenas is a judicial function.</p> <p>The <i>ponencia</i> clarified that the power to issue subpoenas is not exclusively a judicial function. Executive agencies have the power to issue subpoenas as part of their investigatory powers. Further, what Section 14 envisions is merely the enforcement of a duly-issued court warrant. The prescribed procedure for disclosure would not constitute an unlawful search and seizure, nor would it violate the privacy of communications and correspondence. Disclosure can be made only after judicial intervention.</p>
<p>Section 15 provides that the law enforcement authorities shall have the following powers and duties in enforcing a search and seizure warrant:</p> <ul style="list-style-type: none"> (a) To conduct interception; (b) To secure a computer system or a computer data storage medium; (c) To make and retain a copy of those computer data secured; (d) To maintain the integrity of the relevant stored computer data; (e) To conduct forensic analysis or examination of the computer data storage medium; and (f) To render inaccessible or remove those computer data in the accessed computer or computer and communications network. <p>Furthermore, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination.</p>	<p>Constitutional – concur with the <i>ponencia</i></p> <p>As the <i>ponencia</i> explained, Section 15 does not supplant, but merely supplements, the established search and seizure procedures. It merely enumerates the duties of law enforcement authorities that would ensure the proper collection, preservation, and use of computer system or data that have been seized by virtue of a court warrant. The exercise of these duties does not pose any threat on the rights of the person from whom they were taken.</p>
<p>Section 17 provides that “[u]pon</p>	<p>Constitutional – concur with the <i>ponencia</i></p>

<p>expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of a preservation and examination.”</p>	<p>According to the <i>ponencia</i>, Section 17 does not amount to deprivation of property without due process. The user has no demandable right to require the service provider to have the copy of data saved indefinitely for him in its storage system. He should have saved them in his computer if he wanted them preserved. He could also request the service provider for a copy before it is deleted.</p>
<p>Section 19 empowering the Department of Justice (DOJ) Secretary to restrict or block access to computer data when it is found to have <i>prima facie</i> violated the provisions of the Cybercrime Law</p>	<p>Unconstitutional – partially concur with the <i>ponencia</i> in holding Section 19 unconstitutional because it restricts freedom of speech</p> <p>According to the <i>ponencia</i>, the content of the computer data can also constitute speech. Section 19 constitutes an undue restraint on free speech because it allows the DOJ Secretary to block access to computer data only upon a <i>prima facie</i> finding that it violates the Cybercrime Act. Thus, it disregards established jurisprudence on the evaluation of restraints on free speech, i.e., the dangerous tendency doctrine, the balancing of interest test, and the clear and present danger rule</p>
<p>Section 20, which provides that non-compliance with the orders from the law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 (PD 1829) (Obstruction of Justice Law).</p>	<p>Constitutional - concur with the <i>ponencia</i></p> <p>According to the <i>ponencia</i>, Section 20 is not a bill of attainder; it necessarily incorporates the elements of the offense of PD 1829. The act of non-compliance must still be done knowingly or willfully. There must still be a judicial determination of guilt.</p>
<p>Section 24 on the creation of a Cybercrime Investigation and Coordinating Center (CICC); and Section 26(a) on CICC’s Powers and Functions</p>	<p>Constitutional - concur with the <i>ponencia</i></p> <p>The petitioners contended that the legislature invalidly delegated the power to formulate a national cybersecurity plan to the CICC.</p> <p>The <i>ponencia</i> ruled that there is no invalid delegation of legislative power for the following reasons:</p> <p>(1) The cybercrime law is complete in itself. The law gave sufficient standards for the CICC to follow when it provided for the definition of cyber-security. This definition serves as the parameters within which CICC should work in formulating the cyber-security plan.</p> <p>(2) The formulation of the cyber-security plan is consistent with the policy of the law to prevent and combat such cyber-offenses by facilitating their detection, investigation and</p>

	prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.
--	---

Arthur Albin