

EN BANC

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, *Petitioner*, 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, *et al.*, *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

CONCURRING AND DISSENTING OPINION

*[C]orporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes; that's how those targeted ads pop up on your computer or smartphone. But all of us understand that the standards for government surveillance must be higher. Given the unique power of the state, it is not enough for leaders to say:*

*trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached. **Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power; it depends upon the law to constrain those in power.***<sup>1</sup>

*President Barack Obama  
17 January 2014, on National  
Security Agency Reforms*

### **CARPIO, J.:**

I concur in striking down as unconstitutional Section 4(c)(3), Section 7, Section 12, and Section 19 of Republic Act No. 10175 (RA 10175) (1) penalizing unsolicited commercial speech; (2) allowing multiple prosecutions post-conviction under RA 10175; (3) authorizing the warrantless collection in bulk of traffic data; and (4) authorizing the extrajudicial restriction or blocking of access to computer data, respectively, for being violative of the Free Speech, Search and Seizure, Privacy of Communication, and Double Jeopardy Clauses.

I dissent, however, from the conclusion that (1) Article 354 of the Revised Penal Code (Code) creating the presumption of malice in defamatory imputations, and (2) Section 4(c)(1) of RA 10175 penalizing “cybersex,” are not equally violative of the constitutional guarantees of freedom of speech and expression. I therefore vote to declare Article 354 of the Code, as far as it applies to public officers and public figures, and Section 4(c)(1) of RA 10175, unconstitutional for violating Section 4, Article III of the Constitution.

#### ***Article 354 of the Code Repugnant to the Free Speech Clause***

#### ***Article 354's Presumption of Malice Irreconcilable with Free Speech Jurisprudence On Libel of Public Officers and Public Figures***

Article 4(c)(4) of RA 10175 impliedly re-adopts Article 354 of the Code *without any qualification*. Article 354 took effect three years<sup>2</sup> before the ratification of the 1935 Constitution that embodied the Free Speech Clause.<sup>3</sup> Unlike most of the provisions of the Code which are derived from

---

<sup>1</sup>*Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, THE WASHINGTON POST, 17 January 2014, [http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84\\_story.html](http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html).

<sup>2</sup>On 1 January 1932.

<sup>3</sup>Article III, Section 1(8) (“No law shall be passed abridging the freedom of speech, or of the press, or of the right of the people peaceably to assemble and petition the Government for redress of grievances.”). This is substantially reiterated in Article III, Section 9 of the 1973 Constitution and Article III, Section 4 of the 1987 Constitution.

the Spanish Penal Code of 1870, Article 354 is based on legislation<sup>4</sup> passed by the Philippine Commission during the American occupation. Nevertheless, Article 354 is inconsistent with norms on free speech and free expression now prevailing in both American and Philippine constitutional jurisprudence.

Article 354 provides as follows:

*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 delivered in said proceedings, or of any other act performed by public officers in the exercise of their functions. (Italicization supplied)

While the text of Article 354 has remained intact since the Code's enactment in 1930, constitutional rights have rapidly expanded since the latter half of the last century, owing to expansive judicial interpretations of broadly worded constitutional guarantees such as the Free Speech Clause. Inevitably, judicial doctrines crafted by the U.S. Supreme Court protective of the rights to free speech, free expression and free press found their way into local jurisprudence, adopted by this Court as authoritative interpretation of the Free Speech Clause in the Philippine Bill of Rights. One such doctrine is the *New York Times* actual malice rule, named after the 1964 case in which it was crafted, *New York Times v. Sullivan*.<sup>5</sup>

*New York Times* broadened the mantle of protection accorded to communicative freedoms by holding that the “central meaning” of the Free Speech Clause is the protection of citizens who criticize official conduct *even if such criticism is defamatory and false*. True, the defamed public official may still recover damages for libel. However, as precondition for such recovery, *New York Times* laid down a formidable evidentiary burden<sup>6</sup> – the public official must prove that the false defamatory statement was made

---

<sup>4</sup> Act No. 277.

<sup>5</sup>376 U.S. 254 (1964) (involving a libel complaint for damages filed by the Montgomery, Alabama police commissioner against the New York Times Company and other individuals for a paid political advertisement published in the *New York Times*, criticizing police conduct during a series of protests staged by civil rights activists at the height of the campaign for racial equality in the American South in the 1960s).

<sup>6</sup>Also described as “an escalati[on] of the plaintiff’s burden of proof to an almost impossible level.” *Dun & Bradstreet v. Greenmoss Builders*, 472 U.S. 749, 771 (1985) (White, J., concurring).

“with actual malice – that is, with knowledge that it was false or with reckless disregard of whether it was false or not.”<sup>7</sup>

The broad protection *New York Times* extended to communicative rights of citizens and the press *vis-à-vis* the conduct of public officials was grounded on the theory that “unfettered interchange of ideas for the bringing about of political and social changes desired by the people”<sup>8</sup> is indispensable in perfecting the experiment of self-governance. As for erroneous statements, the ruling considered them “inevitable in free debate, and that [they] must be protected if the freedoms of expression are to have the ‘breathing space’ that they need x x x to survive.”<sup>9</sup> The actual malice doctrine was later made applicable to public figures.<sup>10</sup>

Six years after *New York Times* became U.S. federal law in 1964, this Court took note of the actual malice doctrine as part of a trend of local and foreign jurisprudence enlarging the protection of the press under the Free Speech Clause.<sup>11</sup> Since then, the Court has issued a steady stream of decisions applying *New York Times* as controlling doctrine to dismiss civil<sup>12</sup> and criminal<sup>13</sup> libel complaints filed by public officers or public figures. As Justice Teehankee aptly noted:

The Court has long adopted the criterion set forth in the U.S. benchmark case of *New York Times Co. vs. Sullivan* that “libel can claim no talismanic immunity from constitutional limitations” that protect the preferred freedoms of speech and press. *Sullivan* laid down the test of actual malice, viz. “(T)he constitutional guaranty of freedom of speech and press prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with ‘actual malice’ that is, with knowledge that it was false or with reckless disregard of whether it was false or not.” x x x.<sup>14</sup>

Indeed, just as the actual malice doctrine is enshrined in the U.S. First Amendment jurisprudence, it too has become interwoven into our own understanding of the Free Speech Clause of the Philippine Bill of Rights of the 1973 and 1987 Constitutions.<sup>15</sup>

---

<sup>7</sup>Supra note 5 at 279-280.

<sup>8</sup>Supra note 5 at 269 quoting *Roth v. United States*, 354 U.S. 476, 484 (1957).

<sup>9</sup>Supra note 5 at 271-272 citing *N. A. A. C. P. v. Button*, 371 U.S. 415, 433 (1963).

<sup>10</sup>*Curtis Publishing Co. v. Butts*, 388 U.S. 130 (1967).

<sup>11</sup>*Lopez v. Court of Appeals*, 145 Phil. 219 (1970).

<sup>12</sup>*Borjal v. CA*, 361 Phil. 1 (1999); *Baguio Midland Courier v. CA*, 486 Phil. 223 (2004); *Villanueva v. Philippine Daily Inquirer, Inc.*, G.R. No. 164437, 15 May 2009, 588 SCRA 1.

<sup>13</sup>*Flor v. People*, 494 Phil. 439 (2005); *Guinguing v. CA*, 508 Phil. 193 (2005); *Vasquez v. CA*, 373 Phil. 238 (1999).

<sup>14</sup>*Babst v. National Intelligence Board*, 217 Phil. 302, 331-332 (1984) (internal citations omitted).

<sup>15</sup>Justice Enrique Fernando consistently espoused the theory that *U.S. v. Bustos*, 37 Phil. 731 (1918), preceded *New York Times* by over three decades (*Mercado v. CFI of Rizal*, 201 Phil. 565 [1982]; *Philippine Commercial and Industrial Bank v. Philnabank Employees Association*, 192 Phil. 581 [1981]). The OSG does one better than Justice Fernando by claiming that a much earlier case, *U.S. v. Sedano*, 14 Phil. 338 (1909), presaged *New York Times* (OSG Memorandum, pp. 62-63).

The actual malice rule enunciates three principles, namely:

- 1) Malice is *not presumed* even in factually false and defamatory statements against public officers and public figures; it must be proven as a fact for civil and criminal liability to lie;
- 2) Report on official proceedings or conduct of an officer *may contain fair comment*, including factually erroneous and libelous criticism; and
- 3) *Truth* or lack of reckless disregard for the truth or falsity of a defamatory statement *is an absolute defense* against public officers and public figures.

In contrast, Article 354, in relation to Article 361 and Article 362 of the Code, operates on the following principles:

- 1) Malice is *presumed* in every defamatory imputation, even if true (unless good intention and justifiable motives are shown);
- 2) Report on official proceedings or conduct of an officer must be made *without comment or remarks*, or, alternatively, must be made without malice;<sup>16</sup> and
- 3) In defamatory allegations made against a public official, *truth is a defense only if the imputed act or omission constitutes a crime or if the imputed act or omission relates to official duties*.<sup>17</sup>

The actual malice rule and Article 354 of the Code impose contradictory rules on (1) the necessity of proof of malice in defamatory imputations involving public proceedings or conduct of a public officer or public figure; and (2) the availability of truth as a defense in defamatory imputations against public officials or public figures. The former requires proof of malice and allows truth as a defense unqualifiedly, while the latter presumes malice and allows truth as a defense selectively. **The repugnancy between the actual malice rule and Article 354 is clear, direct and absolute.**

---

<sup>16</sup>Art. 362. Libelous remarks. — Libelous remarks or comments connected with the matter privileged under the provisions of Article 354, *if made with malice*, shall not exempt the author thereof nor the editor or managing editor of a newspaper from criminal liability. (Emphasis supplied)

<sup>17</sup>Art. 361. Proof of the truth. — x x x x

*Proof of the truth of an imputation of an act or omission not constituting a crime shall not be admitted, unless the imputation shall have been made against Government employees with respect to facts related to the discharge of their official duties.*

In such cases if the defendant proves the truth of the imputation made by him, he shall be acquitted. (Emphasis supplied)

Nonetheless, the Office of the Solicitor General (OSG) argues for the retention of Article 354 in the Code, suggesting that the Court can employ a “limiting construction” of the provision to reconcile it with the actual malice rule.<sup>18</sup> The *ponencia* appears to agree, holding that the actual malice rule “impl[ies] a stricter standard of ‘malice’ x x x where the offended party is a [public officer or] public figure,” the “penal code and, implicitly, the cybercrime law mainly target libel against private persons.”<sup>19</sup>

Allowing a criminal statutory provision clearly repugnant to the Constitution, and directly attacked for such repugnancy, to nevertheless remain in the statute books is a gross constitutional anomaly which, if tolerated, weakens the foundation of constitutionalism in this country. “The Constitution is either a superior, paramount law, x x x or it is on a level with ordinary legislative acts,”<sup>20</sup> and if it is superior, as we have professed ever since the Philippines operated under a Constitution, then “a law repugnant to the Constitution is void.”<sup>21</sup>

Neither does the *ponencia*’s claim that Article 354 (and the other provisions in the Code penalizing libel) “mainly target libel against private persons” furnish justification to let Article 354 stand. First, it is grossly incorrect to say that Article 354 “mainly target[s] libel against private persons.” Article 354 expressly makes reference to news reports of “any judicial, legislative or other official proceedings” which necessarily involve *public officers* as principal targets of libel. Second, the proposition that this Court ought to refrain from exercising its power of judicial review because a law is constitutional when applied to one class of persons but unconstitutional when applied to another class is fraught with mischief. It stops this Court from performing its duty,<sup>22</sup> as the highest court of the land, to “say what the law is” whenever a law is attacked as repugnant to the Constitution. Indeed, it is not only the power **but also the duty** of the Court to declare such law unconstitutional as to one class, and constitutional as to another, if valid and substantial class distinctions are present.

Undoubtedly, there is a direct and absolute repugnancy between Article 354, on one hand, and the actual malice rule under the Free Speech Clause, on the other hand. Section 4(c)(4) of RA 10175 impliedly re-adopts Article 354 *without qualification*, giving rise to a clear and direct conflict between the re-adopted Article 354 and the Free Speech Clause based on

---

<sup>18</sup>OSG Memorandum, pp. 56-66, citing *Snyder v. Ware*, 397 U.S. 589 (1970).

<sup>19</sup> Decision, p. 15.

<sup>20</sup>*Marbury v. Madison*, 5 U.S. 137, 180 (1803).

<sup>21</sup>*Id.* at 177.

<sup>22</sup>The obligatory nature of judicial power is *textualized* under the 1987 Constitution. Section 1, Article VIII provides: “Judicial power includes the **duty** of the courts of justice to settle actual controversies involving rights which are legally demandable and enforceable, and to determine whether or not there has been a grave abuse of discretion amounting to lack or excess of jurisdiction on the part of any branch or instrumentality of the Government.” (Emphasis supplied)

prevailing jurisprudence. It now becomes imperative for this Court to strike down Article 354, insofar as it applies to public officers and public figures.

The ramifications of thus striking down Article 354 are: (1) for cases filed by public officers or public figures, civil or criminal liability will lie only if the complainants prove, through the relevant quantum of proof, that the respondent made the false defamatory imputation with actual malice, that is, with knowledge that it was false or with reckless disregard of whether it was false or not; and (2) for cases filed by private individuals, the respondent cannot raise truth as a defense to avoid liability if there is no good intention and justifiable motive.

### ***Section 4(c)(1) Fails Strict Scrutiny***

Section 4(c)(1) which provides:

*Cybercrime Offenses.* — The following acts constitute the offense of cybercrime punishable under this Act:

x x x x

(c) Content-related Offenses:

(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 a computer system, for favor or consideration.

is attacked by petitioners as unconstitutionally overbroad. Petitioners in G.R. No. 203378 contend that Section 4(c)(1) sweeps in protected online speech such as “works of art that depict sexual activities” which museums make accessible to the public for a fee.<sup>23</sup> Similarly, the petitioner in G.R. No. 203359, joining causes with the petitioner in G.R. No. 203518, adopts the latter’s argument that the crime penalized by Section 4(c)(1) “encompasses even commercially available cinematic films which feature adult subject matter and artistic, literary or scientific material and instructional material for married couples.”<sup>24</sup>

The OSG counters that Section 4(c)(1) does not run afoul with the Free Speech Clause because it merely “seeks to punish online exhibition of sexual organs and activities or cyber prostitution and white slave trade for favor or consideration.”<sup>25</sup> It adds that “publication of pornographic materials in the internet [is] punishable under Article 201 of the Revised Penal Code x x x which has not yet been declared unconstitutional.”<sup>26</sup> The *ponencia* agrees, noting that the “subject” of Section 4(c)(1) is “not novel” as it

<sup>23</sup> Memorandum (G.R. No. 203378), p. 19.

<sup>24</sup> Memorandum (G.R. No. 203359), p. 58.

<sup>25</sup> OSG Memorandum, p. 43.

<sup>26</sup> *Id.* at 44-45.

is allegedly covered by two other penal laws, Article 201 of the Code and Republic Act No. 9208 (The Anti-Trafficking in Persons Act of 2003 [RA 9208]). The *ponencia* rejects the argument that Section 4(c)(1) is overbroad because “it stands a construction that makes it apply only to persons engaged in the business of maintaining, controlling, or operating x x x the lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system.”<sup>27</sup>

The government and the *ponencia*’s position cannot withstand analysis.

As Section 4(c) of RA 10175 itself states, the crimes defined under that part of RA 10175, including Section 4(c)(1), are “*Content-related Offenses*,” penalizing the *content* of categories of online speech or expression. As a content-based regulation, Section 4(c)(1) triggers the most stringent standard of review for speech restrictive laws – strict scrutiny – to test its validity.<sup>28</sup> Under this heightened scrutiny, a regulation will pass muster only if the government shows (1) a compelling state interest justifying the suppression of speech; and (2) that the law is narrowly-tailored to further such state interest. On both counts, the government in this case failed to discharge its burden.

The state interests the OSG appears to advance as bases for Section 4(c)(1) are: (1) the protection of children “as cybersex operations x x x are most often committed against children,” and (2) the cleansing of cyber traffic by penalizing the online publication of pornographic images.<sup>29</sup> Although legitimate or even substantial, these interests fail to rise to the level of compelling interests because Section 4(c)(1) is both (1) *overinclusive* in its reach of the persons exploited to commit the offense of cybersex, and (2) *underinclusive* in its mode of commission. These defects expose a legislative failure to narrowly tailor Section 4(c)(1) to tightly fit its purposes.

As worded, Section 4(c)(1) penalizes 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.” On the first interest identified by the government, the overinclusivity of this provision rests on the lack of a narrowing clause limiting its application to *minors*. As a result, Section 4(c)(1) penalizes the “lascivious exhibition of sexual organs of, or sexual activity” involving *minors and adults*, betraying a loose fit between the state interest and the means to achieve it.

---

<sup>27</sup> Decision, p. 11.

<sup>28</sup> *Osmeha v. COMELEC*, 351 Phil. 692 (1998).

<sup>29</sup> *Id.* at 44.



Indeed, the proffered state interest of protecting minors is narrowly advanced not by Section 4(c)(1) but by the provision immediately following it, Section 4(c)(2), which penalizes *online child* pornography. Section 4(c)(2) provides:

(2) Child Pornography. — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system x x x.

Republic Act No. 9775 defines “Child pornography” as referring to –

any representation, whether visual, audio, or written combination thereof, by *electronic*, mechanical, digital, optical, magnetic or any other *means*, of **child** engaged or involved in real or simulated **explicit sexual activities**.<sup>30</sup> (Emphasis supplied)

Under Section 3 of that law, the term “explicit sexual activities” is defined as follows:

Section 3. Definition of terms. –

x x x x

(c) “Explicit Sexual Activity” includes actual or simulated –

(1) As to form:

(i) *sexual intercourse or lascivious act* including, but not limited to, contact involving genital to genital, oral to genital, anal to genital, or oral to anal, whether between persons of the same or opposite sex;

x x x x

(5) *lascivious exhibition of the genitals*, buttocks, breasts, pubic area and/or anus[.] (Emphasis supplied)

Clearly then, it is Section 4(c)(2), not Section 4(c)(1), that narrowly furthers the state interest of protecting minors by punishing the “representation x x x by electronic means” of sexually explicit conduct including the exhibition of sexual organs of, or sexual acts, involving *minors*. Section 4(c)(1) does not advance such state interest narrowly because it is broadly drawn to cover both minors *and* adults. Section 4(c)(2) is constitutional because it narrowly prohibits cybersex acts involving minors only, while Section 4(c)(1) is unconstitutional because it expands the prohibition to cybersex acts involving both minors and adults when the justification for the prohibition is to protect minors only.

The overinclusivity of Section 4(c)(1) *vis-a-vis* the second state interest the government invokes results from the broad language Congress employed to define “cybersex.” As the petitioners in G.R. No. 203378, G.R.

---

<sup>30</sup> Section 3(c).

No. 203359 and G.R. No. 203518 correctly point out, the crime of “lascivious *exhibition* of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration” embraces within its ambit “works of art that depict sexual activities” made accessible to the public for a fee or “commercially available cinematic films which feature adult subject matter and artistic, literary or scientific material and instructional material for married couples.”<sup>31</sup> Congress could have narrowly tailored Section 4(c)(1) to cover only online pornography by hewing closely to the *Miller* test – the prevailing standard for such category of unprotected speech, namely, “an average person, applying contemporary standards would find [that] the work, taken as a whole, appeals to the prurient interest by depict[ing] or describ[ing] in a patently offensive way, sexual conduct specifically defined by the applicable x x x law and x x x, taken as a whole, lacks serious literary, artistic, political, or scientific value.”<sup>32</sup>

Moreover, Section 4(c)(1) penalizes “**any** lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.” There are many fee-based online medical publications that illustrate sexual organs and even sexual acts. Section 4(c)(1) will now outlaw all these online medical publications which are needed by doctors in practicing their profession. This again shows the overinclusiveness of Section 4(c)(1) in violation of the Free Speech Clause.

The loose fit between the government interests of cleansing the Internet channels of immoral content and of protecting minors, on the one hand, and the means employed to further such interests, on the other hand, is highlighted by the underinclusivity of Section 4(c)(1) insofar as the manner by which it regulates content of online speech. Section 4(c)(1) limits the ambit of its prohibition to fee-based websites exhibiting sexual organs or sexual activity. In doing so, it leaves **outside its scope and unpunished under Section 4(c)(1) non-fee based porn websites**, such as those generating income through display advertisements. The absence of regulation under Section 4(c)(1) of undeniably unprotected online speech in free and open porn websites defeats the advancement of the state interests behind the enactment of Section 4(c)(1) because unlike fee-based online porn websites where the pool of viewers is narrowed down to credit card-owning subscribers who affirm they are adults, free and open porn websites are accessible to all, minors and adults alike. Instead of purging the Internet of pornographic content, Section 4(c)(1) will trigger the proliferation of free and open porn websites which, unlike their fee-based counterparts, are not subject to criminal regulation under Section 4(c)(1). What Section 4(c)(1)

---

<sup>31</sup>For the same reason, Section 4(c)(1) is unconstitutionally overbroad, sweeping in “too much speech” including the protected indecent but non-obscene type. G. GUNTHER AND K. SULLIVAN, CONSTITUTIONAL LAW 1287 (14<sup>th</sup> ed.).

<sup>32</sup>*Miller v. California*, 413 U.S. 15 (1973), cited with approval in *Soriano v. Laguardia*, G.R. No. 164785, 15 March 2010, 615 SCRA 254, (Carpio, *J.*, dissenting); *Fernando v. Court of Appeals*, 539 Phil. 407 (2006).

should have prohibited and penalized are free and open porn websites which are accessible by minors, and not fee-based porn websites which are accessible only by credit card-owning adults, unless such fee-based websites cater to child pornography, in which case they should also be prohibited and penalized.

It is doubtful whether Congress, in failing to tailor Section 4(c)(1) to narrowly advance state interests, foresaw this worrisome and absurd effect. It is, unfortunately, an altogether common by-product of loosely crafted legislations.

Contrary to the *ponencia*'s conclusion, Section 4(c)(1) does not cover "the same subject" as Article 201 of the Code and RA 9208. Article 201 penalizes "Immoral doctrines, *obscene publications and exhibitions* and indecent shows" as understood under the *Miller* test.<sup>33</sup> On the other hand, RA 9208 penalizes *trafficking in persons* (or its promotion) for illicit purposes (Section 4[a]). The fact that these statutory provisions remain valid in the statute books has no bearing on the question whether a statutory provision penalizing the "lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration" offends the Free Speech Clause.

The majority's decision to uphold the validity of Section 4(c)(1) reverses, without explanation, the well-entrenched jurisprudence in this jurisdiction applying the obscenity test of *Miller*. Just five years ago in 2009, this Court unanimously applied *Miller* in *Soriano v. Laguardia*<sup>34</sup> to test whether the statements aired on late night TV qualified for protection under the Free Speech Clause. Much earlier in 2006, the Court also applied *Miller* to review a conviction for violation of Article 201 of the Code on obscene publications in *Fernando v. Court of Appeals*.<sup>35</sup> It was in *Pita v. Court of Appeals*,<sup>36</sup> however, decided in 1989 over a decade after *Miller*, where the Court had first occasion to describe *Miller* as "the latest word" in the evolution of the obscenity test in the U.S. jurisdiction. Indeed, as I noted in my separate opinion in *Soriano*, *Miller* is an "*expansion*" of previous tests on pornography developed in the U.S. and English jurisdictions, liberalizing the elements of previous tests (*Hicklin* and *Roth*):

The leading test for determining what material could be considered obscene was the famous *Regina v. Hicklin* case wherein Lord Cockburn enunciated thus:

I think the test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into

---

<sup>33</sup>*Fernando v. Court of Appeals*, supra note 32.

<sup>34</sup>G.R. No. 164785, 29 April 2009, 587 SCRA 79.

<sup>35</sup>539 Phil. 407 (2006).

<sup>36</sup>258-A Phil. 134 (1989).

whose hands a publication of this sort may fall.

Judge Learned Hand, in *United States v. Kennerly*, opposed the strictness of the Hicklin test even as he was obliged to follow the rule. He wrote:

I hope it is not improper for me to say that the rule as laid down, however consonant it may be with mid-Victorian morals, does not seem to me to answer to the understanding and morality of the present time.

*Roth v. United States* laid down the more reasonable and thus, more acceptable test for obscenity: "whether to the average person, applying contemporary community standards, the dominant theme of the material taken as a whole appeals to prurient interest." Such material is defined as that which has "a tendency to excite lustful thoughts," and "prurient interest" as "a shameful or morbid interest in nudity, sex, or excretion."

*Miller v. California* merely expanded the *Roth* test to include two additional criteria: "the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and the work, taken as whole, lacks serious literary, artistic, political, or scientific value." The basic test, as applied in our jurisprudence, extracts the essence of both *Roth* and *Miller* – that is, whether the material appeals to prurient interest.<sup>37</sup> (Italicization supplied; internal citations omitted)

*Miller* is the modern obscenity test most protective of speech uniformly followed in this jurisdiction for over two decades. The majority, in upholding Section 4(c)(1) and rejecting *Miller*, regresses to less protective frameworks of speech analysis. Because neither the *ponencia* nor the concurring opinions devote discussion on this doctrinal shift, one is left guessing whether the Philippine jurisdiction's test on pornography has reverted only up to *Roth* or reaches as far back as the discredited *Hicklin* test. Either way, the lowered protection afforded to works claimed as obscene turns back the clock of free expression protection to the late 1960s and beyond when prevailing mores of morality are incongruous to 21<sup>st</sup> century realities.

### ***Section 4(c)(3) Repugnant to the Free Speech Clause***

Section 4(c)(3) of RA 10175 makes criminal the transmission through a computer system of "electronic communication x x x which seek to advertise, sell, or offer for sale products and services" unless they fall under three categories of exceptions. These categories are: (1) the recipient of the commercial message "gave prior affirmative consent" to do so; (2) the

---

<sup>37</sup>G.R. No. 164785, 15 March 2010, 615 SCRA 254, 270-271 (Resolution).

“primary intent” of the commercial message “is for service and/or administrative announcements from the sender” to its “users, subscribers or customers”; and (3) the commercial message (a) has an “opt-out” feature; (b) has a source which is “not purposely disguise[d]”; and (c) “does not purposely include misleading information x x x to induce the recipient to read the message.” According to the OSG, Congress enacted Section 4(c)(3) to improve the “efficiency of commerce and technology” and prevent interference with “the owner’s peaceful enjoyment of his property [computer device].”<sup>38</sup>

Section 4(c)(3) fails scrutiny. Section 4(c)(3) impermissibly restricts the flow of truthful and non-misleading commercial speech in cyberspace that does not fall under any of the exceptions in Section 4(c)(3), lowering the protection it enjoys under the Free Speech Clause.<sup>39</sup> Section 4(c)(3) would be constitutional if it allowed the free transmission of truthful and non-misleading commercial speech, even though not falling under any of the exceptions in Section 4(c)(3). There is no legitimate government interest in criminalizing *per se* the transmission in cyberspace of truthful and non-misleading commercial speech.

Under the exception clauses of Section 4(c)(3), commercial speech may be transmitted online only when (1) the recipient has subscribed to receive it (“opted-in”); or (2) the commercial speech, directed to its “users, subscribers or customers,” contains announcements; or (3) the undisguised, non-misleading commercial speech has an “opt-out” feature. The combination of these exceptions results in penalizing the transmission online (1) of commercial speech with no “opt-out” feature to non-subscribers, **even if truthful and non-misleading**; and (2) of commercial speech which does not relay “announcements” to subscribers, **even if truthful and non-misleading**. Penalizing the transmission of these protected categories of commercial speech is devoid of any legitimate government interest and thus violates the Free Speech Clause.

Indeed, the free flow of truthful and non-misleading commercial speech online should remain unhampered to assure freedom of expression of protected speech. In cyberspace, the free flow of truthful and non-misleading commercial speech does not obstruct the public view or degrade the aesthetics of public space in the way that billboards and poster advertisements mar the streets, highways, parks and other public places. True, commercial speech does not enjoy the same protection as political speech in the hierarchy of our constitutional values. However, any regulation of truthful and non-misleading commercial speech must still have a

---

<sup>38</sup> Decision, p. 13.

<sup>39</sup>The protected nature of truthful and non-misleading commercial speech was adverted to in Philippine jurisprudence in *Pharmaceutical and Health Care Association of the Philippines v. Secretary of Health Duque III*, 562 Phil. 386, 448-451 (Puno, C.J., concurring).

legitimate government purpose. Regulating truthful and non-misleading commercial speech does not result in “efficiency of commerce and technology” in cyberspace.

In fact, the free flow of truthful and non-misleading commercial speech should be encouraged in cyberspace for the enlightenment of the consuming public, considering that it is cost-free to the public and almost cost-free to merchants. Instead of using paper to print and mail truthful and non-misleading commercial speech, online transmission of the same commercial message will save the earth's dwindling forests and be more economical, reducing marketing costs and bringing down consumer prices. If any regulation of truthful and non-misleading commercial speech is to take place, its terms are best fixed through the interplay of market forces in cyberspace. This is evident, in fact, in the menu of options currently offered by email service providers to deal with unwanted or spam email, allowing their account holders to customize preferences in receiving and rejecting them. Unwanted or spam emails automatically go to a separate spam folder where all the contents can be deleted by simply checking the “delete all” box and clicking the delete icon. Here, the account holders are given the **freedom to read, ignore or delete** the unwanted or spam email with hardly any interference to the account holders' peaceful enjoyment of their computer device. Unless the commercial speech transmitted online is misleading or untruthful, as determined by courts, government should step aside and let this efficient self-regulatory market system run its course.

### ***Section 7 of RA 10175 Repugnant to the Double Jeopardy and Free Speech Clauses***

The petitioners in G.R. No. 203335 and G.R. No. 203378 attack the constitutionality of Section 7, which makes conviction under RA 10175 non-prejudicial to “any liability for violation of any provision of the Revised Penal Code, as amended, or special laws,” for being repugnant to the Double Jeopardy Clause. The OSG sees no merit in the claim, citing the rule that “a single set of acts may be prosecuted and penalized under two laws.”<sup>40</sup>

The OSG misapprehends the import of Section 7. Although RA 10175 defines and punishes a number of offenses to which Section 7 applies, its application to the offense of online libel under Section 4(c)(4) of RA 10175, in relation to the offense of libel under Article 353 of the Code, suffices to illustrate its unconstitutionality for trenching the Double Jeopardy and Free Speech Clauses.

---

<sup>40</sup> OSG Consolidated Comment, pp. 109-110, citing *People v. Sandoval*, G.R. Nos. 95353-54, 7 March 1996, 254 SCRA 436.

RA 10175 does not define libel. Its definition is found in the Code (Article 353) which provides:

*Definition of libel* - A libel is 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.

As defined, the medium through which libel is committed *is not an element of such offense*. What is required of the prosecution are proof of the (1) statement of a discreditable act or condition of another person; (2) publication of the charge; (3) identity of the person defamed; and (4) existence of malice.<sup>41</sup> The irrelevance of the medium of libel in the definition of the crime is evident in Article 355 of the Code which punishes libel with a uniform penalty<sup>42</sup> whether it is committed “by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means.”

RA 10175 adopts the Code's definition of libel by describing online libel under Section 4(c)(4) as “[t]he unlawful or prohibited acts *as defined in Article 355 of the Revised Penal Code*, as amended, committed through a computer system or any other similar means which may be devised in the future.” By adopting the Code's definition of libel, Section 4(c)(4) also adopts the elements of libel as defined in Article 353 in relation to Article 355 of the Code. Section 4(c)(4) merely adds the media of “computer system or any other similar means which may be devised in the future” to the list of media enumerated in Article 355. This is understandable because at the time the Code was enacted in 1930, the Internet was non-existent. In the words of the OSG itself (in contradiction to its position on the constitutionality of Section 7), Congress enacted Section 4(c)(4) not to create a new crime, but merely to “ma[ke] express an avenue *already covered by the term 'similar means' under Article 355, to keep up with the times*”:

Online libel is not a new crime. Online libel is a crime punishable under x x x Article 353, in relation to Article 355 of the Revised Penal Code. *Section 4(c)(4) just made express an avenue already covered by the term “similar means” under Article 355, to keep up with the times.*<sup>43</sup> (Emphasis supplied)

**For purposes of double jeopardy analysis, therefore, Section 4(c)(4) of RA 10175 and Article 353 in relation to Article 355 of the Code define and penalize the same offense of libel.** Under the Double Jeopardy

<sup>41</sup>*Vasquez v. Court of Appeals*, 373 Phil. 238 (1999).

<sup>42</sup>*Prision correccional* in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos, or both, in addition to the civil action which may be brought by the offended party.

<sup>43</sup>OSG Consolidated Comment, p. 77.

Clause, conviction or acquittal under either Section 4(c)(4) or Article 353 in relation to Article 355 constitutes a bar to another prosecution *for the same offense* of libel.

The case of petitioners Ellen Tordesillas, Harry Roque and Romel Bagares in G.R. No. 203378 provides a perfect example for applying the rules on print and online libel in relation to the Double Jeopardy Clause. These petitioners write columns which are published online and in print by national and local papers.<sup>44</sup> They allege, and respondents do not disprove, that “their columns see publication in both print and online versions of the papers they write for.”<sup>45</sup> Should these petitioners write columns for which they are prosecuted and found liable under Section 4(c)(4) of RA 10175 for online libel the Double Jeopardy Clause bars their second prosecution for print libel for the same columns upon which their first conviction rested, under Article 353 in relation to Article 355 of the Code. Such constitutional guarantee shields them from being twice put in jeopardy of punishment for the same offense of libel.

The foregoing analysis applies to all other offenses defined and penalized under the Code or special laws which (1) are penalized as the same offense under RA 10175 committed through the use of a computer system; or (2) are considered aggravated offenses under RA 10175. Conviction or acquittal under the Code or such special laws constitutes a bar to the prosecution for the commission of any of the offenses defined under RA 10175. Thus, for instance, conviction or acquittal under Section 4(a) of RA 9775 (use of a child to create child pornography<sup>46</sup>) constitutes a bar to the prosecution for violation of Section 4(c)(2) of RA 19175 (online child pornography) and *vice versa*. This is because the offense of child pornography under RA 9775 is the same offense of child pornography under RA 10175 committed through the use of a computer system.

Section 7 of RA 10175 also offends the Free Speech Clause by assuring multiple prosecutions of those who fall under the ambit of Section 4(c)(4). The specter of multiple trials and sentencing, even after conviction under RA 10175, creates a significant and not merely incidental chill on online speech. Section 7 stifles speech in much the same way that excessive prison terms for libel, subpoenas to identify anonymous online users or high costs of libel litigation do. It has the effect of making Internet users “steer far wide of the unlawful zone”<sup>47</sup> by practicing self-censorship, putting to naught the democratic and inclusive culture of the Internet where anyone can be a

---

<sup>44</sup>*Malaya* (<http://www.malaya.com.ph/>) and *Abante* (<http://www.abante.com.ph/>); *Manila Standard Today* ([manilastandardtoday.com](http://manilastandardtoday.com)); and *The News Today* ([www.thenewstoday.info](http://www.thenewstoday.info)), respectively.

<sup>45</sup> Petition (G.R. No. 203378), p. 37.

<sup>46</sup> “Section 4. Unlawful or Prohibited Acts. - It shall be unlawful for any person: (a) To hire, employ, use, persuade, induce or coerce a child to perform in the creation or production of any form of child pornography[.]”

<sup>47</sup>*Speiser v. Randall*, 357 U.S. 513, 526 (1958).



publisher and everyone can weigh policies and events from anywhere in the world in real time. Although Section 7, as applied to Section 4(c)(4), purports to strengthen the protection to private reputation that libel affords, its sweeping ambit deters not only the online publication of defamatory speech against private individuals but also the online dissemination of scathing, false, and defamatory statements against public officials and public figures which, under the actual malice rule, are conditionally protected. This chilling effect on online communication stifles robust and uninhibited debate on public issues, the constitutional value lying at the core of the guarantees of free speech, free expression and free press.

***Section 12 of RA 10175 Violative  
of the Search and Seizure and  
Privacy of Communication Clauses***

Section 12 of RA 10175 grants authority to the government to record in bulk and in real time electronic data transmitted by means of a computer system,<sup>48</sup> such as through mobile phones and Internet-linked devices. The extent of the power granted depends on the type of electronic data sought to be recorded, that is, whether traffic data or non-traffic data (“all other data”). For traffic data, which RA 10175 defines as “the communication’s origin, destination, route, time, date, size, duration, or type of underlying service,” the government, for “due cause” can record them on its own or with the aid of service providers, **without need of a court order**. For non-traffic data collection, a “court warrant” is required based on reasonable grounds that the data to be collected is “essential” for the prosecution or prevention of violation of any of the crimes defined under RA 10175. The full text of Section 12 provides:

*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.

---

<sup>48</sup>Defined in the law (Section 3[g]) as “refer[ing] to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media.”

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.

Section 12 of RA 10175 is the statutory basis for intelligence agencies of the government to undertake warrantless electronic data surveillance and collection in bulk to investigate and prosecute violations of RA 10175.

Section 12 fails constitutional scrutiny. Collection in bulk of private and personal electronic data transmitted through telephone and the Internet allows the government to create profiles of the surveilled individuals' close social associations, personal activities and habits, political and religious interests, and lifestyle choices expressed through these media. The intrusion into their private lives is as extensive and thorough as if their houses, papers and effects are physically searched. **As such, collection in bulk of such electronic data rises to the level of a search and seizure within the meaning of the Search and Seizure Clause, triggering the requirement for a judicial warrant grounded on probable cause.** By vesting the government with authority to undertake such highly intrusive search and collection in bulk of personal digital data without benefit of a judicial warrant, Section 12 is unquestionably repugnant to the guarantee under the Search and Seizure Clause against warrantless searches and seizures.

Further, Section 12 allows the use of advanced technology to impermissibly narrow the right to privacy of communication guaranteed under the Privacy of Communications Clause. Although such clause exempts from its coverage searches undertaken "when public safety or order requires otherwise, as prescribed by law," Section 12 is not a "law" within the contemplation of such exception because it does not advance the interest of "public safety or order." Nor does it comply with the warrant requirement which applies to all searches of communication and correspondence not falling under recognized exceptions to the Search and Seizure Clause, such as the search of non-legal communication sent and received by detainees<sup>49</sup>

---

<sup>49</sup> *Pollo v. Constantino-David*, G.R. No. 181881, 18 October 2011, 659 SCRA 189.

search of electronic data stored in government issued computers,<sup>50</sup> or security searches at airports.<sup>51</sup>

***Scope of Information Subject of Real-Time  
Extrajudicial Collection and Analysis  
by Government***

Section 12's definition of traffic data – the communication's origin, destination, route, time, date, size, duration, or type of underlying service – encompasses the following information for mobile phone, Internet and email communications:

Mobile phone:

telephone number of the caller  
telephone number of the person called  
location of the caller  
location of the person called  
the time, date, and duration of the call  
(For messages sent via the Short Messaging System, the same information are available save for the duration of the communication.)

Email:

date  
time  
source  
destination and size  
attachment/s  
country of sender and recipient  
city of sender and recipient

Internet:

search keywords  
public IP (Internet Protocol) of user  
geolocation of user  
client's name (for smartphone, PC or desktop)  
browser  
OS (Operating System)  
URL (Universal Source Locator)  
date and time of use

---

<sup>50</sup>*In the Matter of the Petition for Habeas Corpus of Capt. Alejano v. Gen. Cabuay*, 505 Phil. 298 (2005).

<sup>51</sup>*People v. Canton*, 442 Phil. 743 (2002); *People v. Johnson*, 401 Phil. 734 (2000). See also *United States v. Arnold*, 523 F.3d 941 (9th Cir. Cal., 2008), certiorari denied by the U.S. Supreme Court in *Arnold v. United States*, 129 S. Ct. 1312 (2009) (involving a warrantless search of a laptop of a passenger who had arrived from overseas travel).

Unlike personal information which form part of the public domain (hence, readily accessible) because their owners have either disclosed them to the government as a result of employment in that sector or are part of transactions made with regulatory agencies (such as the land transportation, passport and taxing agencies), the information indicated above are personal *and* private. They reveal data on the social associations, personal activities and habits, political and religious interests, and lifestyle choices of individuals that are not freely accessible to the public. **Because Section 12 contains no limitation on the quantity of traffic data the government can collect, state intelligence agencies are free to accumulate and analyze as much data as they want, anytime they want them.**

Randomly considered, traffic data do not reveal much about a person's relationships, habits, interests or lifestyle expressed online or through phone. After all, they are mere bits of electronic footprint tracking a person's electronic communicative or expressive activities. When compiled in massive amounts, however, traffic data, analyzed over time, allows the state to create a virtual profile of the surveilled individuals, revealing their close relationships, mental habits, political and religious interests, as well as lifestyle choices – as detailed as if the government had access to the content of their letters or conversations. Or put differently –

When [traffic] information x x x is combined, it can identify all of our surreptitious connections with the world, providing powerful evidence of our activities and beliefs. [L]aw enforcement can construct a “complete mosaic of a person's characteristics” through this type of x x x surveillance. *Under these circumstances, the information the government accumulates is more akin to content than mere cataloguing.*<sup>52</sup> (Emphasis supplied)

The profiling of individuals is not hampered merely because the bulk data relate to telephone communication. As pointed out in a Report, dated 12 December 2013, by a government panel of experts<sup>53</sup> which reviewed the U.S. government's electronic surveillance policy (Panel's Report) –

[t]he record of every telephone call an individual makes or receives over the course of several years can reveal an enormous amount about that individual's private life. x x x. [T]elephone calling data can reveal x x x an individual's “familial, political, professional, religious, and sexual associations.” It can reveal calls “to the psychiatrist, the plastic surgeon, x x x the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar, and on and on.”<sup>54</sup>

---

<sup>52</sup>Christopher Slobogin, *The Search and Seizure of Computers and Electronic Evidence: Transaction Surveillance by the Government*, 75 *Miss. L.J.* 139, 178. (Hereinafter Slobogin, *Transaction Surveillance*).

<sup>53</sup>Composed of Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire.

<sup>54</sup>Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 12 December 2013, pp. 116-117 (internal citations omitted),

This virtual profiling is possible not only because of software<sup>55</sup> which sifts through telephone and Internet data to locate common patterns but also because, for Internet “Universal Resource Locators x x x, they are [both] addresses (*e.g.*, [www.amazon.com/kidneydisease](http://www.amazon.com/kidneydisease)) and [links] x x x allowing access to the website and thus permit government to ascertain what the user has viewed.”<sup>56</sup> The identities of users of mobile phone numbers can easily be found through Internet search or in public and private mobile phone directories, calling cards, letterheads and similar documents.

***Bulk Data Surveillance Rises to the Level of a “Search and Seizure” Within the Meaning of the Search and Seizure Clause***

There is no quarrel that not all state access to personal information amount to a “search” within the contemplation of the Search and Seizure Clause. Government collection of data readily available (or exposed) to the public, even when obtained using devices facilitating access to the information, does not implicate constitutional concerns of privacy infringement.<sup>57</sup> It is when government, to obtain private information, intrudes into domains over which an individual holds legitimate privacy expectation that a “search” takes place within the meaning of the Search and Seizure Clause.<sup>58</sup> To determine whether the collection of bulk traffic data of telephone and online communication amounts to a constitutional search, the relevant inquiry, therefore, is whether individuals using such media hold legitimate expectation that the traffic data they generate will remain private.

Unlike this Court, the U.S. Supreme Court had weighed such question and answered in the negative. In *Smith v. Maryland*,<sup>59</sup> promulgated in 1979,

---

[http://www.whitehouse.gov/sites/default/files/docs/2013-12-12\\_rg\\_final\\_report.pdf](http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf) (last visited on 29 December 2013).

<sup>55</sup>Commercially available programs are collectively referred to as “snoopware” which “allows its buyer to track the target well beyond a single website; it accumulates the addresses of all the Internet locations the target visits, as well as the recipient of the target’s emails.” Slobogin, *Transaction Surveillance* at 146. The government surveillance agencies tend to develop their own version of such programs.

<sup>56</sup> *Id.* at 153.

<sup>57</sup>See, *e.g.*, *Florida v. Riley*, 488 U.S. 445 (1989) and *California v. Ciraolo*, 476 U.S. 207 (1986) (uniformly holding that aerial surveillance of private homes and surrounding areas is not a “search” under the Fourth Amendment).

<sup>58</sup>This standard, crafted by Mr. Justice Harlan in his separate opinion in *Katz v. US*, 389 U.S. 347 (1967), has been adopted by this Court to settle claims of unreasonable search (see, *e.g.*, *Pollo v. Constantino-David*, G.R. No. 181881, 18 October 2011, 659 SCRA 189; *People v. Johnson*, *supra* note 51).

<sup>59</sup>442 U.S. 735 (1979). The earlier ruling in *United States v. Miller*, 425 U.S. 435 (1976), found no legitimate privacy expectation over the contents of checks and bank deposit slips. Unlike in the United States, however, Philippine law treats bank deposits “as of an absolutely confidential nature” (For deposits in local currency, see Section 2 of Republic Act No. 1405, as amended. For deposits in foreign currency, see Section 8 of Republic Act No. 6426, as amended).

that court was confronted with the issue whether the warrantless monitoring of telephone numbers dialed from a private home and stored by the telephone company, amounted to a search within the meaning of the Fourth Amendment. The U.S. High Court's analysis centered on the reasoning that a caller has no legitimate privacy expectation over telephone numbers stored with telephone companies because he "assumed the risk that the company would reveal to police the numbers he dialed."<sup>60</sup>

Several reasons undercut not only the persuasive worth of *Smith* in this jurisdiction but also the cogency of its holding. First, all three modern Philippine Constitutions, **unlike the U.S. Constitution**, explicitly guarantee "privacy of communications and correspondence."<sup>61</sup> This is a constitutional recognition, no less, of the legitimacy of the expectation of surveilled individuals that their communication and correspondence will remain private and can be searched by the government only upon compliance with the warrant requirement under the Search and Seizure Clause. Although such guarantee readily protects the *content* of private communication and correspondence, the guarantee also protects traffic data collected *in bulk* which enables the government to construct profiles of individuals' close social associations, personal activities and habits, political and religious interests, and lifestyle choices, enabling intrusion into their lives as extensively as if the government was physically searching their "houses, papers and effects."<sup>62</sup>

Second, at the time the U.S. Supreme Court decided *Smith* in 1979, there were no cellular phones, no Internet and no emails as we know and use them today. Over the last 30 years, technological innovations in mass media and electronic surveillance have radically transformed the way people communicate with each other and government surveils individuals. These radical changes undergirded the refusal of the District Court of Columbia to follow *Smith* in its ruling promulgated last 16 December 2013, striking down

---

<sup>60</sup>Id. at 744.

<sup>61</sup>Constitution (1935), Article III, Section 1(5) ("The privacy of communication and correspondence shall be inviolable except upon lawful order of the court or when public safety and order require otherwise."); Constitution (1973), Article III, Section 4(1) ("The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety and order require otherwise."); Constitution (1987), Article III, Section 3(1) ("The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law."). The inclusion of the phrase "as prescribed by law" in the 1987 Constitution indicates heightened protection to the right, removing the executive exemption to the guarantee (on the ground of public safety or order).

<sup>62</sup>The protection afforded by Section 3(1), Article III of the Constitution to the privacy of communication and correspondence is supplemented by the Rule of the Writ of Habeas Data, effective 2 February 2008, giving judicial relief to "any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the x x x correspondence of the aggrieved party" (Section 1). If the writ lies, the court hearing the application for the writ "shall enjoin the act complained of, or order the deletion, destruction, or rectification of the erroneous data or information x x x." (Section 16).

portions of the spying program of the U.S. National Security Agency (NSA).<sup>63</sup> The District Court observed:

[T]he relationship between the police and the phone company in *Smith* is nothing compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies. x x x x In *Smith*, the Court *considered a one-time, targeted request for data* regarding an individual suspect in a criminal investigation, x x x ***which in no way resembles the daily, all-encompassing, indiscriminate dump of phone metadata that the (NSA) now receives as part of its Bulk Telephony Metadata Program.*** *It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government.* x x x.<sup>64</sup> (Emphasis supplied)

Third, individuals using the telephone and Internet do not freely disclose private information to the service providers and the latter do not store such information in trust for the government. Telephone and Internet users divulge private information to service providers *as a matter of necessity* to access the telephone and Internet services, and the service providers store such information (within certain periods) also *as a matter of necessity* to enable them to operate their businesses. In what can only be described as an outright rejection of *Smith*'s analysis, the Panel's Report, in arriving at a similar conclusion, states:<sup>65</sup>

In modern society, individuals, for practical reasons, have to use banks, credit cards, e-mail, telephones, the Internet, medical services, and the like. *Their decision to reveal otherwise private information to such third parties does not reflect a lack of concern for the privacy of the information, but a necessary accommodation to the realities of modern life. What they want — and reasonably expect — is both the ability to use such services and the right to maintain their privacy when they do so.*<sup>66</sup> (Emphasis supplied)

Clearly then, bulk data surveillance and collection is a “search and seizure” within the meaning of the Search and Seizure Clause not only because it enables maximum intrusion into the private lives of the surveilled individuals but also because such individuals do not forfeit their privacy expectations over the traffic data they generate by transacting with service providers. Bulk data and content-based surveillance and collection are functionally identical in their access to personal and private information. It follows that the distinction Section 12 of RA 10175 draws between content-based and bulk traffic data surveillance and collection, requiring judicial warrant for the former and a mere administrative “due cause” for the latter,

---

<sup>63</sup> *Klayman v. Obama*, 2013 U.S. Dist. LEXIS 176928.

<sup>64</sup> *Id.* at 84-85 (internal citations omitted).

<sup>65</sup> Panel's Report at 744.

<sup>66</sup> *Id.* at 111-112.

is unconstitutional. As “searches and seizures” within the contemplation of Search and Seizure Clause, bulk data and content-based surveillance and collection are uniformly subject to the constitutional requirement of a judicial warrant grounded on probable cause.

***Section 12 of RA 10175  
Impermissibly Narrows the  
Right to Privacy of Communication  
and Correspondence***

The grant under Section 12 of authority to the government to undertake bulk data surveillance and collection without benefit of a judicial warrant enables the government to access private and personal details on the surveilled individuals’ close social associations, personal activities and habits, political and religious interests, and lifestyle choices. This impermissibly narrows the sphere of privacy afforded by the Privacy of Communication Clause. It opens a backdoor for government to pry into their private lives as if it obtained access to their phones, computers, letters, books, and other papers and effects. Since Section 12 does not require a court warrant for government to undertake such surveillance and data collection, law enforcement agents can access these information anytime they want to, for whatever purpose they may deem as amounting to “due cause.”

The erosion of the right to privacy of communication that Section 12 sanctions is pernicious because the telephone and Internet are indispensable tools for communication and research in this millennium. People use the telephone and go online to perform tasks, run businesses, close transactions, read the news, search for information, communicate with friends, relatives and business contacts, and in general go about their daily lives in the most efficient and convenient manner. Section 12 forces individuals to make the difficult choice of preserving their communicative privacy but reverting to non-electronic media, on the one hand, or availing of electronic media while surrendering their privacy, on the other hand. These choices are inconsistent with the Constitution’s guarantee to privacy of communication.

***Section 12 of RA 10175 not a “law”  
Within the Contemplation of the  
Exception Clause in Section 3(1),  
Article III of the 1987 Constitution***

Undoubtedly, the protection afforded by the Constitution under the Privacy of Communication Clause is not absolute. It exempts from the



guarantee intrusions “upon lawful order of the court, or *when public safety or order requires otherwise, as prescribed by law.*” Does Section 12 of RA 10175 constitute a “law” within the contemplation of the Privacy of Communication Clause?

When the members of the 1971 Constitutional Convention deliberated on Article III, Section 4(1) of the 1973 Constitution, the counterpart provision of Article III, Section 3(1) of the 1987 Constitution, the phrase “public safety or order” was understood by the convention members to encompass “the security of human lives, liberty and property *against the activities of invaders, insurrectionists and rebels.*”<sup>67</sup> This narrow understanding of the public safety exception to the guarantee of communicative privacy is consistent with Congress’ own interpretation of the same exception as provided in Article III, Section 1(5) of the 1935 Constitution. Thus, when Congress passed the Anti-Wiretapping Act<sup>68</sup> (enacted in 1965), it exempted from the ban on wiretapping “cases involving the crimes of treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage and *other offenses against national security*” (Section 3). In these specific and limited cases where wiretapping has been allowed, **a court warrant is required** before the government can record the conversations of individuals.

Under RA 10175, the categories of crimes defined and penalized relate to (1) offenses against the confidentiality, integrity and availability of computer data and systems (Section 4[a]); (2) computer-related offenses (Section 4[b]); (3) content-related offenses (Section 4[c]); and (4) other offenses (Section 5). None of these categories of crimes are limited to public safety or public order interests (akin to the crimes exempted from the coverage of the Anti-Wiretapping Law). They relate to crimes committed in the cyberspace which have no stated public safety or even national security dimensions. Such fact takes Section 12 outside of the ambit of the Privacy of Communication Clause.

In any event, even assuming that Section 12 of RA 10175 is such a “law,” such “law” can never negate the constitutional requirement under the Search and Seizure Clause that when the intrusion into the privacy of communication and correspondence rises to the level of a search and seizure of personal effects, then a warrant issued by a judge becomes **mandatory** for such search and seizure. Fully cognizant of this fact, Congress, in enacting exceptions to the ban on wiretapping under the Anti-Wiretapping

---

<sup>67</sup>I. J. BERNAS, THE CONSTITUTION OF THE REPUBLIC OF THE PHILIPPINES: A COMMENTARY 135, citing 1971 Constitutional Convention, Session of 25 November 1972.

<sup>68</sup> Republic Act No. 4200.

Act, made sure that law enforcement authorities obtain a warrant from a court based on probable cause to undertake wiretapping. Section 3 of the Anti-Wiretapping Act provides:

Nothing contained in this Act, however, shall render it unlawful or punishable for any peace officer, who is authorized by a *written order of the Court*, to execute any of the acts declared to be unlawful in the two preceding Sections in cases involving the crimes of treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage and other offenses against national security: Provided, *That such written order 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 a 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:* Provided, however, That in cases involving the offenses of rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, and inciting to sedition, *such authority shall be granted only upon prior proof that a rebellion or acts of sedition, as the case may be, have actually been or are being committed; (2) that there are reasonable grounds to believe that evidence will be obtained 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.* (Emphasis supplied)

### ***Section 12 of RA 10175 More Expansive than U.S. Federal Electronic Surveillance Laws***

Under U.S. federal law, authorities are required to obtain a court order to install “a pen register or trap and trace device” to record in real time or decode electronic communications.<sup>69</sup> Although initially referring to technology to record telephone numbers only, the term “pen register or trap and trace device” was enlarged by the Patriot Act to cover devices which record “dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications,” including Internet traffic data.<sup>70</sup> The court of competent jurisdiction may

---

<sup>69</sup>Under the Electronic Communications Privacy Act, codified in 18 USC § 3121(a) which provides: “*In General.*— Except as provided in this section, no person may install or use a pen register or a trap and trace device *without first obtaining a court order* under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)” (Emphasis supplied)

<sup>70</sup>18 USC § 3121 (c) which provides: “*Limitation.*— A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of *electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications* so as not to include the contents of any wire or electronic communications.” (Emphasis supplied)

issue *ex parte* the order for the installation of the device “if [it] finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is *relevant to an ongoing criminal investigation*.”<sup>71</sup>

For electronic surveillance relating to foreign intelligence, U.S. federal law requires the government to obtain *ex parte* orders from the Foreign Intelligence Surveillance Court (FISC)<sup>72</sup> upon showing that “the target of surveillance was a foreign power or an agent of a foreign power.”<sup>73</sup> Under an amendment introduced by the Patriot Act, the government was further authorized to obtain an *ex parte* order from the FISC for the release by third parties of “tangible things” such as books, papers, records, documents and other items “upon showing that the tangible things sought are relevant to an authorized investigation x x x to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.”<sup>74</sup> The investigation is further subjected to administrative oversight by the Attorney General whose prior authorization to undertake such investigation is required.<sup>75</sup>

In contrast, Section 12 of RA 10175 authorizes law enforcement officials “to collect or record by technical or electronic means traffic data in real-time” if, in their judgment, such is for “due cause.”<sup>76</sup> Unlike in the Patriot Act, there is no need for a court order to collect traffic data. RA 10175 does not provide a definition of “due cause” although the OSG suggests that it is synonymous with “just reason or motive” or “adherence to a lawful procedure.”<sup>77</sup> The presence of “due cause” is to be determined solely by law enforcers.

In comparing the U.S. and Philippine law, what is immediately apparent is that the U.S. federal law requires judicial oversight for bulk electronic data collection and analysis while Philippine law leaves such process to the exclusive discretion of law enforcement officials. The absence of judicial participation under Philippine law precludes independent neutral

---

<sup>71</sup> 18 USC § 3123(a) (2) which provides: “State investigative or law enforcement officer.— Upon an application made under section 3122 (a)(2), the court shall enter an *ex parte* order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer *has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation*.” (Emphasis supplied)

<sup>72</sup> Composed of eleven district court judges appointed by the Chief Justice of the U.S. Supreme Court.

<sup>73</sup> Foreign Intelligence Surveillance Act, codified at 50 USC § 1804(a)(3), 1805(a)(2).

<sup>74</sup> 50 USC § 1861(b)(2)(A).

<sup>75</sup> 50 USC § 1861(a)(2)(A).

<sup>76</sup> Under the first paragraph of Section 12 which provides: “*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.*” (Emphasis supplied)

<sup>77</sup> Decision, p. 33.

assessment by a court on the necessity of the surveillance and collection of data.<sup>78</sup> Because the executive's assessment of such necessity is unilateral, Philippine intelligence officials can give the standard of "due cause" in Section 12 of RA 10175 as broad or as narrow an interpretation as they want.

The world by now is aware of the fallout from the spying scandal in the United States arising from the disclosure by one of its intelligence computer specialists that the U.S. government embarked on bulk data mining, in real time or otherwise, of Internet and telephone communication not only of its citizens but also of foreigners, including heads of governments of 35 countries.<sup>79</sup> The District Court's observation in *Klayman* on the bulk data collection and mining undertaken by the NSA of telephone traffic data is instructive:

I cannot imagine a more "indiscriminate" and "arbitrary invasion" than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on "that degree of privacy" that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware "the abridgment of freedom of the people by gradual and silent encroachments by those in power," would be aghast.<sup>80</sup>

Equally important was that court's finding on the efficacy of the bulk surveillance program of the U.S. government: "*the Government does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature.*"<sup>81</sup>

To stem the ensuing backlash, legislative and executive leaders of the U.S. government committed to re-writing current legislation to curb the power of its surveillance agencies.<sup>82</sup> The pressure for reforms increased with the recent release of an unprecedented statement by the eight largest Internet service providers in America calling on the U.S. government to "limit

---

<sup>78</sup>While the U.S. law has been criticized as turning courts into "rubber stamps" which are obliged to issue the order for the installation of recording devices once the applicant law enforcement officer certifies that the information to be recorded is relevant to an ongoing criminal investigation (see Slobogin, *Transaction Investigation* at 154-155), the objection relates to the degree of judicial participation, not to the law's structure.

<sup>79</sup> Costas Pitas, *Report: US Monitored the Phone Calls of 35 World Leaders*, REUTERS <http://worldnews.nbcnews.com/news/2013/10/24/21124561-report-us-monitored-the-phone-calls-of-35-world-leaders> (last visited on 16 December 2013).

<sup>80</sup>Supra note 63 at 114-115 (internal citations omitted).

<sup>81</sup>Supra note 63 at 109 (emphasis supplied).

<sup>82</sup>Dan Roberts, *Patriot Act Author Prepares Bill to Put NSA Bulk Collection 'Out of Business'*, THE GUARDIAN, 10 October 2013 <http://www.theguardian.com/world/2013/oct/10/nsa-surveillance-patriot-act-author-bill>; Andrew Rafferty, *Obama: NSA Reforms Will Give Americans 'More Confidence' in Surveillance Programs*, NBC NEWS, <http://nbcpolitics.nbcnews.com/news/2013/12/05/21776882-obama-nsa-reforms-will-give-americans-more-confidence-in-surveillance-programs> (last visited on 16 December 2013).

surveillance to specific, known users for lawful purposes, and x x x not undertake bulk data collection of Internet communications.”<sup>83</sup> Along the same lines, the Panel’s Report recommended, among others that, “the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes”<sup>84</sup> as such poses a threat to privacy rights, individual liberty and public trust. The Panel’s Report elaborated:

Because international terrorists inevitably leave footprints when they recruit, train, finance, and plan their operations, government acquisition and analysis of such personal information might provide useful clues about their transactions, movements, behavior, identities and plans. It might, in other words, help the government find the proverbial needles in the haystack. *But because such information overwhelmingly concerns the behavior of ordinary, law-abiding individuals, there is a substantial risk of serious invasions of privacy.*

As a report of the National Academy of Sciences (NAS) has observed, the mass collection of such personal information by the government would raise serious “concerns about the misuse and abuse of data, about the accuracy of the data and the manner in which the data are aggregated, and about the possibility that the government could, through its collection and analysis of data, inappropriately influence individuals’ conduct.”

According to the NAS report, “data and communication streams” are ubiquitous:

[They] concern financial transactions, medical records, travel, communications, legal proceedings, consumer preferences, Web searches, and, increasingly, behavior and biological information. This is the essence of the information age — x x x *everyone leaves personal digital tracks in these systems whenever he or she makes a purchase, takes a trip, uses a bank account, makes a phone call, walks past a security camera, obtains a prescription, sends or receives a package, files income tax forms, applies for a loan, e-mails a friend, sends a fax, rents a video, or engages in just about any other activity* x x x x Gathering and analyzing [such data] can play major roles in the prevention, detection, and mitigation of terrorist attacks x x x x [But even] under the pressures of threats as serious as terrorism, the privacy rights and civil liberties that are cherished core values of our nation must not be destroyed x x x x One x x x concern is that law-abiding citizens who come to believe that their behavior is watched too closely by government agencies x x x *may be unduly inhibited from participating in the democratic process, may be*

---

<sup>83</sup>“Global Government Surveillance Reform,” <http://reformgovernmentsurveillance.com/> (last visited on 16 December 2013).

<sup>84</sup> Panel’s Report at 27.

*inhibited from contributing fully to the social and cultural life of their communities, and may even alter their purely private and perfectly legal behavior for fear that discovery of intimate details of their lives will be revealed and used against them in some manner.*<sup>85</sup> (Emphasis supplied)

In lieu of data collection in bulk and data mining, the Panel's Report recommended that such data be held by "private providers or by a private third party,"<sup>86</sup> accessible by American intelligence officials only by order of the FISC, upon showing that the requested information is "relevant to an authorized investigation intended to protect 'against international terrorism or clandestine intelligence activities,'"<sup>87</sup> a more stringent standard than what is required under current federal law.

Finding merit in the core of the Panel's Report's proposal, President Obama ordered a two-step "transition away from the existing program" of telephone data collection in bulk and analysis, first, by increasing the threshold for querying the data and requiring judicial oversight to do so (save in emergency cases), and second, by relinquishing government's possession of the bulk data:

[I]'ve ordered that the transition away from the existing program will proceed in two steps.

Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization, instead of the current three, and I have directed the attorney general to work with the Foreign Intelligence Surveillance Court so that during this transition period, *the database can be queried only after a judicial finding or in the case of a true emergency.*

Next, step two: I have instructed the intelligence community and the attorney general to use this transition period to develop options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address, *without the government holding this metadata itself.* x x x.<sup>88</sup> (Emphasis supplied)

The U.S. spying fiasco offers a cautionary tale on the real danger to privacy of communication caused by the grant of broad powers to the state to place anyone under electronic surveillance without or with minimal judicial oversight. If judicial intervention under U.S. law for real time surveillance of electronic communication did not rein in U.S. spies, the total absence of such intervention under Section 12 of RA 10175 is a blanket legislative authorization for data surveillance and collection in bulk to take place in this country.

---

<sup>85</sup> Id. at 109-111 (internal citations omitted).

<sup>86</sup> Id. at 25.

<sup>87</sup> Id. at 26.

<sup>88</sup> Supra note 1.

***Section 12 Tilts the Balance in Favor  
of Broad State Surveillance Over  
Privacy of Communications Data***

As large parts of the world become increasingly connected, with communications carried on wired or wirelessly and stored electronically, the need to balance the state's national security and public safety interest, on the one hand, with the protection of the privacy of communication, on the other hand, has never been more acute. Allowing the state to undertake extrajudicial, unilateral surveillance and collection of electronic data in bulk which, in the aggregate, is just as revealing of a person's mind as the content of his communication, impermissibly tilts the balance in favor of state surveillance at the expense of communicative and expressive privacy. More than an imbalance in the treatment of equally important societal values, however, such government policy gives rise to fundamental questions on the place of human dignity in civilized society. This concern was succinctly articulated by writers from all over the world protesting the policy of mass surveillance and collection of data in bulk:

With a few clicks of the mouse, the state can access your mobile device, your email, your social networking and Internet searches. It can follow your political leanings and activities and, in partnership with Internet corporations, it collects and stores your data.

The basic pillar of democracy is the inviolable integrity of the individual. x x x [A]ll humans have a right to remain unobserved and unmolested. x x x.

A person under surveillance is no longer free; a society under surveillance is no longer a democracy. [O]ur democratic rights must apply in virtual as in real space.<sup>89</sup>

The Government must maintain fidelity to the 1987 Constitution's guarantee against warrantless searches and seizures, as well as the guarantee of privacy of communication and correspondence. Thus, the Government, consistent with its national security needs, may enact legislation allowing surveillance and data collection in bulk only if **based on individualized suspicion and subject to meaningful judicial oversight**.

---

<sup>89</sup> *World Writers Demand UN Charter to Curb State Surveillance*, AGENCE FRANCE-PRESSE, 10 December 2013, <http://www.globalpost.com/dispatch/news/afp/131210/world-writers-demand-un-charter-curb-state-surveillance>.

***Section 19 of RA 10175 Violative of the  
Free Speech, Free Press, Privacy of Communication  
and Search and Seizure Clauses***

The OSG concedes the unconstitutionality of Section 19 which authorizes the Department of Justice (DOJ) to “issue an order to restrict or block access” to computer data, that is, “any representation of facts, information, or concepts in a form suitable for processing in a computer system,”<sup>90</sup> whenever the DOJ finds such data *prima facie* violative of RA 10175. The OSG's stance on this “take down” clause is unavoidable. Section 19 allows the government to search without warrant the content of private electronic data *and administratively* censor *all* categories of speech. Although censorship or prior restraint is permitted on speech which is pornographic, commercially misleading or dangerous to national security,<sup>91</sup> only pornographic speech is covered by RA 10175 (under Section 4(c)(2) on online child pornography). Moreover, a court order is required to censor or effect prior restraint on protected speech.<sup>92</sup> By allowing the government to electronically search without warrant and administratively censor all categories of speech, specifically speech which is non-pornographic, not commercially misleading and not a danger to national security, which cannot be subjected to censorship or *prior* restraint, Section 19 is unquestionably repugnant to the guarantees of free speech, free expression and free press and the rights to privacy of communication and against unreasonable searches and seizures. Indeed, as a system of *prior* restraint on *all* categories of speech, Section 19 is glaringly unconstitutional.

**ACCORDINGLY**, I vote to **DECLARE UNCONSTITUTIONAL** Article 354 of the Revised Penal Code, insofar as it applies to public officers and public figures, and the following provisions of Republic Act No. 10175, namely: Section 4(c)(1), Section 4(c)(3), Section 7, Section 12, and Section 19, for being violative of Section 2, Section 3(1) Section 4, and Section 21, Article III of the Constitution.



**ANTONIO T. CARPIO**  
Associate Justice

<sup>90</sup> Section 3(e), RA 10175.

<sup>91</sup> *Chavez v. Gonzales*, 569 Phil. 155, 237 (2008), Carpio, *J.*, concurring.

<sup>92</sup> *Iglesia ni Cristo v. Court of Appeals*, G.R. No. 119673, 26 July 1996, 259 SCRA 529, 575-578 (1996) (Mendoza, *J.*, Separate Opinion)