

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, *Respondent*; 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

SERENO, CJ:

The true role of Constitutional Law is to effect an equilibrium between authority and liberty so that rights are exercised within the framework of the law and the laws are enacted with due deference to rights.

Justice Isagani A. Cruz¹

¹ ISAGANI A. CRUZ, CONSTITUTIONAL LAW, 1 (2000).

When the two other branches of government transgress their inherent powers, often out of a well-intentioned zeal that causes an imbalance between authority and liberty, it is the Court's solemn duty to restore the delicate balance that has been upset. This is the difficult task before us now, involving as it does our power of judicial review over acts of a coequal branch.

The task is complicated by the context in which this task is to be discharged: a rapidly evolving information and communications technology, which has been an enormous force for good as well as for evil. Moreover, the Court is forced to grapple with the challenge of applying, to the illimitable cyberspace, legal doctrines that have heretofore been applied only to finite physical space. Fortunately, we have the Constitution as our North Star as we try to navigate carefully the uncharted terrain of cyberspace as the arena of the conflict between fundamental rights and law enforcement.

I concur with the *ponencia* in finding unconstitutional Section 12 of *Cybercrime Prevention Act* on the real-time collection of traffic data and Section 19 on the restriction or blocking of access to computer data. I also adopt the *ponencia*'s discussion of Sections 12 and 19. I write this Separate Opinion, however, to explain further why real-time collection of traffic data may be indispensable in certain cases, as well as to explain how the nature of traffic data *per se* undercuts any expectation of privacy in them.

I also concur with the *ponencia*'s partial invalidation of Section 4(c)(4) on libel insofar as it purports to create criminal liability on the part of persons who receive a libelous post and merely react to it; and of Section 7, in so far as it applies to libel.

However, I dissent from the *ponencia*'s upholding of Section 6 as not unconstitutional in all its applications. I find Section 6 to be unconstitutional insofar as it applies to cyberlibel because of its "chilling effect." Hence, I am writing this Separate Opinion also to explain my dissent on this issue.

I find the rest of the constitutional challenges not proper for a pre-enforcement judicial review and therefore dismissible.

I.

THIS COURT MAY EMPLOY A PRE-ENFORCEMENT JUDICIAL REVIEW OF THE *CYBERCRIME PREVENTION ACT*.

As distinguished from the general notion of judicial power, the power of judicial review especially refers to both the authority and the duty of this Court to determine whether a branch or an instrumentality of government has acted beyond

the scope of the latter's constitutional powers.² It includes the power to resolve cases in which the constitutionality or validity of any treaty, international or executive agreement, law, presidential decree, proclamation, order, instruction, ordinance, or regulation is in question.³ This power, first verbalized in the seminal case *Marbury v. Madison*,⁴ has been exercised by the Philippine Supreme Court since 1902.⁵ The 1936 case *Angara v. Electoral Commission* exhaustively discussed the concept as follows:⁶

The separation of powers is a fundamental principle in our system of government. It obtains not through express provision but by actual division in our Constitution. **Each department of the government has exclusive cognizance of matters within its jurisdiction, and is supreme within its own sphere.** But it does not follow from the fact that the three powers are to be kept separate and distinct that the Constitution intended them to be absolutely unrestrained and independent of each other. **The Constitution has provided for an elaborate system of checks and balances to secure coordination in the workings of the various departments of the government. x x x. And the judiciary in turn, with the Supreme Court as the final arbiter, effectively checks the other departments in the exercise of its power to determine the law, and hence to declare executive and legislative acts void if violative of the Constitution.**

x x x x

As any human production, **our Constitution** is of course lacking perfection and perfectibility, but as much as it was within the power of our people, acting through their delegates to so provide, that instrument **which is the expression of their sovereignty however limited, has established a republican government intended to operate and function as a harmonious whole, under a system of checks and balances, and subject to specific limitations and restrictions provided in the said instrument. The Constitution sets forth in no uncertain language the restrictions and limitations upon governmental powers and agencies. If these restrictions and limitations are transcended it would be inconceivable if the Constitution had not provided for a mechanism by which to direct the course of government along constitutional channels, for then the distribution of powers would be mere verbiage, the bill of rights mere expressions of sentiment, and the principles of good government mere political apothegms.** Certainly, the limitations and restrictions embodied in our Constitution are real as they should be in any living constitution. In the United States where no express constitutional grant is found in their constitution, the possession of this moderating power of the courts, not to speak of its historical origin and development there, has been set at rest by popular acquiescence for a period of more than one and a half centuries. In our case, **this moderating power is granted, if not expressly, by clear implication from section 2 of article VIII of our Constitution.**

² See: *Chavez v. Judicial and Bar Council*, G.R. No. 202242, 17 July 2012, 676 SCRA 579; *Tagolino v. House of Representatives Electoral Tribunal*, G.R. No. 202202, 19 March 2013; *Gutierrez v. House of Representatives Committee on Justice*, G.R. No. 193459, 15 February 2011, 643 SCRA 198; *Francisco v. House of Representatives*, 460 Phil. 830 (2003); *Demetria v. Alba*, 232 Phil. 222 (1987).

³ CONSTITUTION, Art. VIII, Sec. 2(a).

⁴ 5 U.S. 137 (1803).

⁵ *Francisco v. House of Representatives*, supra note 2 (citing *U.S. v. Ang Tang Ho*, 43 Phil 1 [1922]; *McDaniel v. Apacible*, 42 Phil 749 [1922]; *Concepcion v. Paredes*, 42 Phil 599 [1921]; *In re Prautch*, 1 Phil. 132 [1902]; and *Casanovas v. Hord*, 8 Phil 125 [1907]).

⁶ *Angara v. Electoral Commission*, 63 Phil. 139, 156-158 (1936).

The Constitution is a definition of the powers of government. Who is to determine the nature, scope and extent of such powers? The Constitution itself has provided for the instrumentality of the judiciary as the rational way. **And when the judiciary mediates to allocate constitutional boundaries, it does not assert any superiority over the other departments; it does not in reality nullify or invalidate an act of the legislature, but only asserts the solemn and sacred obligation assigned to it by the Constitution to determine conflicting claims of authority under the Constitution and to establish for the parties in an actual controversy the rights which that instrument secures and guarantees to them.** This is in truth all that is involved in what is termed “judicial supremacy” **which properly is the power of judicial review under the Constitution.** (Emphases supplied)

The power of judicial review has since been strengthened in the 1987 Constitution, extending its coverage to the determination of whether 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.⁷ The expansion made the political question doctrine “no longer the insurmountable obstacle to the exercise of judicial power or the impenetrable shield that protects executive and legislative actions from judicial inquiry or review.”⁸ Thus, aside from the test of constitutionality, this Court has been expressly granted the power and the duty to examine whether the exercise of discretion in those areas that are considered political questions was attended with grave abuse.⁹

This moderating power of the Court, however, must be exercised carefully, and only if it cannot be feasibly avoided, as it **involves the delicate exercise of pronouncing an act of a branch or an instrumentality of government unconstitutional, at the risk of supplanting the wisdom of the constitutionally appointed actor with that of the judiciary.**¹⁰ It cannot be overemphasized that our Constitution was so incisively designed that the different branches of government were made the respective experts in their constitutionally assigned spheres.¹¹ Hence, even as the Court dutifully exercises its power of judicial review to check – in this case, the legislature – it must abide by the strict requirements of its exercise under the Constitution. Indeed, “[a] ruling of unconstitutionality frustrates the intent of the elected representatives of the people.”¹²

⁷ *Francisco v. House of Representatives*, supra note 2; *Gutierrez v. House of Representatives Committee on Justice*, supra note 2; CONSTITUTION, Art. VIII, Sec. 1.

⁸ *Oposa v. Factoran*, G.R. No. 101083, 30 July 1993, 224 SCRA 792, 809.

⁹ *Francisco v. House of Representatives*, supra note 2; *Tañada v. Angara*, 338 Phil. 546 (1997); *Oposa v. Factoran*, supra (citing *Llamas v. Orbos*, 279 Phil. 920 [1991]; *Bengzon v. Senate Blue Ribbon Committee*, 203 SCRA 767 [1991]); *Gonzales v. Macaraig*, 191 SCRA 452 [1990]; *Coseteng v. Mitra*, 187 SCRA 377 [1990]; *Daza v. Singson*, 259 Phil. 980 [1989]; and I RECORD, CONSTITUTIONAL COMMISSION 434-436 [1986].

¹⁰ See: *Francisco v. House of Representatives*, supra note 2; *United States v. Raines*, 362 U.S. 17 (1960); and *Angara v. Electoral Commission*, supra note 6.

¹¹ *Morfe v. Mutuc*, 130 Phil. 415 (1968); *Angara v. Electoral Commission*, supra.

¹² *Washington State Grange v. Washington State Republican Party*, 552 U.S. 442, 450 (2008) (citing *Ayotte v. Planned Parenthood of Northern New Eng.*, 546 U. S. 320, 329 [2006]; and *Regan v. Time, Inc.*, 468 U. S. 641, 652 [1984]).

*Demetria v. Alba*¹³ and *Francisco v. House of Representatives*¹⁴ cite the “seven pillars” of the limitations of the power of judicial review, enunciated in the concurring opinion of U.S. Supreme Court Justice Louis Brandeis in *Ashwander v. Tennessee Valley Authority*¹⁵ as follows:

1. The Court will not pass upon the constitutionality of legislation in a **friendly, non-adversary, proceeding**, declining because to decide such questions “is legitimate only in the last resort, and as a necessity in the determination of real, earnest and vital controversy between individuals. It never was the thought that, by means of a friendly suit, a party beaten in the legislature could transfer to the courts an inquiry as to the constitutionality of the legislative act.” x x x.
2. The Court will not “anticipate a question of constitutional law in advance of the necessity of deciding it.” x x x. “It is not the habit of the Court to decide questions of a constitutional nature unless absolutely necessary to a decision of the case.”
3. The Court will not “formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied.” x x x.
4. The Court will not pass upon a constitutional question although properly presented by the record, if there is also present some other ground upon which the case may be disposed of. This rule has found most varied application. Thus, if a case can be decided on either of two grounds, one involving a constitutional question, the other a question of statutory construction or general law, the Court will decide only the latter. x x x.
5. The Court will not pass upon the validity of a statute upon complaint of one who fails to show that he is injured by its operation. x x x. Among the many applications of this rule, none is more striking than the denial of the right of challenge to one who lacks a personal or property right. Thus, the challenge by a public official interested only in the performance of his official duty will not be entertained. x x x.
6. The Court will not pass upon the constitutionality of a statute at the instance of one who has availed himself of its benefits. x x x.
7. “When the validity of an act of the Congress is drawn in question, and even if a serious doubt of constitutionality is raised, it is a cardinal principle that **this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.**” (Citations omitted, emphases supplied)

These are specific safeguards laid down by the Court when it exercises its power of judicial review. Thus, as a threshold condition, the power of judicial review may be invoked only when the following four stringent requirements are satisfied: (a) there must be an actual case or controversy; (b) petitioners must possess *locus standi*; (c) the question of constitutionality must be raised at the

¹³ *Supra* note 2.

¹⁴ *Supra* note 2, at 922-923.

¹⁵ *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288 (1936).

earliest opportunity; and (d) the issue of constitutionality must be the *lis mota* of the case.¹⁶

Specifically focusing on the first requisite, it necessitates that there be an existing case or controversy that is appropriate or ripe for determination as opposed to a case that is merely conjectural or anticipatory.¹⁷ The case must involve a definite and concrete issue concerning real parties with conflicting legal rights and opposing legal claims, admitting of a specific relief through a decree conclusive in nature.¹⁸ The “ripeness” for adjudication of the controversy is generally treated in terms of actual injury to the plaintiff.¹⁹ Hence, a question is ripe for adjudication when the act being challenged has had a direct adverse effect on the individual challenging it. The case should not equate with a mere request for an opinion or an advice on what the law would be upon an abstract, hypothetical, or contingent state of facts.²⁰ As explained in *Angara v. Electoral Commission*:²¹

[The] power of **judicial review is limited to actual cases and controversies to be exercised after full opportunity of argument by the parties**, and limited further to the constitutional question raised or the very *lis mota* presented. **Any attempt at abstraction could only lead to dialectics and barren legal questions and to sterile conclusions of wisdom, justice or expediency of legislation.** More than that, courts accord the presumption of constitutionality to legislative enactments, not only because the legislature is presumed to abide by the Constitution but also because **the judiciary in the determination of actual cases and controversies must reflect the wisdom and justice of the people as expressed through their representatives in the executive and legislative departments of the government.** (Emphases supplied)

According to one of the most respected authorities in American constitutional law, Professor Paul A. Freund, the actual case or controversy requirement is a crucial restraint on the power of unelected judges to set aside the acts of the people’s representative to Congress.²² Furthermore, he explains:²³

The rules of “case and controversy” can be seen as the necessary corollary of this vast power – necessary for its wise exercise and its popular acceptance. **By declining to give advisory opinions, the Court refrains from intrusion into**

¹⁶ *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, G.R. No. 178552, 5 October 2010, 632 SCRA 146; *David v. Macapagal-Arroyo*, 522 Phil. 705, 753 (2006); *Francisco v. House of Representatives*, supra note 2, at 923-924; *Angara v. Electoral Commission*, supra note 6.

¹⁷ *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra.

¹⁸ *Information Technology Foundation of the Philippines v. Commission on Elections*, 499 Phil. 281 (2005) (citing *Aetna Life Insurance Co. v. Hayworth*, 300 U.S. 227 [1937]); *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra; *David v. Macapagal-Arroyo*, supra note 16; *Francisco v. House of Representatives*, supra note 2; *Angara v. Electoral Commission*, supra note 6.

¹⁹ *Lozano v. Nograles*, G.R. Nos. 187883 & 187910, 16 June 2009, 589 SCRA 356.

²⁰ *Information Technology Foundation of the Philippines v. Commission on Elections*, supra note 18; *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra; *Lozano v. Nograles*, supra.

²¹ *Angara v. Electoral Commission*, supra note 6, at 158-159.

²² VICENTE V. MENDOZA, JUDICIAL REVIEW OF CONSTITUTIONAL QUESTIONS: CASES AND MATERIALS 91 (2nd Ed. 2013) (MENDOZA) (citing Paul A. Freund, “The Supreme Court,” in TALKS ON AMERICAN LAW 81 [H. J. Berman Rev. Ed. 1972]).

²³ Paul A. Freund, “The Supreme Court,” in TALKS ON AMERICAN LAW 81 (H. J. Berman Rev. Ed. 1972) (quoted in MENDOZA, supra)

the lawmaking process. By requiring a concrete case with litigants adversely affected, the Court helps itself to avoid premature, abstract, ill-informed judgments. By placing a decision on a non-constitutional ground whenever possible, the **Court gives the legislature an opportunity for sober second thought, an opportunity to amend the statute to obviate the constitutional question, a chance to exercise that spirit of self-scrutiny and self-correction** which is the essence of a successful democratic system. (Emphases supplied)

While the actual controversy requirement has been largely interpreted in the light of the implications of the assailed law *vis-à-vis* the legally demandable rights of real parties and the direct injury caused by the assailed law, **we have also exceptionally recognized the possibility of lodging a constitutional challenge sans a pending case involving a directly injured party.** In *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*,²⁴ we conceded the possibility of a **pre-enforcement judicial review** of a penal statute, **so long as there is a real and credible threat of prosecution involving the exercise of a constitutionally protected conduct or activity.**²⁵ We noted that the petitioners therein **should not be required to expose themselves to criminal prosecution before they could assail the constitutionality of a statute, especially in the face of an imminent and credible threat of prosecution.**²⁶

On 5 February 2013, this Court extended indefinitely the temporary restraining order enjoining the government from implementing and enforcing the *Cybercrime Prevention Act of 2012*. As the assailed law is yet to be enforced, I believe that in order to give due course to the Petitions, we would have to test their qualification for pre-enforcement judicial review of the assailed law and its provisions.

In discussing the requirements of a pre-enforcement judicial review, we refer to our ruling in *Southern Hemisphere*. We declined to perform a pre-enforcement judicial review of the assailed provisions of the *Human Security Act of 2007*, because petitioners failed to show that the law forbade them from exercising or performing a constitutionally protected conduct or activity that they sought to do. We also explained that the obscure and speculative claims of the petitioners therein that they were being subjected to sporadic “surveillance” and tagged as “communist fronts” were insufficient to reach the level of a credible threat of prosecution that would satisfy the actual-controversy requirement. Thus, from the facts they had shown, we ruled that the Court was merely “being lured to render an advisory opinion, which [was] not its function.”²⁷

²⁴ See: *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16.

²⁵ *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16.

²⁶ Nevertheless, we ultimately found that the petitioners therein failed to show their entitlement to a pre-enforcement judicial review of the *Human Security Act of 2007*. *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16 (quoting *Holder v. Humanitarian Law Project*, 561 U.S. [unpaginated] [2010]); *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118 (2007); See also: *Babbitt v. United Farm Workers National Union*, 442 U.S. 289 (1979); *Doe v. Bolton*, 410 U.S. 179, 188-189 (1973) (citing *Epperson v. Arkansas*, 393 U.S. 97 [1968]);

²⁷ *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16.

We then drew a distinction between the facts in *Southern Hemisphere* and those in *Holder v. Humanitarian Law Project*, a case decided by the United States Supreme Court. We noted that in *Holder*, a pre-enforcement judicial review of the assailed criminal statute was entertained because the plaintiffs therein had successfully established that there was a genuine threat of imminent prosecution against them, thereby satisfying the actual-controversy requirement. The case concerned a new law prohibiting the grant of material support or resources to certain foreign organizations engaged in terrorist activities. Plaintiffs showed that they had been providing material support to those declared as foreign terrorist organizations; and that, should they continue to provide support, there would be a credible threat of prosecution against them pursuant to the new law. The plaintiffs therein insisted that they only sought to facilitate the lawful, nonviolent purposes of those groups – such as the latter’s political and humanitarian activities – and that the material-support law would prevent the plaintiffs from carrying out their rights to free speech and to association. Based on the foregoing considerations, the U.S. Supreme Court concluded that the claims of the plaintiffs were suitable for judicial review, as there was a justiciable case or controversy.

We may thus cull from the foregoing cases that an anticipatory petition assailing the constitutionality of a criminal statute that is yet to be enforced may be exceptionally given due course by this Court when the following circumstances are shown: (a) the challenged law or provision **forbids a constitutionally protected conduct or activity** that a petitioner seeks to do; (b) a **realistic, imminent, and credible threat or danger of sustaining a direct injury or facing prosecution** awaits the petitioner should the prohibited conduct or activity be carried out; and (c) the **factual circumstances** surrounding the prohibited conduct or activity sought to be carried out are **real, not hypothetical and speculative, and are sufficiently alleged and proven**.²⁸ It is only when these minimum conditions are satisfied can there be a finding of a justiciable case or actual controversy worthy of this Court’s dutiful attention and exercise of pre-enforcement judicial review. Furthermore, since the issue of the propriety of resorting to a pre-enforcement judicial review is subsumed under the threshold requirement of actual case or controversy, we need not go through the merits at this stage. **Instead, the determination of whether or not to exercise this power must hinge solely on the allegations in the petition, regardless of the petitioner’s entitlement to the claims asserted.**

A review of the petitions before us shows that, save for the Disini Petition,²⁹ all petitions herein have failed to establish that their claims call for this Court’s exercise of its power of pre-enforcement judicial review.

²⁸ See: *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16; *De Castro v. Judicial and Bar Council*, G.R. No. 202242, 17 July 2012, 676 SCRA 579 (citing *Buckley v. Valeo*, 424 U.S. 1, 113-118 [1976]; *Regional Rail Reorganization Act Cases*, 419 U.S. 102, 138-148 [1974]); *Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010); *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118 (2007); *Babbitt v. United Farm Workers National Union*, 442 U.S. 289 (1979) (citing *Regional Rail Reorganization Act Cases*, 419 U.S. 102 [1974]; *Steffel v. Thompson*, 415 U.S. 452 [1974]; *O’Shea v. Littleton*, 414 U.S. 488 [1974]; *Doe v. Bolton*, 410 U.S. 179 [1973]; *Younger v. Harris*, 401 U.S. 37 [1971]; *Golden v. Zwickler*, 394 U.S. 103 [1969]; *Epperson v. Arkansas*, 393 U.S. 97 [1968]; *Evers v. Dwyer*, 358 U.S. 202 [1958]; *Pierce v. Society of Sisters*, 268 U.S. 510 [1925]; *Pennsylvania v. West Virginia*, 262 U.S. 553 [1923]).

²⁹ G.R. No. 203325, *Jose Jesus M. Disini, Jr. v. The Secretary of Justice*.

Petitioners allege that they are users of various information and communications technologies (ICT) as media practitioners, journalists, lawyers, businesspersons, writers, students, Internet and social media users, and duly elected legislators. **However, except for the Petition of *Disini*, none of the other petitioners have been able to show that they are facing an imminent and credible threat of prosecution or danger of sustaining a direct injury.** Neither have they established any real, factual circumstances in which they are at risk of direct injury or prosecution, should those acts continue to be carried out.

They have simply posed hypothetical doomsday scenarios and speculative situations, such as round-the-clock, Big-Brother-like surveillance; covert collection of digital and personal information by the government; or a wanton taking down of legitimate websites.³⁰ Others have made outright legal queries on how the law would be implemented in various circumstances, such as when a person disseminates, shares, affirms, “likes,” “retweets,” or comments on a potentially libelous article.³¹ A considerable number of them have merely raised legal conclusions on the implication of the new law, positing that the law would *per se* prevent them from freely expressing their views or comments on intense national issues involving public officials and their official acts.³² **While these are legitimate concerns of the public, giving in to these requests for advisory opinion would amount to an exercise of the very same function withheld from this Court by the actual controversy requirement entrenched in Section 1, Article III of our Constitution.**

The Petition of *Disini* is the only pleading before the Court that seems to come close to the actual-controversy requirement under the Constitution. What sets the Petition apart is that it does not merely allege that petitioners therein are ICT users who have posted articles and blogs on the Internet. The Petition also cites particular blogs or online articles of one of the petitioners who was critical of a particular legislator.³³ Furthermore, it refers to a newspaper article that reported the legislator’s intent to sue under the new law, once it takes effect. The pertinent portion of the Petition reads:³⁴

5. Petitioners are all users of the Internet and social media. **Petitioner Ernesto Sonido, Jr. (“Petitioner Sonido”), in particular, maintains the blog “Baratillo Pamphlet” over the Internet.**

³⁰ See Petition of *Disini* (G.R. No. 203335), pp. 22-23, 26-27; Petition of Reyes (G.R. No. 203407), p. 25; Petition of Castillo, (G.R. No. 203454), pp. 10-11; Petition of Cruz (G.R. No. 203469), pp. 39-40; Petition of Philippine Internet Freedom Alliance (G.R. No. 203518), p. 9.

³¹ See Petition of Adonis (G.R. No. 203378), p. 29; Petition of Sta. Maria (G.R. No. 203440), p. 22; Petition of Cruz (G.R. No. 203469), pp. 60-61; Petition of Philippine Bar Association (GRN 203501), p. 19; Petition of Colmenares (G.R. No. 203509), p. 15; Petition of National Press Club of the Philippines (G.R. No. 203515), pp. 16-17.

³² See Petition of Adonis (G.R. No. 203378), p. 33; Petition of National Union of Journalists of the Philippines (G.R. No. 203453), p. 11; Petition of National Press Club of the Philippines (G.R. No. 203515), p. 9; Petition of Philippine Internet Freedom Alliance (G.R. No. 203518), pp. 47-48; Petition of Philippine Bar Association (GRN 203501), p. 19.

³³ See Petition of *Disini* (G.R. No. 203335), pp. 10-12.

³⁴ Petition of *Disini* (G.R. No. 203335), pp. 10-12.

6. **On August 22, 2012 and September 7, 2012, Petitioner Sonido posted 2 blogs entitled “Sotto Voce: Speaking with Emphasis” and “Sotto and Lessons on Social Media” in which he expressed his opinions regarding Senator Vicente “Tito” Sotto III’s (“Senator Sotto”) alleged plagiarism of online materials for use in his speech against the Reproductive Health Bill.**
7. **On August 30, 2012, Senator Sotto disclosed that the Cybercrime Bill was already approved by the Senate and the House of Representatives and was merely awaiting the President’s signature. He then warned his critics that once signed into law, the Cybercrime Bill will penalize defamatory statements made online.** To quote Senator Sotto:

“Walang ginawa yan [internet users] umaga, hapon, nakaharap sa computer, target nuon anything about the [Reproductive Health] Bill. Ganun ang strategy nun and unfortunately, di panapipirmahan ang Cybercrime bill. Pwede na sana sila tanungin sa pagmumura at pagsasabi ng di maganda. Sa Cybercrime bill, magkakaroon ng accountability sa kanilang pinagsasabi, penalties na haharapin, same penalties as legitimate journalists, anything that involves the internet,” he said.
8. The threat of criminal prosecution that was issued by Senator Sotto affected not only bloggers like Petitioner Sonido but all users of the Internet and social media as the other Petitioners herein who utilize online resources to post comments and express their opinions about social issues.
9. The President finally signed the Cybercrime Act into law on September 12, 2012.
10. **With the passage of the Cybercrime Act, the threat that was issued by Senator Sotto against his online critics has become real.** (Emphases and italics supplied)

The Petition of *Disini* appears to allege sufficient facts to show a realistic, imminent, and credible danger that at least one of its petitioners may sustain a direct injury should respondents proceed to carry out the prohibited conduct or activity. First, there was a citation not only of a particular blog, but also of two potentially libelous entries in the blog. Second, the plausibly libelous nature of the articles was specifically described. Third, the subject of the articles, Senator Vicente Sotto III, was alleged to have made threats of using the assailed statute to sue those who had written unfavorably about him; a verbatim quote of the legislator’s threat was reproduced in the Petition. Fourth, the person potentially libeled is a nationally elected legislator.

This combination of factual allegations seems to successfully paint a realistic possibility of criminal prosecution under Section 4(c)(4) of a specific person under the assailed law. Consequently, there is now also a possibility of the writer being penalized under Section 6, which raises the penalty for crimes such as libel by one degree when committed through ICT. The alleged facts would also open the possibility of his being charged twice under Section 4(c)(4) and Article 353 of the Revised Penal Code by virtue of Section 7. Furthermore, since

he might become a suspect in the crime of libel, his online activities might be in danger of being investigated online by virtue of Section 12 or his access to computer data might be restricted under Section 19.

Therefore, it is submitted that the Court must limit its discussion of the substantive merits of the cases to the Petition of *Disini*, at the most and only on the provisions questioned therein.

II. PARTICULAR PROVISIONS OF THE CYBERCRIME PREVENTION ACT MAY BE FACIALY INVALIDATED.

A facial challenge refers to the call for the scrutiny of an entire law or provision by identifying its flaws or defects, not only on the basis of its actual operation on the attendant facts raised by the parties, but also on the assumption or prediction that the very existence of the law or provision is repugnant to the Constitution.³⁵ This kind of challenge has the effect of totally annulling the assailed law or provision, which is deemed to be unconstitutional *per se*. The challenge is resorted to by courts, especially when there is no instance to which the law or provision can be validly applied.³⁶

In a way, a facial challenge is a deviation from the general rule that Courts should only decide the invalidity of a law “as applied” to the actual, attending circumstances before it.³⁷ An as-applied challenge refers to the localized invalidation of a law or provision, limited by the factual milieu established in a case involving real litigants who are actually before the Court.³⁸ This kind of challenge is more in keeping with the established canon of adjudication that “the court should not form a rule of constitutional law broader than is required by the precise facts to which it is applied.”³⁹ Should the petition prosper, **the unconstitutional aspects of the law will be carved away by invalidating its improper applications on a case-to-case basis.**⁴⁰ For example, in *Ebralinag v. Division of Superintendent of Schools of Cebu*,⁴¹ the Court exempted petitioner-members of the religious group Jehovah’s Witness from the application of the *Compulsory Flag Ceremony in Educational Institutions Act* on account of their religious beliefs. The Court ruled that the law requiring them to salute the flag, sing the national anthem, and recite the patriotic pledge cannot be enforced against them at the risk of expulsion, because the law violated their freedom of religious

³⁵ *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16 (citing *David v. Macapagal-Arroyo*, supra note 16; *Romualdez v. Commission on Elections*, 576 Phil. 357 (2008)).

³⁶ *Estrada v. Sandiganbayan*, 421 Phil. 290 (2001); *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16.

³⁷ *Id.*

³⁸ *See: Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, G.R. No. 178552, supra note 16.

³⁹ *Francisco v. House of Representatives*, supra note 2 (citing *Estrada v. Desierto*, [Sep. Op. of J. Mendoza], 406 Phil. 1 [2001]; *Demetria v. Alba*, supra note 2; *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288 [1936]).

⁴⁰ *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16; *David v. Macapagal-Arroyo*, supra note 16.

⁴¹ G.R. No. 95770, 1 March 1993, 219 SCRA 256.

expression. In effect, the law was deemed unconstitutional insofar as their religious beliefs were concerned.

Because of its effect as a total nullification, the facial invalidation of laws is deemed to be a “manifestly strong medicine” that must be used sparingly and only as a last resort.⁴² The general disfavor towards it is primarily due to the “combination of the relative remoteness of the controversy, the impact on the legislative process of the relief sought, and above all the speculative and amorphous nature of the required line-by-line analysis of detailed statutes.”⁴³ Claims of facial invalidity “raise the risk of ‘premature interpretation of statutes on the basis of factually barebones records.’”⁴⁴

A. Section 6 – Increase of Penalty by One Degree

Section 6 was worded to apply to all existing penal laws in this jurisdiction. Due to the sheer extensiveness of the applicability of this provision, I believe it unwise to issue a wholesale facial invalidation thereof, especially because of the insufficiency of the facts that would allow the Court to make a conclusion that the provision has no valid application.

Alternatively, the discussion can be limited to the allegations raised in the Petition of *Disini* concerning the right to free speech. The Petition asserts that Section 6 (on the increase of penalty by one degree), in conjunction with the provision on cyberlibel, has the combined chilling effect of curtailing the right to free speech. The Petition posits that the law “imposes heavier penalties for online libel than paper-based libel” in that the imposable penalty for online libel is now increased from *prisión correccional* in its minimum and medium periods (6 months and 1 day to 4 years and 2 months) to *prisión mayor* in its minimum and medium periods (6 years and 1 day to 10 years).⁴⁵

The *ponencia* correctly holds that libel is not a constitutionally protected conduct. It is also correct in holding that, generally, penal statutes cannot be invalidated on the ground that they produce a “chilling effect,” since by their very nature, they are intended to have an *in terrorem* effect (benign chilling effect)⁴⁶ to prevent a repetition of the offense and to deter criminality.⁴⁷ The “chilling effect” is therefore equated with and justified by the intended *in terrorem* effect of penal provisions.

⁴² *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16; *David v. Macapagal-Arroyo*, supra note 16; *Estrada v. Sandiganbayan*, 421 Phil. 290 (2001).

⁴³ *Id.*

⁴⁴ *Washington State Grange v. Washington State Republican Party*, 552 U.S. 442, 449 (2008) (citing *Sabri v. United States*, 541 U. S. 600, 609 [2004]).

⁴⁵ Petition of *Disini*, pp. 9-10. The computation of the imposable penalty in the Petition seems to be erroneous. Insofar as the crime of libel is concerned, I have discussed below that the imposable penalty in libel qualified by the use of ICT should be *prisión correccional* in its maximum period to *prisión mayor* in its minimum period.

⁴⁶ *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 16.

⁴⁷ *The Philippine Railway Co. v. Geronimo Paredes*, 64 Phil. 129 (1936).

This does not mean, however, that the Constitution gives Congress the *carte blanche* power to indiscriminately impose and increase penalties. While the determination of the severity of a penalty is a prerogative of the legislature, when laws and penalties affect free speech, it is beyond question that the Court may exercise its power of judicial review to determine whether there has been a grave abuse of discretion in imposing or increasing the penalty. The Constitution's command is clear: "No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances." Thus, **when Congress enacts a penal law affecting free speech and accordingly imposes a penalty that is so discouraging that it effectively creates an invidious chilling effect, thus impeding the exercise of speech and expression altogether, then there is a ground to invalidate the law. In this instance, it will be seen that the penalty provided has gone beyond the *in terrorem* effect needed to deter crimes and has thus reached the point of encroachment upon a preferred constitutional right.** I thus vote to facially invalidate Section 6 insofar as it applies to the crime of libel.

As will be demonstrated below, the confluence of the effects of the increase in penalty under this seemingly innocuous provision, insofar as it is applied to libel, will practically result in chilling the right of the people to free speech and expression.

Section 6 creates an additional in terrorem effect on top of that already created by Article 355 of the Revised Penal Code

The basic postulate of the classical penal system on which our *Revised Penal Code* is based is that humans are rational and calculating beings who guide their actions by the principles of pleasure and pain.⁴⁸ They refrain from criminal acts if threatened with punishment sufficient to cancel the hope of possible gain or advantage in committing the crime.⁴⁹ This consequence is what is referred to as the *in terrorem* effect sought to be created by the *Revised Penal Code* in order to deter the commission of a crime.⁵⁰ Hence, in the exercise of the people's freedom of speech, they carefully decide whether to risk publishing materials that are potentially libelous by weighing the severity of the punishment – if and when the speech turns out to be libelous – against the fulfillment and the benefits to be gained by them.

Our *Revised Penal Code* increases the imposable penalty when there are attending circumstances showing a *greater perversity* or an *unusual criminality* in the commission of a felony.⁵¹ The intensified punishment for these so-called aggravating circumstances is grounded on various reasons, which may be

⁴⁸ RAMON C. AQUINO, *THE REVISED PENAL CODE – VOL. 1*, 3 (1961) (AQUINO).

⁴⁹ *Id.*

⁵⁰ *See* AQUINO, at 8-11.

⁵¹ *Id.* at 277; LUIS B. REYES, *THE REVISED PENAL CODE – CRIMINAL LAW, BOOK ONE*, 328 (2008) (REYES).

categorized into (1) the motivating power itself, (2) the place of commission, (3) the means and ways employed, (4) the time, or (5) the personal circumstances of the offender or of the offended party.⁵² Based on the aforementioned basic postulate of the classical penal system, this is an additional *in terrorem* effect created by the *Revised Penal Code*, which targets the deterrence of a resort to *greater perversity* or to an *unusual criminality* in the commission of a felony.

Section 4(c)(4) of the *Cybercrime Prevention Act* expressly amended Article 355 of the *Revised Penal Code*, thereby clarifying that the use of a “computer system or any other similar means” is a way of committing libel. On the other hand, Section 6 of the *Cybercrime Prevention Act* introduces a qualifying aggravating circumstance, which reads:

SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, **if committed by, through and with the use of information and communications technologies** shall be covered by the relevant provisions of this Act: *Provided*, That the **penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code**, as amended, and special laws, as the case may be. (Emphases supplied)

A perfunctory application of the aforementioned sections would thus suggest the amendment of the provision on libel in the *Revised Penal Code*, which now appears to contain a graduated scale of penalties as follows:

ARTICLE 355. *Libel by Means Writings or Similar Means*. — A libel committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means, shall be punished by *prisión 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.

[**Libel committed by, through and with the use of a computer system or any other similar means which may be devised in the future** shall be punished by⁵³ *prisión correccional* in its maximum period to *prisión mayor* in its minimum period]. (Emphases supplied)

Section 6 effectively creates an additional *in terrorem* effect by introducing a qualifying aggravating circumstance: the use of ICT. This additional burden is on top of that already placed on the crimes themselves, since the *in terrorem* effect of the latter is already achieved through the original penalties imposed by the *Revised Penal Code*. Consequently, another consideration is added to the calculation of penalties by the public. It will now have to weigh not only whether to exercise freedom of speech, but also whether to exercise this freedom through ICT.

⁵² *People v. Lab-ao*, 424 Phil. 482 (2002); REYES, *supra*.

⁵³ See REVISED PENAL CODE, Art. 61 (on rules for graduating penalties); REYES, *supra*, at 705-706 (2008); Cf.: *People v. Medroso*, G.R. No. L-37633, 31 January 1975, 62 SCRA 245.

One begins to see at this point how the exercise of freedom of speech is clearly burdened. The Court can take judicial notice of the fact that ICTs are fast becoming the most widely used and accessible means of communication and of expression. Educational institutions encourage the study of ICT and the acquisition of the corresponding skills. Businesses, government institutions and civil society organizations rely so heavily on ICT that it is no exaggeration to say that, without it, their operations may grind to a halt. News organizations are increasingly shifting to online publications, too. The introduction of social networking sites has increased public participation in socially and politically relevant issues. In a way, the Internet has been transformed into “freedom parks.” Because of the inextricability of ICT from modern life and the exercise of free speech and expression, I am of the opinion that the increase in penalty *per se* effectively chills a significant amount of the exercise of this preferred constitutional right.

The chill does not stop there. As will be discussed below, **this increase in penalty has a domino effect on other provisions in the Revised Penal Code thereby further affecting the public’s calculation of whether or not to exercise freedom of speech.** It is certainly disconcerting that these effects, in combination with the increase in penalty *per se*, clearly operate to tilt the scale heavily against the exercise of freedom of speech.

The increase in penalty also results in the imposition of harsher accessory penalties.

Under the Revised Penal Code, there are accessory penalties that are inherent in certain principal penalties. Article 42 thereof provides that the principal (afflictive) penalty of *prisión mayor* carries with it the accessory penalty of temporary absolute disqualification. According to Article 30, this accessory penalty shall produce the following effects:

1. The **deprivation of the public offices and employments** which the offender may have held, even if conferred by popular election.
2. The **deprivation of the right to vote** in any election for any popular elective office or to be elected to such office.
3. The **disqualification for the offices or public employments** and for the exercise of any of the rights mentioned.

In case of temporary disqualification, such disqualification as is comprised in **paragraphs 2 and 3 of this article shall last during the term of the sentence.**

4. The **loss of all right to retirement pay or other pension for any office formerly held.** (Emphases supplied)

Furthermore, the accessory penalty of **perpetual** special disqualification from the right of suffrage shall be meted out to the offender. Pursuant to Article 32, this penalty means that the offender shall be **perpetually** deprived of the right (a) to vote in any popular election for any public office; (b) to be elected to that office; and (c) to hold any public office.⁵⁴ This perpetual special disqualification will only be wiped out if expressly remitted in a pardon.

On the other hand, Article 43 provides that when the principal (correctional) penalty of *prisión correccional* is meted out, the offender shall also suffer the accessory penalty of **suspension from public office and from the right to follow a profession or calling during the term of the sentence**. While the aforementioned principal penalty may carry with it the accessory penalty of perpetual special disqualification from the right of suffrage, it will only be imposed upon the offender if the duration of imprisonment exceeds 18 months.

Before the *Cybercrime Prevention Act*, the imposable penalty for libel under Art. 355 of the Revised Penal Code, even if committed by means of ICT, is *prisión correccional* in its minimum and medium periods. Under Section 6 of the *Cybercrime Prevention Act*, the imposable penalty for libel qualified by ICT is now increased to *prisión correccional* in its maximum period to *prisión mayor* in its minimum period.⁵⁵ Consequently, it is now possible for the above-enumerated harsher accessory penalties for *prisión mayor* to attach depending on the presence of mitigating circumstances.

Hence, the public will now have to factor this change into their calculations, which will further burden the exercise of freedom of speech through ICT.

The increase in penalty neutralizes the full benefits of the law on probation, effectively threatening the public with the guaranteed imposition of imprisonment and the accessory penalties thereof.

Probation⁵⁶ is a special privilege granted by the State to penitent, qualified offenders who immediately admit to their liability and thus renounce the right to appeal. In view of their acceptance of their fate and willingness to be reformed, the State affords them a chance to avoid the stigma of an incarceration record by making them undergo rehabilitation outside prison.

⁵⁴ See: *Jalosjos v. Commission on Elections*, G.R. Nos. 193237 and 193536, 9 October 2012, 683 SCRA 1 (citing *Lacuna v. Abes*, 133 Phil. 770, 773-774 [1968]); *Aratea v. Commission on Elections*, G.R. No. 195229, 9 October 2012, 683 SCRA 105.

⁵⁵ See REVISED PENAL CODE, Art. 61 (on rules for graduating penalties); REYES, *supra* note 51, at 705-706; *cf.*: *People v. Medroso*, G.R. No. L-37633, 31 January 1975, 62 SCRA 245.

⁵⁶ Probation Law; *Francisco v. Court of Appeals*, 313 Phil. 241 (1995); and *Baclayon v. Mutia*, 241 Phil. 126 (1984). See: *Del Rosario v. Rosero*, 211 Phil. 406 (1983).

Section 9 of Presidential Decree No. (P.D.) 968, as amended – otherwise known as the *Probation Law* – provides as follows:

Sec. 9. *Disqualified Offenders.* — The benefits of this Decree shall not be extended to those:

- (a) **sentenced to serve a maximum term of imprisonment of more than six years;**
- (b) convicted of subversion or any crime against the national security or the public order;
- (c) who have previously been convicted by final judgment of an offense punished by imprisonment of not less than one month and one day and/or a fine of not less than Two Hundred Pesos;
- (d) who have been once on probation under the provisions of this Decree; and
- (e) who are already serving sentence at the time the substantive provisions of this Decree became applicable pursuant to Section 33 hereof. (Emphasis supplied)

Pursuant to Article 355 of the Revised Penal Code, libel is punishable by *prisión correccional* in its minimum (from 6 months and 1 day to 2 years and 4 months) and medium (from 2 years, 4 months, and 1 day to 4 years and 2 months) periods. However, in the light of the increase in penalty by one degree under the *Cybercrime Prevention Act*, libel qualified by the use of ICT is now punishable by *prisión correccional* in its maximum period (from 4 years, 2 months and 1 day to 6 years) to *prisión mayor* in its minimum period (from 6 years and 1 day to 8 years).⁵⁷ This increased penalty means that if libel is committed through the now commonly and widely used means of communication, ICT, libel becomes a non-probationable offense.

One of the features of the *Probation Law* is that it suspends the execution of the sentence imposed on the offender.⁵⁸ In *Moreno v. Commission on Elections*,⁵⁹ we reiterated our discussion in *Baclayon v. Mutia*⁶⁰ and explained the effect of the suspension as follows:

In *Baclayon v. Mutia*, the Court declared that an order placing defendant on probation is not a sentence but is rather, in effect, a suspension of the imposition of sentence. We held that the **grant of probation to petitioner suspended the imposition of the principal penalty of imprisonment, as well as the accessory penalties of suspension from public office and from the right to follow a profession or calling, and that of perpetual special disqualification from the right of suffrage.** We thus deleted from the order granting probation the paragraph which required that petitioner refrain from continuing with her teaching profession.

⁵⁷ See REVISED PENAL CODE, Art. 61 (on rules for graduating penalties); REYES, *supra* note 51, at 705-706; *Cf.*: *People v. Medroso*, G.R. No. L-37633, 31 January 1975, 62 SCRA 245.

⁵⁸ Probation Law, Sec. 4.

⁵⁹ *Moreno v. Commission on Elections*, G.R. No. 168550, 10 August 2006, 498 SCRA 547.

⁶⁰ *Baclayon v. Mutia*, 241 Phil. 126 (1984).

Applying this doctrine to the instant case, **the accessory penalties of suspension from public office, from the right to follow a profession or calling, and that of perpetual special disqualification from the right of suffrage, attendant to the penalty of *arresto mayor* in its maximum period to *prisión correccional* in its minimum period imposed upon Moreno were similarly suspended upon the grant of probation.**

It appears then that **during the period of probation, the probationer is not even disqualified from running for a public office because the accessory penalty of suspension from public office is put on hold for the duration of the probation.** (Emphases supplied)

It is not unthinkable that some people may risk a conviction for libel, considering that they may avail themselves of the privilege of probation for the sake of exercising their cherished freedom to speak and to express themselves. **But when this seemingly neutral technology is made a qualifying aggravating circumstance to a point that a guaranteed imprisonment would ensue, it is clear that the *in terrorem* effect of libel is further magnified, reaching the level of an invidious chilling effect.** The public may be forced to forego their prized constitutional right to free speech and expression in the face of as much as eight years of imprisonment, like the sword of Damocles hanging over their heads.

Furthermore, it should be noted that one of the effects of probation is the suspension not only of the penalty of imprisonment, but also of the accessory penalties attached thereto. Hence, in addition to the *in terrorem* effect supplied by the criminalization of a socially intolerable conduct and the *in terrorem* effect of an increase in the duration of imprisonment in case of the presence of an aggravating circumstance, the *Revised Penal Code* threatens further⁶¹ by attaching accessory penalties to the principal penalties.

Section 6 increases the prescription periods for the crime of cyberlibel and its penalty to 15 years.

Crimes and their penalties prescribe. The *prescription of a crime* refers to the loss or waiver by the State of its right to *prosecute* an act prohibited and punished by law.⁶² It commences from the day on which the crime is discovered by the offended party, the authorities or their agents.⁶³ On the other hand, the *prescription of the penalty* is the loss or waiver by the State of its right to *punish* the convict.⁶⁴ It commences from the date of evasion of service after final sentence.

⁶¹ See generally: *Monsanto v. Factoran*, G.R. No. 78239, 9 February 1989, 170 SCRA.

⁶² AQUINO, *supra* note 48, at 695-696 (citing *People v. Montenegro*, 68 Phil 659 [1939]; *People v. Moran*, 44 Phil. 387, 433 [1923]; *Santos v. Superintendent*, 55 Phil. 345 [1930]).

⁶³ *Id.*

⁶⁴ *Id.*

Hence, in the *prescription of crimes*, it is the penalty prescribed by law that is considered; in the *prescription of penalties*, it is the penalty imposed.⁶⁵

By setting a prescription period for crimes, the State by an act of grace surrenders its right to *prosecute* and declares the offense as no longer subject to prosecution after a certain period.⁶⁶ It is an amnesty that casts the offense into oblivion and declares that the offenders are now at liberty to return home and freely resume their activities as citizens.⁶⁷ They may now rest from having to preserve the proofs of their innocence, because the proofs of their guilt have been blotted out.⁶⁸

The Revised Penal Code sets prescription periods for crimes according to the following classification of their penalties:

ARTICLE 90. *Prescription of Crimes.* — Crimes punishable by death, *reclusión perpetua* or *reclusión temporal* shall prescribe in twenty years.

Crimes punishable by other afflictive penalties shall prescribe in fifteen years.

Those punishable by a correctional penalty shall prescribe in ten years; with the exception of those punishable by *arresto mayor*, which shall prescribe in five years.

The crime of libel or other similar offenses shall prescribe in one year.

The offenses of oral defamation and slander by deed shall prescribe in six months.

Light offenses prescribe in two months.

When the penalty fixed by law is a compound one the highest penalty shall be made the basis of the application of the rules contained in the first, second and third paragraphs of this article. (Emphases supplied)

On the other hand, Article 92 on the prescription of penalties states:

ARTICLE 92. *When and How Penalties Prescribe.* — The penalties imposed by final sentence prescribe as follows:

1. Death and *reclusión perpetua*, in twenty years;
2. **Other afflictive penalties, in fifteen years;**
3. **Correctional penalties, in ten years;** with the exception of the penalty of *arresto mayor*, which prescribes in five years;
4. Light penalties, in one year. (Emphases supplied)

⁶⁵ Id.

⁶⁶ Id.

⁶⁷ Id.

⁶⁸ Id.

As seen above, before the passage of the *Cybercrime Prevention Act*, the state effectively waives its right to prosecute crimes involving libel. Notably, the prescription period for libel used to be two years, but was reduced to one year through Republic Act No. 4661 on 18 June 1966.⁶⁹ Although the law itself does not state the reason behind the reduction, we can surmise that it was made in recognition of the harshness of the previous period, another act of grace by the State.

With the increase of penalty by one degree pursuant to Section 6 of the *Cybercrime Prevention Act*, however, the penalty for libel through ICT becomes *afflictive* under Article 25 of the Revised Penal Code. Accordingly, under the above-quoted provision, the crime of libel through ICT shall now possibly prescribe in 15 years – a 15-fold increase in the prescription period.⁷⁰ In effect, the State’s grant of amnesty to the offender will now be delayed by 14 years more. Until a definite ruling from this Court in a proper case is made, there is uncertainty as to whether the one-year prescription period for ordinary libel will also apply to libel through ICT.

Similarly, under Article 92, the prescription period for the *penalty* of libel through ICT is also increased from 10 years– the prescription period for correctional penalties – to 15 years, the prescription for afflictive penalties other than *reclusión perpetua*.

These twin increases in both the prescription period for the crime of libel through ICT and in that for its penalty are additional factors in the public’s rational calculation of whether or not to exercise their freedom of speech and whether to exercise that freedom through ICT. Obviously, the increased prescription periods – yet again – tilt the scales, heavily against the exercise of this freedom.

Regrettably, the records of the Bicameral Conference Committee deliberation do not show that the legislators took into careful consideration this domino effect that, when taken as a whole, clearly discourages the exercise of free speech. This, despite the fact that the records of the committee deliberations show that the legislators became aware of the need to carefully craft the application of the one-degree increase in penalty and “to review again the Revised Penal Code and see what ought to be punished, if committed through the computer.” But against their better judgment, they proceeded to make an all-encompassing application of the increased penalty sans *any* careful study, as the proceedings show:

THE CHAIRMAN (REP. TINGA). With regard to some of these offenses, the reason why they were not included in the House version initially is that, the assumption that the acts committed that would make it illegal in the real world would also be illegal in the cyberworld, ‘no.

⁶⁹ REYES, *supra* note 51, at 845.

⁷⁰ See also TSN dated 15 January 2013, pp. 80-81.

For example, libel *po*. When we discussed this again with the Department of Justice, it was their suggestion to include an all-encompassing paragraph...

THE CHAIRMAN (SEN. ANGARA). (Off-mike) A catch all–

THE CHAIRMAN (SEN. TINGA). ...a catch all, wherein all crimes defined and penalized by the Revised Penal Code as amended and special criminal laws committed by, through, and with the use of information and communications technology shall be covered by the relevant provisions of this act. By so doing, Mr. Chairman, we are saying that if we missed out on any of these crimes – we did not specify them, point by point – they would still be covered by this act, ‘*no*.’

So it would be up to you, Mr. Chairman...

THE CHAIRMAN (SEN. ANGARA). Yeah.

X X X X

THE CHAIRMAN (REP. TINGA). **...do we specify this and then or do we just use an all-encompassing paragraph to cover them.**

THE CHAIRMAN (SEN. ANGARA). Well, as you know, the Penal Code is really a very, very old code. In fact, it dates back to the Spanish time and we amend it through several Congresses. So like child pornography, this is a new crime, cybersex is a new crime. Libel through the use of computer system is a novel way of slandering and maligning people. So we thought that we must describe it with more details and specificity as required by the rules of the Criminal Law. **We’ve got to be specific and not general in indicting a person so that he will know in advance what he is answering for. But we can still include and let-anyway, we have a separability clause, a catch all provision that you just suggested and make it number five. Any and all crimes punishable under the Revised Penal Code not heretofore enumerated above but are committed through the use of computer or computer system shall also be punishable but we should match it with a penalty schedule as well.**

So we’ve got to review. *Mukhang mahirap gawin yun, huh. We have to review again the Revised Penal Code and see what ought to be punished, if committed through the computer. Then we’ve got to review the penalty, huh.*

THE CHAIRMAN (REP. TINGA). I agree, Mr. Chairman, that you are defining the newer crimes. But I also agree as was suggested earlier that **there should be an all-encompassing phrase to cover these crimes in the Penal Code, ‘no’. Can that not be matched with a penalty clause that would cover it as well? Instead of us going line by line through the–**

THE CHAIRMAN (SEN. ANGARA). **So you may just have to do that by a reference. The same penalty imposed under the Revised Penal Code shall be imposed on these crimes committed through computer or computer systems.**

X X X X

THE CHAIRMAN (REP. TINGA). Okay.

And may we recommend, Mr. Chairman, that your definition of the penalty be added as well where it will be one degree higher...

THE CHAIRMAN (SEN. ANGARA). Okay.

THE CHAIRMAN (REP. TINGA). **...than the relevant penalty as prescribed in the Revised Penal Code.**

So, we agree with your recommendation, Mr. Chairman.

X X X X

THE CHAIRMAN (SEN. ANGARA). Okay, provided that the penalty shall be one degree higher than that imposed under the Revised Penal Code.

Okay, so—

X X X X

REP. C. SARMIENTO. **Going by that ruling, if one commits libel by email, then the penalty is going to be one degree higher...**

THE CHAIRMAN (SEN. ANGARA). **One degree higher.**

REP. C. SARMIENTO . **...using email?**

THE CHAIRMAN (SEN. ANGARA). **Yes.**

REP. C. SARMIENTO. **As compared with libel through media or distributing letters or faxes.**

THE CHAIRMAN (SEN. ANGARA). **I think so, under our formulation. Thank you.** (Emphases supplied)⁷¹

ICT as a qualifying aggravating circumstance cannot be offset by any mitigating circumstance.

A qualifying aggravating circumstance has the effect not only of giving the crime its proper and exclusive name, but also of placing the offender in such a situation as to deserve no other penalty than that especially prescribed for the crime.⁷² Hence, a qualifying aggravating circumstance increases the penalty by degrees. For instance, homicide would become murder if attended by the qualifying circumstance of treachery, thereby increasing the penalty from *reclusión temporal* to *reclusión perpetua*.⁷³ It is unlike a generic aggravating circumstance, which increases the penalty only to the maximum period of the penalty prescribed

⁷¹ Senate Transcript of the Bicameral Conference Committee on the Disagreeing Provisions of SBN 2796 and HBN 5808 (Cybercrime Prevention Act of 2012) (31 May 2012) 15th Congress, 2nd Regular Sess. at 43-47, 52-56 [hereinafter Bicameral Conference Committee Transcript].

⁷² AQUINO, *supra* note 48, at 277 (citing *People v. Bayot*, 64 Phil. 269 [1937]). *See also* VICENTE J. FRANCISCO, THE REVISED PENAL CODE: ANNOTATED AND COMMENTED, BOOK I, 414 (2ND ED. 1954).

⁷³ LEONOR D. BOADO, NOTES AND CASES ON THE REVISED PENAL CODE, 147 (2008)

by law, and not to an entirely higher degree.⁷⁴ For instance, if the generic aggravating circumstance of dwelling or nighttime attends the killing of a person, the penalty will remain the same as that for homicide (*reclusión temporal*), but applied to its maximum period. Also, a generic aggravating circumstance may be offset by a generic mitigating circumstance, while a qualifying aggravating circumstance cannot be.⁷⁵

Hence, before the *Cybercrime Prevention Act*, libel – even if committed through ICT – was punishable only by *prisión correccional* from its minimum (6 months and 1 day to 2 years and 4 months) to its medium period (2 years, 4 months, and 1 day to 4 years and 2 months).

Under Section 6 however, the offender is now punished with a new range of penalty – *prisión correccional* in its maximum period (from 4 years, 2 months and 1 day to 6 years) to *prisión mayor* in its minimum period (from 6 years and 1 day to 8 years). And since the use of ICT as a qualifying aggravating circumstance cannot be offset by any mitigating circumstance, such as voluntary surrender, the penalty will remain within the new range of penalties.

As previously discussed, qualifying aggravating circumstances, by themselves, produce an *in terrorem* effect. A twofold increase in the maximum penalty – from 4 years and 2 months to 8 years – for the use of an otherwise beneficial and commonly used means of communication undeniably creates a heavier invidious chilling effect.

***The Court has the duty to restore
the balance and protect the
exercise of freedom of speech.***

Undeniably, there may be substantial distinctions between ICT and other means of committing libel that make ICT a more efficient and accessible means of committing libel. However, it is that same efficiency and accessibility that has made ICT an inextricable part of people's lives and an effective and widely used tool for the exercise of freedom of speech, a freedom that the Constitution protects and that this Court has a duty to uphold.

Facial challenges have been entertained when, in the judgment of the Court, the possibility that the freedom of speech may be muted and perceived grievances left to fester outweighs the harm to society that may be brought about by allowing some unprotected speech or conduct to go unpunished.⁷⁶

In the present case, it is not difficult to see how the increase of the penalty under Section 6 mutes freedom of speech. It creates a domino effect that

⁷⁴ *Id* at 146.

⁷⁵ AQUINO, *supra* note 48, at 277.

⁷⁶ *Quinto v. COMELEC*, G.R. No. 189698, 22 February 2010 (citing *Broadrick v. Oklahoma* 413 U.S. 601, 93 S.Ct. 2908 [1973]).

effectively subjugates the exercise of the freedom – longer prison terms, harsher accessory penalties, loss of benefits under the Probation Law, extended prescription periods, and ineligibility of these penalties to be offset by mitigating circumstances. What this Court said in *People v. Godoy*,⁷⁷ about “mankind’s age-old observation” on capital punishment, is appropriate to the penalty in the present case: “If it is justified, it serves as a deterrent; if injudiciously imposed, it generates resentment.”⁷⁸ Thus, I am of the opinion that Section 6, as far as libel is concerned, is facially invalid.

B. Section 12 – Real-Time Collection of Traffic Data.

Real-time collection of traffic data may be indispensable to law enforcement in certain instances. Also, traffic data *per se* may be examined by law enforcers, since there is no privacy expectation in them. However, the authority given to law enforcers must be circumscribed carefully so as to safeguard the privacy of users of electronic communications. **Hence, I support the ponencia in finding the first paragraph of Section 12 unconstitutional because of its failure to provide for strong safeguards against intrusive real-time collection of traffic data. I clarify, however, that this declaration should not be interpreted to mean that Congress is now prevented from going back to the drawing board in order to fix the first paragraph of Section 12. Real-time collection of traffic data is not invalid per se. There may be instances in which a warrantless real-time collection of traffic data may be allowed when robust safeguards against possible threats to privacy are provided.** Nevertheless, I am of the opinion that there is a need to explain why real-time collection of traffic data may be vital at times, as well as to explain the nature of traffic data.

Indispensability of Real-time Collection of Traffic Data

In order to gain a contextual understanding of the provision under the *Cybercrime Prevention Act* on the real-time collection of traffic data, it is necessary to refer to the *Budapest Convention on Cybercrime*, which the Philippine Government requested⁷⁹ to be invited to accede to in 2007. The Cybercrime Prevention Act was patterned after this convention.⁸⁰

⁷⁷ 321 Phil. 279 (1995).

⁷⁸ *Id.*, at 346.

⁷⁹ Undersecretary of the Department of Justice Ernesto L. Pineda sent a letter to the Secretary General of the Council of Europe dated 31 August 2007, expressing the wish of the Philippine government to be invited to accede to the Convention on Cybercrime. The Council of Europe granted the request in 2008. *See* Decision of the Council of Europe on the Request by the Philippines to be invited to accede to the Convention on Cybercrime, 1021st Meeting of the Ministers’ Deputies, dated 12 March 2008. Available at <<https://wcd.coe.int/ViewDoc.jsp?id=1255665&Site=CM>>, accessed on 12 September 2013.

⁸⁰ Committee Report No. 30 on Senate Bill No. 2796 (12 September 2011), pp. 280-281; Committee Report No. 30 on Senate Bill No. 2796 (13 December 2011), p. 804.

The Budapest Convention on Cybercrime is an important treaty, because it is the first and only multinational agreement on cybercrime.⁸¹ It came into force on 1 July 2004⁸² and, to date, has been signed by 45 member states of the Council of Europe (COE), 36 of which have ratified the agreement.⁸³ Significantly, the COE is the leading human rights organization of Europe.⁸⁴ Moreover, two important non-member states or “partner countries”⁸⁵ have likewise ratified it – the United States on 29 September 2006 and Japan on 3 July 2012. Australia and the Dominican Republic have also joined by accession.⁸⁶

The Convention “represents a comprehensive international response to the problems of cybercrime”⁸⁷ and is the product of a long process of careful expert studies and international consensus. From 1985 to 1989, the COE’s Select Committee of Experts on Computer-Related Crime debated issues before drafting Recommendation 89(9). This Recommendation stressed the need for a quick and adequate response to the cybercrime problems emerging then and noted the need for an international consensus on criminalizing specific computer-related offenses.⁸⁸ In 1995, the COE adopted Recommendation No. R (95)13, which detailed principles addressing search and seizure, technical surveillance, obligations to cooperate with the investigating authorities, electronic evidence, and international cooperation.⁸⁹ In 1997, the new Committee of Experts on Crime in Cyberspace was created to examine, “in light of Recommendations No R (89)9 and No R (95)13,” the problems of “cyberspace offenses and other substantive criminal law issues where a common approach may be necessary for international cooperation.” It was also tasked with the drafting of “a binding legal instrument” to deal with these issues. The preparation leading up to the Convention entailed 27 drafts over four years.⁹⁰

As mentioned earlier, the Philippines was one of the countries that requested to be invited to accede to this very important treaty in 2007, and the Cybercrime Prevention Act was patterned after the convention.⁹¹

Article 1 of the *Budapest Convention on Cybercrime* defines “traffic data” as follows:

- d. “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed

⁸¹ JONATHAN CLOUGH, *PRINCIPLES OF CYBERCRIME*, 22 (2010);

⁸² *Id.*

⁸³ <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>>, accessed on 20 October 2013.

⁸⁴ Twenty-eight of COE’s members also belong to the European Union (EU). All its member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. <<http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=en>> accessed on 20 October 2013.

⁸⁵ Canada, Japan, South Africa, and the United States.

⁸⁶ <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>> accessed on 20 October 2013.

⁸⁷ *Supra* note 28.

⁸⁸ SUMIT GHOSH ET AL., *EDITORS, CYBERCRIMES: A MULTIDISCIPLINARY ANALYSIS*, 330 (2010).

⁸⁹ *Id.* at 330-331.

⁹⁰ *Id.* at 331.

⁹¹ Committee Report No. 30 on Senate Bill No. 2796 (12 September 2011), pp. 280-281; Committee Report No. 30 on Senate Bill No. 2796 (13 December 2011), p. 804.

a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Section 3 of the *Cybercrime Prevention Act* has a starkly similar definition of "traffic data":

(p) *Traffic data or non-content data* refers to any computer data **other than the content** of the communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

However, the definition in the *Cybercrime Prevention Act* improves on that of the Convention by clearly restricting traffic data to those that are *non-content* in nature. On top of that, Section 12 further restricts traffic data to *exclude* those that refer to the *identity* of persons. The provision states:

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.**
(Emphasis supplied)

Undoubtedly, these restrictions were made because Congress wanted to ensure the protection of the privacy of users of electronic communication. Congress must have also had in mind the *1965 Anti-Wiretapping Act*, as well as the *Data Privacy Act* which was passed only a month before the *Cybercrime Prevention Act*. However, as will be shown later, the restrictive definition is not coupled with an equally restrictive procedural safeguard. This deficiency is the Achilles' heel of the provision.

One of the obligations under the *Budapest Convention on Cybercrime* is for state parties to enact laws and adopt measures concerning the real-time collection of traffic data, *viz*:

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary **to empower its competent authorities** to:
 - a. **collect or record** through the **application of technical means** on the territory of that Party, **and**
 - b. **compel a service provider**, within its existing technical capability:
 - i. **to collect or record** through the application of technical means on the territory of that Party; or
 - ii. **to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time**, associated with specified communications in its territory transmitted by means of a computer system.

2. **Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.**
3. Each Party shall adopt such legislative and other measures as may be necessary to **oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.**
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. (Emphases supplied)

The Explanatory Report on the *Budapest Convention on Cybercrime* explains the ephemeral and volatile nature of traffic data, which is the reason why it has to be collected in real-time if it is to be useful in providing a crucial lead to investigations of criminality online as follows:⁹²

29. In case of an investigation of a criminal offence committed in relation to a computer system, **traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only momentarily, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication** which is regarded to be more sensitive.

x x x x

133. One of the major challenges in combating crime in the networked environment is the **difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act.** A further problem is caused by the **volatility of electronic data, which may be altered, moved or deleted in seconds.** For example, **a user who is in control of the data may use the computer system to erase the data that is the subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation.**

134. The Convention adapts traditional procedural measures, such as search and seizure, to the new technological environment. Additionally, new measures have been created, such as expedited preservation of data, in order to ensure that traditional measures of collection, such as search and seizure, remain effective in the volatile technological environment. **As data in the new technological environment is not always static, but may be flowing in the process of communication, other traditional collection procedures relevant to**

⁹² *Explanatory Report to the Convention on Cybercrime*, [2001] COETSER 8 (23 November 2001), available at <<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>>, accessed on 12 September 2013.

telecommunications, such as real-time collection of traffic data and interception of content data, have also been adapted in order to permit the collection of electronic data that is in the process of communication. Some of these measures are set out in Council of Europe Recommendation No. R (95) 13 on problems of criminal procedural law connected with information technology.

X X X X

214. For some States, the offences established in the Convention would normally not be considered serious enough to permit interception of content data or, in some cases, even the collection of traffic data. **Nevertheless, such techniques are often crucial for the investigation of some of the offences established in the Convention, such as those involving illegal access to computer systems, and distribution of viruses and child pornography. The source of the intrusion or distribution, for example, cannot be determined in some cases without real-time collection of traffic data. In some cases, the nature of the communication cannot be discovered without real-time interception of content data. These offences, by their nature or the means of transmission, involve the use of computer technologies.** The use of technological means should, therefore, be permitted to investigate these offences. XXX.

X X X X

216. **Often, historical traffic data may no longer be available or it may not be relevant as the intruder has changed the route of communication.** Therefore, the real-time collection of traffic data is an important investigative measure. Article 20 addresses the subject of real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings.

X X X X

218. XXX. **When an illegal distribution of child pornography, illegal access to a computer system or interference with the proper functioning of the computer system or the integrity of data, is committed, particularly from a distance such as through the Internet, it is necessary and crucial to trace the route of the communications back from the victim to the perpetrator. Therefore, the ability to collect traffic data in respect of computer communications is just as, if not more, important as it is in respect of purely traditional telecommunications.** This investigative technique can correlate the time, date and source and destination of the suspect's communications with the time of the intrusions into the systems of victims, identify other victims or show links with associates.

219. Under this article, the traffic data concerned must be associated with specified communications in the territory of the Party. The specified 'communications' are in the plural, as traffic data in respect of several communications may need to be collected in order to determine the human source or destination (for example, in a household where several different persons have the use of the same telecommunications facilities, it may be necessary to correlate several communications with the individuals' opportunity to use the computer system). The communications in respect of which the traffic data may be collected or recorded, however, must be specified. **Thus, the Convention does not require or authorise the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of 'fishing expeditions' where criminal activities are hopefully sought to be discovered, as opposed to specific instances of criminality being investigated.**

The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.

X X X X

225. Like real-time interception of content data, **real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Interception is surreptitious and must be carried out in such a manner that the communicating parties will not perceive the operation.** Service providers and their employees knowing about the interception must, therefore, be under an obligation of secrecy in order for the procedure to be undertaken effectively. (Emphases supplied)

We can gather from the Explanatory Note that there are two seemingly conflicting ideas before us that require careful balancing – the fundamental rights of individuals, on the one hand, and the interests of justice (which may also involve the fundamental rights of another person) on the other. There is no doubt that privacy is vital to the existence of a democratic society and government such as ours. It is also critical to the operation of our economy. Citizens, governments, and businesses should be able to deliberate and make decisions in private, away from the inhibiting spotlight.⁹³ Certainly, this privacy should be maintained in the electronic context as social, governmental and economic transactions are made in this setting.⁹⁴ At the same time however, law enforcers must be equipped with up-to-date tools necessary to protect society and the economy from criminals who have also taken advantage of electronic technology. These enforcers must be supplied with investigative instruments to solve crimes and punish the criminals.⁹⁵

What is beyond debate, however, is that real-time collection of traffic data may be absolutely necessary in criminal investigations such that, without it, authorities may not be able to probe certain crimes at all. In fact, it has been found that crucial electronic evidence may never be stored at all, as it may exist only in transient communications.⁹⁶ The UN Office on Drugs and Crime requires real-time collection of data because of the urgency, sensitivity, or complexity of a law enforcement investigation.⁹⁷

Hence, it is imprudent to precipitately make (1) an absolute declaration that *all* kinds of traffic data from *all* types of sources are protected by the constitutional right to privacy; and (2) a blanket pronouncement that the real-time collection thereof may *only* be conducted upon a *prior* lawful order of the court to constitute a valid search and seizure. Rather, the Court should impose a strict interpretation of Section 12 in the light of existing constitutional, jurisprudential and statutory guarantees and safeguards.

⁹³ Richard W. Downing. *Columbia Journal of Transnational Law*, Vol. 43, p. 743 (2005).

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ UNITED NATIONS OFFICE ON DRUGS AND CRIME, COMPREHENSIVE STUDY ON CYBERCRIME (DRAFT), 130 (2013).

⁹⁷ *Id.*

The Constitutional guarantee against unreasonable search and seizure is inviolable.

The inviolable right against unreasonable search and seizure is enshrined in Article III of the Constitution, which states:

Section 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

It is clear from the above that the constitutional guarantee does not prohibit all searches and seizures, but only *unreasonable* ones.⁹⁸ As a general rule, a search and seizure is reasonable when probable cause has been established. Probable cause is the most restrictive of all thresholds. It has been broadly defined as those facts and circumstances that would lead a reasonably discreet and prudent man to believe that an offense has been committed, and that the objects sought in connection with the offense are in the place sought to be searched.⁹⁹ It has been characterized as referring to “*factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.*”¹⁰⁰ Furthermore, probable cause is to be determined by a judge *prior* to allowing a search and seizure. The judge’s determination shall be contained in a warrant, which shall particularly describe the place to be searched and the things to be seized. Thus, when no warrant is issued, it is assumed that there is no probable cause to conduct the search, making that act unreasonable.

For the constitutional guarantee to apply, however, there must first be a search in the constitutional sense.¹⁰¹ It is only when there is a search that a determination of probable cause is required. In *Valmonte v. De Villa*, the Court said that the constitutional rule cannot be applied when mere routine checks consisting of “a brief question or two” are involved.¹⁰² The Court said that if neither the vehicle nor its occupants are subjected to a search – the inspection of the vehicle being limited to a visual search – there is no violation of an individual’s right against unreasonable searches and seizures. Hence, for as long as there is no *physical* intrusion upon a constitutionally protected area, there is no search.¹⁰³

⁹⁸ JOAQUIN BERNAS, THE 1987 CONSTITUTION OF THE REPUBLIC OF THE PHILIPPINES: A COMMENTARY, 162 (2003).

⁹⁹ *Tan v. Sy Tiong Gue*, G.R. No. 174570, 17 February 2010, 613 SCRA 98, 106;

¹⁰⁰ *Supra* note 1 at 163, citing *Brinegar v. United States*, 338 U.S. 160, 175 (1949)

¹⁰¹ *Supra* note 44.

¹⁰² *Id.*

¹⁰³ *See: United States v. Jones* 132 S. Ct. 945, 950 n.3 (2012).

In recent years, the Court has had occasion to rule¹⁰⁴ that a search occurs when the government violates a person's "reasonable expectation of privacy," a doctrine first enunciated in *Katz v. United States*.¹⁰⁵ *Katz* signalled a paradigm shift, as the inquiry into the application of the constitutional guarantee was now expanded beyond "the presence or absence of a physical intrusion into any given enclosure" and deemed to "[protect] people, not places."¹⁰⁶ Under this expanded paradigm, the "reasonable expectation of privacy" can be established if the person claiming it can show that (1) by his conduct, he exhibited an expectation of privacy and (2) his expectation is one that society recognizes as reasonable. In *People v. Johnson*,¹⁰⁷ which cited *Katz*, the seizure and admissibility of the dangerous drugs found during a routine airport inspection were upheld by the Court, which explained that "[p]ersons may lose the protection of the search and seizure clause by exposure of their persons or property to the public in a manner reflecting a **lack of subjective expectation of privacy**, which expectation society is prepared to recognize as reasonable."¹⁰⁸

Traffic data per se do not enjoy privacy protection; hence, no determination of probable cause is needed for the real-time collection thereof.

The very public structure of the Internet and the nature of traffic data *per se* undermine any *reasonable* expectation of privacy in the latter. The Internet is custom-designed to frustrate claims of reasonable expectation of privacy in traffic data *per se*, since the latter are necessarily disclosed to the public in the process of communication.

Individuals have no legitimate expectation of privacy in the data they disclose to the public and should take the risks for that disclosure. This is the holding of the U.S. Supreme Court in *Smith v. Maryland*.¹⁰⁹ The 1979 case, which has stood the test of time and has been consistently applied by American courts in various communications cases – including recent ones in the electronic setting – arose from a police investigation of robbery. The woman who was robbed gave the police a description of the robber and of a car she had observed near the scene of the crime. After the robbery, she began receiving threatening phone calls from a man identifying himself as the robber. The car was later found to be registered in the name of the petitioner, Smith. The next day, the telephone company, upon police request, installed a pen register at its central offices to record the numbers dialled from the telephone at the home of Smith. The register showed that he had indeed been calling the victim's house. However, since the installation of the pen

¹⁰⁴ *Pollo v. Constantino-David*, G.R. No. 181881, 18 October 2011, 659 SCRA 189; *People v. Johnson*, 401 Phil 734 (2000).

¹⁰⁵ 389 U.S. 347 (1967).

¹⁰⁶ *Id.*

¹⁰⁷ *Supra* note 104.

¹⁰⁸ *Id.*

¹⁰⁹ 442 U.S. 735 (1979).

register was done without a warrant, he moved to suppress the evidence culled from the device. In affirming **the warrantless collection and recording of phone numbers dialed** by Smith, the U.S. Supreme Court said:

This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. **All telephone users realize that they must “convey” phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.** All subscribers realize, moreover, that **the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.** x x x.

x x x x

Second, **even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not “one that society is prepared to recognize as ‘reasonable.’”** *Katz v. United States*, 389 U. S., at 361. **This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.** *E.g., United States v. Miller*, 425 U. S., at 442-444; x x x.¹¹⁰ (Emphases supplied)

I am of the opinion that this Court may find the ruling in *United States v. Forrester*,¹¹¹ persuasive. In that case, the U.S. 9th Circuit Court of Appeals applied the doctrine in *Smith* to electronic communications, and ruled that Internet users have no expectation of privacy in the to/from addresses of their messages or in the IP addresses of the websites they visit. According to the decision, users should know that these bits of information are provided to and used by Internet service providers for the specific purpose of directing the routing of information. **It then emphasized that this examination of traffic data is “conceptually indistinguishable from government surveillance of physical mail,” and that the warrantless search of envelope or routing information has been deemed valid as early as the 19th century.** The court therein held:

We conclude that the [electronic] surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*. First, e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users’ imputed knowledge that their calls are completed through telephone company switching equipment. x x x. **Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.** Like telephone numbers, which provide

¹¹⁰ Supra note 55.

¹¹¹ 512 F.3d 500 (2007).

instructions to the “switching equipment that processed those numbers,” e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party’s servers. x x x.

Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person’s e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses — but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. x x x. Nonetheless, **the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information** that the government did not cross here.

The government’s surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail. In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties. x x x. E-mail, like physical mail, has an outside address “visible” to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. **The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not.**¹¹² (Emphases and underscoring supplied)

Based on the cogent logic explained above, I share the view that Internet users have no reasonable expectation of privacy in traffic data *per se* or in those pieces of information that users necessarily provide to the ISP, a third party, in order for their communication to be transmitted. This position is further bolstered by the fact that such communication passes through as many ISPs as needed in order to reach its intended destination. Thus, the collection and recording of these data do not constitute a search in the constitutional sense. As such, the collection thereof may be done without the necessity of a warrant.

Indeed, Professor Orin Kerr,¹¹³ a prominent authority on electronic privacy, observes that in the U.S., **statutory rather than constitutional protections provide the essential rules governing Internet surveillance law. He explains that the very nature of the Internet requires the disclosure of non-content information**, not only to the ISP contracted by the user, but also to other computers in order for the communication to reach the intended recipient. Professor Kerr explains thus:

¹¹² 512 F.3d 500 (2007).

¹¹³ Fred C. Stevenson Research Professor, George Washington University Law School.

Recall that **the Fourth Amendment effectively carves out private spaces where law enforcement can't ordinarily go without a warrant and separates them from public spaces where it can.** One important corollary of this structure is that **when a person sends out property or information from her private space into a public space, the exposure to the public space generally eliminates the Fourth Amendment protection.** If you put your trash bags out on the public street, or leave your private documents in a public park, the police can inspect them without any Fourth Amendment restrictions.

The Supreme Court's cases interpreting **this so-called "disclosure principle" have indicated that the principle is surprisingly broad.** For example, **the exposure need not be to the public. Merely sharing the information or property with another person allows the government to go to that person to obtain it without Fourth Amendment protection.** x x x.

Why does this matter to Internet surveillance? It matters because **the basic design of the Internet harnesses the disclosure, sharing, and exposure of information to many machines connected to the network. The Internet seems almost custom-designed to frustrate claims of broad Fourth Amendment protection: the Fourth Amendment does not protect information that has been disclosed to third-parties, and the Internet works by disclosing information to third-parties.** Consider what happens when an Internet user sends an e-mail. By pressing "send" on the user's e-mail program, the user sends the message to her ISP, disclosing it to the ISP, with instructions to deliver it to the destination. The ISP computer looks at the e-mail, copies it, and then **sends a copy across the Internet where it is seen by many other computers before it reaches the recipient's ISP.** The copy sits on the ISP's server until the recipient requests the e-mail; at that point, the ISP runs off a copy and sends it to the recipient. While the e-mail may seem like a postal mail, it is sent more like a post card, exposed during the course of delivery.¹¹⁴ (Emphases and underscoring supplied.)

Clearly, considering that the Internet highway is so public, and that non-content traffic data, unlike content data, are necessarily exposed as they pass through the Internet before reaching the recipient, there cannot be any reasonable expectation of privacy in non-content traffic data *per se*.

Traffic data to be collected are explicitly limited to non-content and non-identifying public information which, unlike content data, are not constitutionally protected.

The U.S. Supreme Court and Court of Appeals in the above cases emphasized the distinction between content and non-content data, with only content data enjoying privacy protection. In *Smith* the Court approved of the use of

¹¹⁴ Orin S. Kerr, *Enforcing Privacy Rights: Communications Privacy: Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003).

pen registers, pointing out that “a pen register differs significantly from [a] listening device ... for pen registers do not acquire the contents of communications.”¹¹⁵ Hence, the information derived from the pen register, being non-content, is not covered by the constitutional protection. In *Forrester*, it was held that **while the content of both e-mail and traditional mail are constitutionally protected, the non-content or envelope information is not.** On the other hand, in the 2007 case *Warshak v. United States*,¹¹⁶ the Sixth Circuit Court of Appeals held that the contents of emails are protected. It employed the content/non-content distinction in saying that the “combined precedents of Katz and Smith” required a “heightened protection for the *content* of the communications.”¹¹⁷ Consequently, it found a strong “*content*-based privacy interest” in e-mails.¹¹⁸

Traffic data are of course explicitly restricted to non-content and non-identifying data as defined in Section 12 of the Cybercrime Prevention Act itself. As such, it is plain that traffic data *per se* are not constitutionally protected.

The distinction between content and non-content data, such as traffic data, is important because it keeps the balance between protecting privacy and maintaining public order through effective law enforcement. That is why our Congress made sure to specify that the traffic data to be collected are limited to non-content data. For good measure, it additionally mandated that traffic data be non-identifying.

Kerr explains how the distinction between *content* and *non-content* information in electronic communication mirrors perfectly and logically the established *inside* and *outside* distinction in physical space, as far as delineating the investigative limitations of law enforcers is concerned. *Inside* space is constitutionally protected, and intrusion upon it requires a court warrant; in contrast, surveillance of *outside* space does not require a warrant because it is not a constitutionally cognizable search. He explains thus:

Whereas the inside/outside distinction is basic to physical world investigations, the content/non-content distinction is basic to investigations occurring over communications networks. Communications networks are tools that allow their users to send and receive communications from other users and services that are also connected to the network. This role requires a distinction between addressing information and contents. The addressing (or “envelope”) information is the data that the network uses to deliver the communications to or from the user; the content information is the payload that the user sends or receives.

X X X X

¹¹⁵ 442 U.S. 735 (1979).

¹¹⁶ 490 F.3d 455, 470-71 (6th Cir. 2007).

¹¹⁷ Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2115 (2009).

¹¹⁸ *Id.* The Sixth Circuit later granted a petition for rehearing en banc and skirted the constitutional issue. It vacated the Decision upon a finding that the case was unripe.

We can see the same distinctions at work with the telephone network. The telephone network permits users to send and receive live phone calls. The addressing information is the number dialed (“to”), the originating number (“from”), the time of the call, and its duration. Unlike the case of letters, this calling information is not visible in the same way that the envelope of a letter is. At the same time, it is similar to the information derived from the envelope of a letter. In contrast, the contents are the call itself, the sound sent from the caller’s microphone to the receiver’s speaker and from the receiver’s microphone back to the caller’s speaker.

Drawing the content/non-content distinction is somewhat more complicated because the Internet is multifunctional. x x x. Still, the content/non-content distinction holds in the Internet context as well. The easiest cases are human-to-human communications like e-mail and instant messages. The addressing information is the “to” and “from” e-mail address, the instant message to and from account names, and the other administrative information the computers generate in the course of delivery. As in the case of letters and phone calls, the addressing information is the information that the network uses to deliver the message. In contrast, the actual message itself is the content of the communication.

x x x x

The content/non-content distinction provides a natural replacement for the inside/outside distinction. To apply the Fourth Amendment to the Internet in a technologically neutral way, access to the contents of communications should be treated like access to evidence located inside. Accessing the contents of communications should ordinarily be a search. In contrast, access to non-content information should be treated like access to evidence found outside. Collection of this information should presumptively not be a search.

This translation is accurate because the distinction between content and non-content information serves the same function online that the inside/outside distinction serves in the physical world. Non-content information is analogous to outside information; it concerns where a person is and where a person is going. Consider what the police can learn by watching a suspect in public. Investigating officers can watch the suspect leave home and go to different places. They can watch him go to lunch, go to work, and go to the park; they can watch him drive home; and they can watch him park the car and go inside. In effect, this is to/from information about the person’s own whereabouts.

On the other hand, content information is analogous to inside information. The contents of communications reveal the substance of our thinking when we assume no one else is around. It is the space for reflection and self-expression when we take steps to limit the audience to a specific person or even just to ourselves. The contents of Internet communications are designed to be hidden from those other than the recipients, much like property stored inside a home is hidden from those who do not live with us.
x x x.

The connection between content/non-content on the Internet and inside/outside in the physical world is not a coincidence. Addressing information is itself a network substitute for outside information, and contents are a network substitute for inside information. Recall the basic function of communications networks: they are systems that send and receive

communications remotely so that its users do not have to deliver or pick up the communications themselves. The non-content information is the information the network uses to deliver communications, consisting of where the communication originated, where it must be delivered, and in some cases the path of delivery. This information is generated in lieu of what would occur in public; it is information about the path and timing of delivery. In contrast, the contents are the private communications themselves that would have been inside in a physical network.

X X X X

In light of this, a technologically neutral way to translate the Fourth Amendment from the physical world to the Internet would be to treat government collection of the contents of communications as analogous to the government collection of information inside and the collection of non-content information as analogous to the collection of information outside. X X X.

This approach would mirror the line that the Fourth Amendment imposes in the physical world. In the physical world, the inside/outside distinction strikes a sensible balance. It generally lets the government observe where people go, when they go, and to whom they are communicating while protecting the actual substance of their speech from government observation without a warrant unless the speech is made in a setting open to the public. The content/non-content distinction preserves that function. It generally lets the government observe where people go in a virtual sense, and to observe when and with whom communications occur. The essentially transactional information that would occur in public in a physical world has been replaced by non-content information in a network environment, and the content/non-content line preserves that treatment. At the same time, the distinction permits individuals to communicate with others in ways that keep the government at bay. The Fourth Amendment ends up respecting private areas where people can share their most private thoughts without government interference both in physical space and cyberspace alike.¹¹⁹ (Emphases supplied.)

Indeed, there is a clear distinction between content and non-content data. The distinction presents a reasonable conciliation between privacy guarantees and law enforcement needs, since the distinction proceeds from logical differences between the two in their nature and privacy expectations. According to a comprehensive UN study on six international or regional cybercrime instruments,¹²⁰ which include provisions on real-time collection of computer data, these instruments “make a distinction between real-time collection of traffic data and of content data” to account for the “differences in the level of intrusiveness into the private life of persons subject to each of the measures.”¹²¹

From the above jurisprudence and scholarly analysis, there is enough basis to conclude that, given the very public nature of the Internet and the nature of

¹¹⁹ Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010).

¹²⁰ These are: 1.) COMESA Draft Model Bill, Art. 38; 2.) Commonwealth Model Law, Art. 19; 3.) Council of Europe Cybercrime Convention, Art. 20; 4.) ITU/CARICOM/CTU Model Legislative Texts, Art. 25; 5.) League of Arab States Convention, Art. 28 and 6.) Draft African Union Convention, Art. 3-55.

¹²¹ UNITED NATIONS OFFICE ON DRUGS AND CRIME, COMPREHENSIVE STUDY ON CYBERCRIME (DRAFT), 130 (2013).

traffic data as non-content and non-identifying information, individuals cannot have legitimate expectations of privacy in traffic data *per se*.

Section 12, however, suffers from lack of procedural safeguards to ensure that the traffic data to be obtained are limited to non-content and non-identifying data, and that they are obtained only for the limited purpose of investigating specific instances of criminality.

Thus far, it has been shown that real-time collection of traffic data may be indispensable in providing a crucial first lead in the investigation of criminality. Also, it has been explained that there is clearly no legitimate expectation of privacy in traffic data *per se* because of the nature of the Internet – it requires disclosure of traffic data which, unlike content data, will then travel exposed as it passes through a very public communications highway. It has also been shown that the definition of traffic data under the law is sufficiently circumscribed to cover only non-content and non-identifying data and to explicitly exclude content data. This distinction is important in protecting privacy guarantees while supporting law enforcement needs.

However, Section 12 suffers from a serious deficiency. The narrow definition of traffic data *per se* as non-content and non-identifying data is not supported by equally narrow procedural criteria for the exercise of the authority to obtain them. The government asserts that Section 12 provides for some protection against abuse. While this may be true, the safeguards provided are not sufficient to protect constitutional guarantees.

Firstly, the provision does not indicate what the purpose of the collection would be, since it only provides for “due cause” as a trigger for undertaking the activity. While the government has explained the limited purpose of the collection of traffic data, which purportedly can only go as far as providing an initial lead to an ongoing criminal investigation primarily in the form of an IP address, this limited purpose is not explicit in the assailed provision. Moreover, there is no assurance that the collected traffic data would not be used for preventive purposes as well. Notably, the Solicitor-General defines “due cause” as “good faith law enforcement reason”¹²² or “when there’s a complaint from a citizen that cybercrime has been committed.” According to the Solicitor General this situation is “enough to trigger” a collection of traffic data.¹²³ However, during the oral arguments, the Solicitor General prevaricated on whether Section 12 could also be used for preventive monitoring. He said that there might be that possibility, although the purpose would “largely” be for the investigation of an existing

¹²² TSN dated 29 January 2013, p. 49.

¹²³ *Id* at 86.

criminal act.¹²⁴ This vagueness is disconcerting, since a preventive monitoring would necessarily entail casting a wider net than an investigation of a specific instance of criminality would. Preventive monitoring would correspondingly need more restrictive procedural safeguards. This failure to provide an unequivocally specified purpose is fatal because it would give the government the roving authority to obtain traffic data for any purpose.¹²⁵

Secondly, Section 12 does not indicate who will determine “due cause.” This failure to assign the determination of due cause to a specific and independent entity opens the floodgates to possible abuse of the authority to collect traffic data in real-time, since the measure will be undertaken virtually unchecked. Also, while Section 12 contemplates the collection only of data “associated with specified communications,” it does not indicate who will make the specification and how specific it will be.

Finally, the collection of traffic data under Section 12 is not time-bound. This lack of limitation on the period of collection undoubtedly raises concerns about the possibility of unlimited collection of traffic data in bulk for purposes beyond the simple investigation of specific instances of criminality.

Existing approaches in other jurisdictions for collection of traffic data

To foreclose an Orwellian collection of traffic data in bulk that may lead to the invasion of privacy, the relevant law must be canalized to accommodate only an acceptable degree of discretion to law enforcers. It must provide for clear parameters and robust safeguards for the exercise of the authority. Notably, the Solicitor General himself has observed that stronger safeguards against abuse by law enforcers may have to be put in place.¹²⁶ There are also indications that the legislature is willing to modify the law to provide for stronger safeguards, as shown in the bills filed in both chambers of Congress.¹²⁷

In fashioning procedural safeguards against invasion of privacy, the rule of thumb should be: the more intrusive the activity, the stricter the procedural safeguards. Other countries have put in place some restrictions on the real-time collection of traffic data in their jurisdictions. In the United States, the following are the requirements for the exercise of this authority:

¹²⁴ Id at 95-96.

¹²⁵ *Ople v. Torres*, 354 Phil. 948 (1998).

¹²⁶ TSN dated 29 January 2013, p. 48.

¹²⁷ See Senate Bill (SB) No. 126, “An Act Repealing Section 4(c) (4), Chapter II of Republic Act No. 10175”; SB No. 11, “An Act Amending Section 6 of Republic Act 10175 Otherwise Known as an Act Defining Cybercrime, Providing For the Prevention, Investigation and Imposition of Penalties Therefor and For Other Purposes”; SB No. 154, “An Act Amending Republic Act No. 10175, Otherwise Known as the Cybercrime Prevention Act of 2012”; SB No. 249, “An Act Repealing Sections 4 (c) (4), 5, 6, and 7 of RA 10175, Otherwise Known as the Cybercrime Prevention Act of 2012”; SB Nos 53 and 1091 and House Bill (HB) No. 1086 or the Magna Carta for Philippine Internet Freedom; HB No. 1132, “An Act Repealing Republic Act No. 10175 or the Cybercrime Prevention Act of 2012.”

- (1) **relevance** of the collected information to an ongoing criminal investigation;
- (2) **court order** issued by a judicial officer based upon the **certification of a government attorney**; and
- (3) **limitation of the period** of collection to sixty days (with the **possibility of extension**).

In the United Kingdom, the following requirements must be complied with:

- (1) **necessity** of the information to be collected for the investigation of crime, protection of public safety, or a similar goal;
- (2) **approval of a high-level government official**;
- (3) **proportionality** of the collection to what is sought to be achieved; and
- (4) **limitation of the period** of collection to thirty days.¹²⁸

The above requirements laid down by two different jurisdictions offer different but similar formulations. As to what the triggering threshold or purpose would be, it could be the necessity threshold (for the investigation of crime, protection of public safety, or a similar goal) used in the United Kingdom or the relevance threshold (to an ongoing criminal investigation) in the United States. Note that these thresholds do not amount to probable cause.

As to who determines compliance with the legal threshold that triggers the exercise of the authority to collect traffic data in real time, the laws of the United States suggest that special judicial intervention is required. This intervention would be a very strong measure against the violation of privacy even if the judicial order does not require determination of probable cause. At the same time, however, the general concern of Justice Brion that “time is of the utmost essence in cyber crime law enforcement” needs to be considered. Hence, procedural rules of court will have to be adjusted so as not to unduly slow down law enforcement response to criminality considering how ephemeral some information could be. We must ensure that these rules are not out of step with the needs of law enforcement, given current technology. It may be noted that Justice Carpio has broached the idea of creating 24-hour courts to address the need for speedy law enforcement response.¹²⁹

In the United Kingdom, the mechanism suggests that the authorizing entity need not be a judge, as it could be a high-ranking government official. Perhaps this non-judicial authorization proceeds from the consideration that since the triggering threshold is not probable cause, but only necessity to an ongoing criminal investigation, there is no need for a judicial determination of compliance with the aforesaid threshold.

¹²⁸ Richard W. Downing, *Shoring up the Weakest Link: What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime*, 43 COLUM. J. TRANSNAT'L L. 705 (2005).

¹²⁹ TSN dated 29 January 2013, p. 50.

The above requirements also provide limits on the period of collection of traffic data. In the United States, the limit is 60 days with a possibility of extension. This period and the possibility of extension are similar to those provided under our Anti-Wiretapping Law. Note, however, that the Anti-Wiretapping Law concerns the content of communications whereas the traffic data to be collected under Section 12 of the *Cybercrime Prevention Act* is limited to non-content and non-identifying data. Hence, the restriction on the period of collection could perhaps be eased by extending it to a longer period in the case of the latter type of data. In the United Kingdom, the limit is 30 days.

From the above observation of the deficiencies of Section 12, as well as the samples from other jurisdictions, the following general guidelines could be considered to strengthen the safeguards against possible abuse.

First, the relevance or necessity of the collection of traffic data to an ongoing criminal investigation must be established. This requirement to specify the purpose of the collection (to aid ongoing criminal investigation) will have the effect of limiting the usage of the collected traffic data to exclude dossier building, profiling and other purposes not explicitly sanctioned by the law. It will clarify that the intention for the collection of traffic data is not to create a historical data base for a comprehensive analysis of the personal life of an individual whose traffic data is collected, but only for investigation of specific instances of criminality. More important, it is not enough that there be an ongoing criminal investigation; the real-time collection must be shown to be necessary or at least relevant to the investigation. Finally, it should be explicitly stated that the examination of traffic data will not be for the purpose of preventive monitoring which, as observed earlier, would necessarily entail a greater scope than that involved in a targeted collection of traffic data for the investigation of a specific criminal act.

Second, there must be an independent authority – judicial or otherwise – who shall review compliance with the relevance and necessity threshold. The designation of this authority will provide additional assurance that the activity will be employed only in specific instances of criminal investigation and will be necessary or relevant. The designation of an authorizing entity will also inhibit the unjustified use of real-time collection of traffic data. The position of this person should be sufficiently high to ensure greater accountability. For instance, it was suggested during the oral arguments that the authorizing person be a lawyer of the national government in order to additionally strengthen that person's accountability, proceeding as it would from his being an officer of the court.¹³⁰

Third, there must be a limitation on the period of collection. The restriction on the time period will further prevent the indiscriminate and bulk collection of traffic data beyond what is necessary for a regular criminal investigation.

¹³⁰ TSN dated 29 January 2013, p. 92.

As to the type of technology to be used for collection, it seems that this cannot be specified beforehand. Certainly, only a general restriction can be made – that the technology should be capable of collecting only non-content and non-identifying traffic data. It should not be able to directly point to the location of the users of the Internet, the websites visited, the search words used, or any other data that reveal the thoughts of the user.

In the end, whatever mechanism is to be set in place must satisfy the Constitution's requirements for the safeguard of the people's right to privacy and against undue incursions on their liberties.

Final Words

Laws and jurisprudence should be able to keep current with the exponential growth in information technology.¹³¹ The challenge is acute, because the rapid progress of technology has opened up new avenues of criminality. Understandably, governments try to keep pace and pursue criminal elements that use new technological avenues. It is precisely during these times of zeal that the Court must be ever ready to perform its duty to uphold fundamental rights when a proper case is brought before it.

The Court has carefully trod through the issues that have been heard in these Petitions, especially since they involve the exercise of our power of judicial review over acts of the legislature. I believe that we have tried to exercise utmost judicial restraint and approached the case as narrowly as we could so as to avoid setting sweeping and overreaching precedents.¹³² We have thus prudently resolved the present Petitions with the view in mind that a future re-examination of the law is still possible,¹³³ especially when the constitutional challenges set forth become truly ripe for adjudication. This is also so that we do not unduly tie the hands of the government when it regulates socially harmful conduct in the light of sudden changes in technology, especially since the regulation is meant to protect the very same fundamental rights that petitioners are asking this Court to uphold.

However, we have also not hesitated to strike down as unconstitutional those regulatory provisions that clearly transgress the Constitution and upset the balance between the State's inherent police power and the citizen's fundamental rights. After all, the lofty purpose of police power is to be at the loyal service of personal freedom.

¹³¹ RAY KURZWEIL, *THE AGE OF SPIRITUAL MACHINES: WHEN COMPUTERS EXCEED HUMAN INTELLIGENCE*, 13 (1999); Ray Kurzweil, *The Law of Accelerating Returns*, 7 March 2001, available at <<http://www.kurzweilai.net/the-law-of-accelerating-returns>>, accessed on 29 September 2013.

¹³² See: *Francisco v. House of Representatives*, supra note 2 (citing *Estrada v. Desierto*, [Sep. Op. of J. Mendoza] 406 Phil. 1 [2001]; *Demetria v. Alba*, supra note 2; and *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288 [1936]).

¹³³ See: *Republic v. Roque*, G.R. No. 204603, 24 September 2013.


WHEREFORE, I join the *ponencia* in resolving to leave the determination of the correct application of Section 7 to actual cases, except as it is applied to libel. Charging an offender both under Section 4(c)(4) of the *Cybercrime Prevention Act* and under Article 353 of the *Revised Penal Code* violates the guarantee against double jeopardy and is **VOID** and **UNCONSTITUTIONAL** for that reason.

Moreover, I join in declaring the following as **UNCONSTITUTIONAL**:

1. Section 4(c)(4), insofar as it creates criminal liability on the part of persons who receive a libelous post and merely react to it ;
2. Section 12, insofar as it fails to provide proper safeguards for the exercise of the authority to collect traffic data in real time;
3. Section 19, also insofar as it fails to provide proper standards for the exercise of the authority to restrict or block access to computer data.

However, I vote to declare Section 6 **UNCONSTITUTIONAL**, insofar as it applies to Section 4(c)(4), for unduly curtailing freedom of speech.

As regards the remaining assailed provisions, I vote to **DISMISS** the Petitions for failure to establish that a pre-enforcement judicial review is warranted at this time.


MARIA LOURDES P. A. SERENO
Chief Justice