A Critique of *Disini, Jr. v. Secretary of Justice* on the Constitutionality of the Cybercrime Prevention Act of 2012 in Light of Applicable American Jurisprudence and Recommendations on How to Improve the Act or its Implementing Rules and Regulations

Jose Arturo C. De Castro[*]
Arianne Vanessa Josephine T. Jimenez[**]

---

* '16 J.S.D., cand., University of California-Berkeley School of Law; '14 LL.M., University of California-Berkeley School of Law; '03 J.D., *with honors*, Ateneo de Manila University School of Law. The Author worked as a Presidential Staff Officer and as a Director in the Office of the Executive Secretary from 2003 to 2004 and from 2004 to 2005, respectively. He was also a former Prosecution Attorney under the Office of the Provincial Prosecutor in Bulacan. He was a former Assistant Secretary for the Department of Justice from 2006 to 2010. He was previously a partner at the De Castro & Cagampang-De Castro Law Firm from 2010 to 2013. He is currently a Professor at the Ateneo de Manila University School of Law. The Author previously wrote *The Nature-Based Classification of Crimes: Issues and Clarifications*, 54 ATENEO L.J. 549 (2009); *The Philippine Renewable Energy Act of 2008: Law, Policy, and Promise of Renewables in the Philippines*, 54 ATENEO L.J. 343 (2009); and co-wrote *Recent Amendments and Legislation Affecting the Revised Penal Code of the Philippines*, 58 ATENEO L.J. 289 (2013) with Arianne Vanessa Josephine T. Jimenez.

** '14 LL.M., University of California-Berkeley School of Law; '09 J.D., Ateneo de Manila University School of Law. The Author is a professor at the De La Salle University. She previously worked in the Supreme Court of the Philippines as a Court Attorney under Former Associate Justice, and later Chief Justice, Renato C. Corona from 2009 to 2012. She previously worked under Associate Justice Martin S. Villarama, Jr. from 2012 to 2013. She co-wrote *Recent Amendments and Legislation Affecting the Revised Penal Code of the Philippines*, 58 ATENEO L.J. 289 (2013) with Jose Arturo C. De Castro.

I. INTRODUCTION

This Article evaluates *Disini, Jr. v. Secretary of Justice*,[1] the Philippine Supreme Court decision that discussed the constitutionality of Republic Act (R.A.) No. 10175 (Cybercrime Prevention Act of 2012),[2] from the perspective of United States (U.S.) Supreme Court and various State Supreme Court cases.

To a reader unfamiliar with Philippine law, it is probably surprising to see a critique of a Philippine Supreme Court decision that uses, as its primary tool for analysis, American jurisprudence — both state and federal. However, not only is this method appropriate and practicable in this situation, but it is also necessary. Jurisprudence from various courts of the U.S. have persuasive effect on Philippine Supreme Court decisions.[3] This is due, in large part, to the fact that the 1935 Philippine Constitution was patterned after the constitution of the U.S.[4] Also, Philippine jurisprudence provides that "[w]hen a statute has been adopted from some other state or country and said statute has previously been construed by the courts of such state or country, the statute is deemed to have been adopted with the construction given."[5] With the Cybercrime Prevention Act of 2012 having been patterned after American — even European — statutes[6] and there being a lack of Philippine legal precedent, the use of American jurisprudence

---

Cite as 60 ATENEO L.J. 529 (2015).

1. *Disini, Jr.* v. Secretary of Justice, 716 SCRA 237 (2014).
2. An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes [Cybercrime Prevention Act of 2012], Republic Act No. 10175, § 1 (2012).
3. *See* Philippine Health Care Providers, Inc. v. Commission of Internal Revenue, 600 SCRA 413, 427 (2009).
4. Javellana v. The Executive Secretary, 50 SCRA 30, 82 (1973).
5. *Philippine Health Care Providers, Inc.*, 600 SCRA at 427.
6. *See* Department of Justice Office of Cybercrime, 2014-2015 Cybercrime Report: The Rule of Law in Cyberspace (A Report of the Department of Justice Office of Cybercrime) 17-19, *available at* https://www.doj.gov.ph/files/cybercrime_office/2014-2015_Annual_Cybercrime_Report.pdf (last accessed Nov. 29, 2015).

to analyze and critique *Disini, Jr.*, which is the subject matter of this Article, is appropriate.

The catalyst for the Philippine Supreme Court decision that this Article seeks to analyze is the Cybercrime Prevention Act of 2012; to wit —

> Although the law's stated purpose is to facilitate the prevention, detection, investigation[,] and prosecution of criminal acts online, and the law's proponents claim that it effectively serves to extend the Philippines' constitutional protections into the digital realm, it has been criticized by journalists and civil society organizations who claim that it violates freedom of expression. In the days following its passage, 15 separate petitions were filed [with] the [Philippine Supreme] Court challenging 14 of the law's provisions. As a result, the [Philippine] Supreme Court has suspended [the] implementation of the Cybercrime Prevention Act [of 2012] for 120 days, in order to allow the challenges to proceed.[7]

The Cybercrime Prevention Act of 2012 criminalizes several types of offenses, such as illegal access,[8] data interference,[9] misuse of devices,[10] cyber-squatting,[11] computer-related fraud,[12] and cybersex.[13] Further, the Cybercrime Prevention Act of 2012 reaffirms existing laws against child pornography,[14] an offense punished by R.A. No. 9775 — or the Anti-Child Pornography Act of 2009.[15] It also criminalizes libel[16] — an offense punished by the Revised Penal Code[17] — when committed using a computer

---

7. Centre for Law and Democracy, Philippines: An Analysis of the Cybercrime Prevention Act of 2012 (A Paper by Centre for Law and Democracy) 1, *available at* http://www.law-democracy.org/live/wp-content/uploads/2012/08/Phil.Cybercrime.final_.pdf (last accessed Nov. 29, 2015).
8. Cybercrime Prevention Act of 2012, § 4 (a) (1).
9. *Id.* § 4 (a) (3).
10. *Id.* § 4 (a) (5).
11. *Id.* § 4 (a) (6).
12. *Id.* § 4 (b) (2).
13. *Id.* § 4 (c) (1).
14. Cybercrime Prevention Act of 2012, § 4 (c) (2).
15. An Act Defining the Crime of Child Pornography, Prescribing Penalties Therefor and for Other Purposes, [Anti-Child Pornography Act of 2009], Republic Act No. 9775, §§ 4-5 (2009).
16. Cybercrime Prevention Act of 2012, § 4 (c) (4).
17. An Act Revising the Penal Code and Other Penal Laws [REVISED PENAL CODE], Act No. 3815, as Amended, arts. 353-364 (1930).

system.[18] The Cybercrime Prevention Act of 2012 also mandates that all offenses in the Revised Penal Code and offenses punished by special penal laws are likewise punishable under the Cybercrime Prevention Act of 2012 when committed using a computer.[19] Notably, the corresponding penalties "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."[20]

Moreover, the National Bureau of Investigation and the Philippine National Police must organize a cybercrime unit manned by special investigators who shall exclusively handle cases pertaining to violations of the Cybercrime Prevention Act of 2012.[21] This unit can require the disclosure of computer data from a service provider within 72 hours after receipt of a court warrant[22] and can conduct searches and seizures of computer data and equipment.[23] Special cybercrime courts shall handle cases involving offenses punished by the Cybercrime Prevention Act of 2012.[24] There is also a clause mandating the retention of data on the computer servers of service providers for six months after the date of every electronic transaction, which may be extended for another six months should law enforcement authorities request it.[25]

Initially, the Cybercrime Prevention Act of 2012 also contained provisions that:

(1) penalized spamming;[26]

(2) authorized the collection or recording of traffic data in real-time;[27] and

(3) authorized the Department of Justice to restrict or block access to suspect computer data without need of a court order.[28]

18. Cybercrime Prevention Act of 2012, § 4 (c) (4).

19. *Id.* §§ 6-7.

20. *Id.* § 6.

21. *Id.* § 10.

22. *Id.* § 14.

23. *Id.* § 15.

24. Cybercrime Prevention Act of 2012, § 21.

25. *Id.* § 13.

26. *Id.* § 4 (c) (3). *See also Disini, Jr.*, 716 SCRA at 354.

27. Cybercrime Prevention Act of 2012, § 12. *See also Disini, Jr.*, 716 SCRA at 354.

28. Cybercrime Prevention Act of 2012, § 19. *See also Disini, Jr.*, 716 SCRA at 354.

However, on 18 February 2014, the Philippine Supreme Court promulgated *Disini, Jr.*, which struck down the abovementioned three provisions as unconstitutional[29] and, in the same vein, upheld the rest as valid and constitutional. The parts of the Cybercrime Prevention Act of 2012 that were declared constitutional are the provisions that:

(1) penalize computer-related forgery;[30]

(2) penalize data and system interference,[31] including transmission of viruses;[32]

(3) penalize cyber-squatting;[33]

(4) penalize identity theft;[34]

(5) penalize cybersex;[35]

(6) penalize production of child pornography;[36]

(7) impose penalties one degree higher when crimes defined under the Revised Penal Code are committed with the use of information and communications technologies;[37]

(8) prescribe the penalties for the acts punished by the Cybercrime Prevention Act of 2012;[38]

(9) permit law enforcement authorities to require service providers to preserve traffic data, subscriber information, and specified content data for six months;[39]

(10) authorize the disclosure of computer data when ordered by a court;[40]

---

29. *Disini, Jr.*, 716 SCRA at 354.
30. Cybercrime Prevention Act of 2012, § 4 (b) (1).
31. *Id.* §§ 4 (a) (3) & (4).
32. *Id.* § 4 (a) (4).
33. *Id.* § 4 (a) (6).
34. *Id.* § 4 (b) (3).
35. *Id.* § 4 (c) (1).
36. Cybercrime Prevention Act of 2012, § 4 (c) (2).
37. *Id.* § 6.
38. *Id.* §§ 8-9.
39. *Id.* § 13.
40. *Id.* § 14.

(11) authorize the search, seizure, and examination of computer data when ordered by a court;[41]

(12) authorize the destruction of computer data preserved previously after the expiration of prescribed holding periods;[42]

(13) penalize obstruction of justice in relation to cybercrime investigations;[43]

(14) establish a Cybercrime Investigation and Coordinating Center (CICC);[44]

(15) define the CICC's powers;[45] and

(16) penalize libel according to Articles 353, 354, 361, and 362 of the Revised Penal Code in relation to the Cybecrime Prevention Act of 2012.[46]

This Article demonstrates how portions of *Disini, Jr.* could have been justified in a better manner by adopting certain American court decisions. This Article also shows how some portions of *Disini, Jr.* are erroneous in light of American jurisprudence. This Article also presents recommendations to improve the language of the implementing rules and regulations (IRR) of the Cybercrime Prevention Act of 2012.[47]

II. CRITIQUE

A. On Cybet-squatting

The Cybercrime Prevention Act of 2012 provides —

> Section 4. Cybercrime Offenses. — The following acts constitute the offense of cybercrime punishable under this Act:
>
> (a) Offenses against the confidentiality, integrity[,] and availability of computer data and systems:

41. *Id.* § 15.
42. Cybercrime Prevention Act of 2012, § 17.
43. *Id.* § 20.
44. *Id.* § 24.
45. *Id.* § 26.
46. *Disini, Jr.*, 716 SCRA at 354-355. *See also* REVISED PENAL CODE, arts. 353-54 & 361-62.
47. Rules and Regulations Implementing the Cybercrime Prevention Act of 2012, Republic Act No. 10175 (2015).

...

(6) Cyber-squatting. — The acquisition of domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

(i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;

(ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

(iii) Acquired without right or with intellectual property interests in it.[48]

The petitioners in the *Disini, Jr.* case claimed that the provision on cyber-squatting "violates the equal protection clause in that, not being narrowly tailored, it will cause a user using his real name to suffer the same fate as those who use aliases or take the name of another in satire, parody, or any other literary device."[49] The Philippine Supreme Court dismissed this claim by concluding that "the law is reasonable in penalizing [a person] for acquiring the domain name in bad faith to profit, mislead, destroy reputation, or deprive others who are not ill-motivated of the rightful opportunity of registering the same."[50] The Philippine Supreme Court stated that "it is the evil purpose for which [a person] uses the [domain] name that the law condemns."[51] The constitutionality of the provision on cyber-squatting has, thus, been validated.

Though the ruling is correct, this would have been an opportune time for the Philippine Supreme Court to clarify the nuances between the issues of bad faith on one hand and satire, parody, or any other literary device on the other vis-à-vis the acquisition of domain names. Resorting to *Lamparello v. Falwell*,[52] a case decided by the U.S. Court of Appeals, would be appropriate —

> Reverend Falwell is 'a nationally known minister who has been active as a commentator on politics and public affairs.' He holds the common law

48. Cybercrime Prevention Act of 2012, § 4 (a) (6).

49. *Disini, Jr.*, 716 SCRA at 305.

50. *Id.* at 305-06.

51. *Id.* at 305.

52. Lamparello v. Farewell, 420 F.3d 309 (4th Cir. 2005) (U.S.).

> trademarks 'Jerry Falwell[,]' [ ] 'Falwell,' and the registered trademark 'Listen America with Jerry Falwell.' Jerry Falwell Ministries can be found online at 'www.falwell.com,' a website[,] which receives 9,000 hits (or visits) per day.
>
> Lamparello registered the domain name 'www.fallwell.com' on [11 February 1999], after hearing Reverend Falwell give an interview 'in which he expressed opinions about gay people and homosexuality that [Lamparello] considered ... offensive.' Lamparello created a website at that domain name to respond to what he believed were 'untruths about gay people.'[53]

Christopher Lamparello's website contained criticisms against Reverend Jerry L. Falwell Sr.'s views.[54] In response, Falwell sent Lamparello cease and desist letters, demanding that the latter stop using the domain "www.fallwell.com" or any other domain name employing a variation of Falwell's name.[55] Lamparello filed an action for declaratory judgment of non-infringement.[56] In response, Falwell alleged, among others, a violation of the cyber-squatting provision under the provision on cyberpiracy prevention of the Anticybersquatting Consumer Protection Act (ACPA).[57]

---

53. *Id.* at 311 (citing Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 47 (1988)).

54. *Id.*

55. *Id.* at 312.

56. *Id.*

57. *Id.* Reverend Jerry S. Falwell, Sr. cited a violation of this provision of the Anticybersquatting Consumer Protection Act —

> (a) Cyberpiracy prevention
>
> (1)
>
> (A) A person shall be liable in a civil action by the owner of a mark, including a personal name which[,] is protected as a mark under this section, if, without regard to the goods or services of the parties, that person —
>
> (i) has a bad faith intent to profit from that mark, including a personal name[,] which is protected as a mark under this section; and
>
> (ii) registers, traffics in, or uses a domain name that —
>
> (I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;
>
> (II) in the case of a famous mark that is famous at the time of registration of the domain

The U.S. Court of Appeals ruled in favor of Lamparello with regard to the cyber-squatting claim.[58] The U.S. Court of Appeals relied primarily on the ACPA —

> To prevail on a cyber[-]squatting claim, Reverend Falwell must show that [Lamparello] (1) 'had a bad faith intent to profit from using the [www.fallwell.com] domain [name]' and [that] (2) the domain name www.fallwell.com 'is identical or confusingly similar to, or dilutive of, the distinctive and famous [Falwell] mark.'
>
> 'The paradigmatic harm that the ACPA was enacted to eradicate' is 'the practice of cyber[-]squatters registering several hundred domain names in an effort to sell them to the legitimate owners of the mark.' The [ACPA] was also intended to stop the registration of multiple marks with the hope of selling them to the highest bidder, 'distinctive marks to defraud consumers' or 'to engage in counterfeiting activities,' and 'well-known marks to prey on consumer confusion by misusing the domain name to divert customers from the mark owner's site to the cyber[-]squatter's own site, many of which are pornography sites that derive advertising revenue based on the number of visits, or 'hits,' the site receives.' The [ACPA] was not intended to prevent 'noncommercial uses of a mark, such as for comment, criticism, parody, news reporting, etc.,' and[,] thus[,] they 'are beyond the scope' of the ACPA.[59]

The U.S. Court of Appeals went on to say that the ACPA instructs the courts to consider the following factors (Factors) in distinguishing abusive domain name registrations from legitimate ones:[60]

> (I) [T]he trademark or other intellectual property rights of the person, if any, in the domain name;

> name, is identical or confusingly similar to or dilutive of that mark; or
>
> (III) is a trademark, word, or name protected by reason of section 706 of title 18 or section 220506 of title 36.

Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125 (d) (1999).

58. *Lamparello*, 420 F.3d at 322.

59. *Id.* at 318-19 (citing People for the Ethical Treatment of Animals v. Doughney, 263 F.3d 359, 364 (4th Cir. 2001) (U.S.); Lucas Nursery & Landscaping, Inc. v. Grosse, 359 F.3d 806, 810 (6th Cir. 2004) (U.S.); & Committee on the Judiciary, S. Rep. No. 106-140, at 5-6, 106th Cong., 1st Sess. (U.S.) (1999)).

60. *Id.* at 319.

(II) [T]he extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) [T]he person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) [T]he person's bona fide non[-]commercial or fair use of the mark in a site accessible under the domain name;

(V) [T]he person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) [T]he person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) [T]he person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) [T]he person's registration or acquisition of multiple domain names[,] which the person knows are identical or confusingly similar to marks of others[,] that are distinctive at the time of the registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) [T]he extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c) (1) of this section.[61]

The U.S. Court of Appeals continued its reasoning in favor of Lamparello by saying that "Reverend Falwell cannot demonstrate that Lamparello 'had a bad faith intent to profit from using the www.fallwell.com domain name.'"[62] It was clear to the U.S. Court of Appeals that Lamparello used the domain name "www.fallwell.com" simply to criticize Reverend

61. *Id.* (citing ACPA, 15 U.S.C. §§ 1125 (d) (1) (B) (i) (I)-(IX)).

62. *Id.* at 320 (citing *People for the Ethical Treatment of Animals*, 263 F.3d at 367).

Falwell's views.[63] Also, "Factor IV of the ACPA counsels against finding a bad faith intent to profit in such circumstances because 'use of a domain name for purposes of ... comment, [and] criticism' constitutes a 'bona fide non[-]commercial or fair use' under the statute.'"[64] The U.S. Court of Appeals also said that "Lamparello has not engaged in the type of conduct described in the statutory factors as typifying the bad faith intent to profit essential to a successful cyber[-]squatting claim"[65] because the subject domain name does not create a likelihood of confusion.[66] The U.S. Court of Appeals also held that Factors VI and VIII, among the Factors listed above, counsel against a finding of bad faith because Lamparello neither made attempt to transfer the domain name for financial gain, nor did he use multiple domain names.[67]

The Philippine Supreme Court should not have stopped at merely identifying that bad faith characterizes the offense of cyber-squatting in the Cybercrime Prevention Act of 2012. It should have given factors to consider in weighing whether one's act of acquiring a domain name was done in bad faith. It should have also addressed the concerns of possible defenses when one is charged with the offense of cyber-squatting, specifically satire, parody, or any other form of fair criticism and comment protected by the right of free speech enshrined in the Constitution.[68]

The Philippine Supreme Court could have adopted the jurisprudential doctrines presented in *Lamparello* — as adopted from the Factors listed in the ACPA — to illustrate what characterizes bad faith, or the absence thereof, in the use or acquisition of domain names. The Philippine Supreme Court could have also used the opportunity to clarify that the use of a domain name can be a legitimate exercise or mode of fair criticism and comment.

The Authors recommend that the IRR of the Cybercrime Prevention Act of 2012 should provide a test or a list of factors, similar to that listed above, that could aid the courts in determining whether one's act of acquiring a domain name is legitimate or abusive. This could be a useful tool

63. *Id.*

64. *Lamparello*, 420 F.3d at 320 (citing ACPA, 15 U.S.C. § 1125 (d) (1) (B) (i) (IV)).

65. *Id.*

66. *Id.*

67. *Id.*

68. The Constitution provides that "[n]o 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." PHIL. CONST. art. III, § 4.

in interpreting the more general cyber-squatting provision of the Cybercrime Prevention Act of 2012. What the Philippine Supreme Court failed to do may still be remedied by the amendments to the IRR. Also, in doing this, the IRR could lessen litigation on the matter by giving potential acquirers of domain names and prospective complainants a guide in determining whether such acquisition of a domain name is legitimate or whether it is abusive.

B. On Cybersex

The Cybercrime Prevention Act of 2012 provides —

> Sec. 4. Cybercrime Offenses. — The following acts constitute the offense of cybercrime punishable under this Act:
>
> ...
>
> (c) Content-related Offenses:
>
> (1) Cybersex. — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.[69]

The same petitioners in the *Disini, Jr.* case claimed that this provision violates the freedom of expression protected by the Constitution and that private communications of sexual character between consenting adults, which are not crimes under the Revised Penal Code, would, then, be regarded as crimes when done "for favor" in cyberspace.[70] Note that both in common usage and Philippine jurisprudence, "for favor" includes "gracious kindness," "a special privilege or right granted or conceded," or "a token of love ... usually worn conspicuously."[71]

The Philippine Supreme Court addressed this issue by reasoning that the Congressional records of the deliberations on the Cybercrime Prevention Act of 2012 reveal that there is "a lack of intent to penalize a 'private showing ... between and among two private persons ... although that may be a form of obscenity to some.'"[72] The Philippine Supreme Court stated that "the understanding of those who drew up the [Cybercrime Prevention Act of 2012] is that the element of 'engaging in a business' is necessary to

69. Cybercrime Prevention Act of 2012, § (4) (c) (1).

70. *Disini, Jr.*, 716 SCRA at 309.

71. *Id.* (citing Merriam-Webster Dictionary, Favor, *available at* http://www.merriam-webster.com/dictionary/favor (last accessed Nov. 29, 2015)).

72. *Id.* at 310.

constitute the illegal cybersex. The [Cybrercrime Prevention Act of 2012] actually seeks to punish cyber prostitution."[73]

The problem with this kind of reasoning is that the Philippine Supreme Court is not restricted from interpreting the cybersex provision of the Cybercrime Prevention Act of 2012 in a manner contrary to its current interpretation. The "'plain meaning rule' or *verba legis* in statutory construction [means] that if the statute is clear, plain, and free from ambiguity, it must be given its literal meaning and applied without interpretation."[74] Hence, it is possible that a future composition of the Philippine Supreme Court will choose to use the plain meaning rule in interpreting the cybersex provision. Applying the plain meaning rule, even consenting adults who engage in cybersex for favor, such as "gracious kindness," as stated above, would be committing a crime.

Moreover, in choosing to uphold the validity and constitutionality of the cybersex provision, as it is currently worded, the Philippine Supreme Court neglected the overbreadth rule employed in the Philippines as a test to determine the constitutionality of statutes, which could infringe fundamental constitutional rights, such as freedom of speech. The overbreadth doctrine decrees "that a governmental purpose to control or prevent activities constitutionally subject to state regulations may not be achieved by means[,] which sweep unnecessarily broadly and[,] thereby[,] invade the area of protected freedoms."[75] As the wording of the cybersex provision now stands, the stated government purpose of preventing online prostitution is sought to be achieved by a regulation that unnecessarily intrudes into a protected freedom, such as private sexual conduct between two consenting adults. Clearly, the cybersex provision is overbroad.

A U.S. Supreme Court case that could have been used by the Philippine Supreme Court to address the overbreadth of the cybersex provision is *Brown v. Entertainment Merchants Assn.*[76] In this case, a California statute that "prohibits the sale or rental of 'violent video games' to minors and requires their packaging to be [labelled] '18'"[77] was alleged as being in violation of

73. *Id.*

74. Republic v. Lacap, 517 SCRA 255, 268 (2007) (citing Commissioner of Internal Revenue v. Central Luzon Drug Corporation, 456 SCRA 414, 443 (2005); National Federation of Labor v. NLRC, 327 SCRA 158, 165 (2000); & RUBEN E. AGPALO, STATUTORY CONSTRUCTION 124 (2003 ed.)).

75. Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council, 632 SCRA 146, 185 (2010).

76. Brown v. Entertainment Merchants Assn., 564 U.S. 08-1448 (2011).

77. *Id.*

the First Amendment.[78] The parties in *Brown* agreed that video games qualify for First Amendment protection.[79] Further, "[b]ecause the Act imposes a restriction on the content of protected speech, it is invalid unless California can demonstrate that it passes strict scrutiny — that is, unless it is justified by a compelling government interest and is narrowly drawn to serve that interest."[80] The U.S. Supreme Court ruled that the challenged California statute is, among other things, overbroad.[81] It stated that "California's legislation straddles the fence between addressing [ ] a serious social problem and [ ] helping concerned parents control their children. Both ends are legitimate[;] but when they affect First Amendment rights[,] they must be pursued by means that are neither seriously under[-]inclusive nor seriously over[-]inclusive."[82] The over-inclusiveness in *Brown* was due to the challenged California statute abridging the "First Amendment rights of young people whose parents (and [aunties] and uncles) think violent video games are a harmless [pastime]."[83]

Both the cybersex provision of the Cybrecrime Prevention Act of 2012 and the California statute regarding violent video games that were struck down as unconstitutional had legitimate ends to achieve. However, both these statutes utilize means that unnecessarily intrude into protected freedoms. The Philippine Supreme Court should have recognized the overbreadth of the cybersex provision of the Cybercrime Prevention Act of 2012 and declared it void and unconstitutional.

The Authors recommend that the IRR of the Cybercrime Prevention Act of 2012 be amended to explicitly clarify that the cybersex provision does not cover sexual acts between two consenting adults or, at most, that the criminal act be restricted to adults engaging in habitual cybersex involving monetary consideration to make it consistent with Philippine criminal laws on prostitution.[84]

C. On Libel

78. *Id. See also* U.S. CONST. amend. I.

79. *Brown*, 564 U.S. 08-1448.

80. *Id.* (citing R. A. V. v. St. Paul, 505 U.S. 377, 395 (1992)).

81. *Id.*

82. *Id.*

83. *Id.*

84. The Revised Penal Code provides that "women who, for money or profit, habitually indulge in sexual intercourse or lascivious conduct, are deemed to be prostitutes." REVISED PENAL CODE, art. 202.

The petitioners in the *Disini, Jr.* case also challenged the constitutionality of both the Revised Penal Code and the Cybercrime Prevention Act of 2012 provisions on libel. The Revised Penal Code provides —

> Art. 353. *Definition of libel.* — A libel is [a] public and malicious imputation of a crime, or of a vice or defect, real or imaginary, or any act, omission, condition, status, or circumstance tending to cause the dishonor, discredit, or contempt of a natural or juridical person, or to blacken the memory of one who is dead.
>
> Art. 354. *Requirement for publicity.* — Every defamatory imputation is presumed to be malicious, even if it be true, if no good intention and justifiable motive for making it is shown, except in the following cases:
>
> (1) A private communication made by any person to another in the performance of any legal, moral[,] or social duty; and
>
> (2) A fair and true report, made in good faith, without any comments or remarks, of any judicial, legislative[,] or other official proceedings[,] which are not of confidential nature, or of any statement, report[,] or speech delivered in said proceedings, or of any other act performed by public officers in the exercise of their functions.[85]

The Cybercrime Prevention Act of 2012, on the other hand, states —

> Sec. 4. Cybercrime Offenses. — The following acts constitute the offense of cybercrime punishable under this Act:
>
> ...
>
> (c) Content-related Offenses:
>
> ...
>
> (4) Libel. — The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means[,] which may be devised in the future.[86]

The petitioners argued that the libel provisions of both the Revised Penal Code and the Cybercrime Prevention Act of 2012 carry with them the requirement of "presumed malice" even though the most recent Philippine jurisprudence already utilizes the higher standard of "actual malice" as a basis for conviction.[87] Further, the petitioners "argue that inferring 'presumed

85. *Id.* arts. 353-54.

86. Cybercrime Prevention Act of 2012, § (4) (c) (4).

87. *Disini, Jr.*, 716 SCRA at 316 (citing Borjal v. Court of Appeals, 301 SCRA 1, 31 (1999)).

malice' from the accused's defamatory statement by virtue of Article 354 of the [Revised Penal Code] infringes on [their] constitutionally guaranteed freedom of expression."[88] The petitioners even went as far as saying that both the Revised Penal Code and the Cybercrime Prevention Act of 2012 violate the Philippines' obligations under the International Covenant of Civil and Political Rights.[89] The petitioners referred[90] to *Alexander Adonis v. Republic of the Philippines*,[91] where the United Nations Human Rights Committee (UNHRC) cited its General Comment No. 34[92] to "the effect that penal defamation laws should include the defense of truth."[93]

The Philippine Supreme Court, in upholding the constitutionality of the libel provisions both in the Revised Penal Code and in the Cybercrime Prevention Act of 2012, stated that "General Comment [No.] 34 does not say that the veracity of the libelous statement should be an all-encompassing defense."[94] The Philippine Supreme Court then referred to Article 361[95] of

88. *Id.* at 317.

89. *Id.* at 319.

90. *Id.*

91. U.N. Human Rights Committee, *Alexander Adonis v. The Philippines, Communication No. 1815/2008*, U.N. Doc. CCPR/C/103/D/1815/2008 (Apr. 26, 2012).

92. Specifically, the petitioners in the *Disini, Jr.* case argued that

> defamation laws must be crafted with care to ensure that they comply with paragraph 3, and that they do not serve, in practice, to stifle freedom of expression. All such laws, [penal defamation laws in particular], should include such [defenses] as the [defense] of truth and they should not be applied with regard to those forms of expression that are not, of their nature, subject to verification. At least with regard to comments about public figures, consideration should be given to avoiding penalizing or otherwise rendering unlawful untrue statements that have been published in error but without malice. In any event, a public interest in the subject matter of the criticism should be recognized as a [defense]. Care should be taken by States parties to avoid excessively punitive measures and penalties. ... States parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty.

Id. (citing U.N. Human Rights Committee, *General Comment No. 34 (Article 19: Freedoms of Opinion and Expression)*, ¶ 47 at 12, U.N. Doc. CCPR/C/GC/34 (Sep. 12, 2011) [hereinafter *General Comment No. 34*]).

93. *Disini, Jr.*, 716 SCRA at 319.

94. *Id.* (citing *General Comment No. 34*, *supra* note 92).

the Revised Penal Code, which recognizes truth as a defense,[96] but only under the condition that the accused was "prompted in making the statement by good motives and for justifiable ends."[97] The Philippine Supreme Court went on to say that the UNHRC did not, in actuality, demand that the Philippines decriminalize libel;[98] it merely suggested that defamation laws be crafted carefully so that they do not stifle freedom of expression.[99]

The Authors agree with the Concurring and Dissenting Opinion of Associate Justice Antonio T. Carpio[100] that the libel provisions of both the Revised Penal Code and the Cybercrime Prevention Act of 2012 are inconsistent with the free speech principles prevailing in both American and Philippine jurisprudence —

> [w]hile the text of Article 354 has remained intact since the [Revised Penal] Code's enactment in 1930, constitutional rights have rapidly expanded since the latter half of the last century, owing to expansive judicial interpretations of broadly worded constitutional guarantees such as the Free Speech Clause. Inevitably, judicial doctrines crafted by the U.S. Supreme Court protective of the rights to free speech, free expression[,] and free press found their way into local jurisprudence, adopted by [the Philippine Supreme] Court as authoritative interpretation of the Free Speech Clause in the Philippine Bill of Rights. One such doctrine is the

---

95. The Revised Penal Code provides —

> Art 361. *Proof of the truth.* — In every criminal prosecution for libel, the truth may be given in evidence to the court and if it appears that the matter charged as libelous is true, and moreover, that it was published with good motives and for justifiable ends, the defendant shall be acquitted.
>
> Proof of the truth of an imputation of an act or omission not constituting a crime shall not be admitted unless the imputation shall have been made against Government employees with respect to facts related to the discharge of their official duties.
>
> In such cases if the defendant proves the truth of the imputation made by him, he shall be acquitted.

REVISED PENAL CODE, art. 361.

96. *Disini, Jr.*, 716 SCRA at 319.

97. *Id.*

98. *Id.*

99. *Id.* at 319-20.

100. *Id.* at 427 (J. Carpio, concurring and dissenting opinion).

> *New York Times* [*Co.*] actual malice rule, named after the 1964 case in which it was crafted, [*New York Times Co. v. Sullivan*].[101]

New York Times Co. recognized that "erroneous statement is inevitable in free [debate] and that it must be protected if the freedoms of expression are to have the 'breathing space' that they 'need ... to survive."[102] Hence, *New York Times Co.* held that constitutional guarantees require a rule "that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice' — that is, with knowledge that it was false or with reckless disregard of whether it was false or not."[103] Further, a "rule compelling the critic of official conduct to guarantee the truth of all his factual assertions — and to do so on pain of libel judgments virtually unlimited in amount — leads to a comparable 'self-censorship.'"[104] Indeed, adhering to the "defense of truth" would see the difficulty of "adducing legal proofs that the alleged libel was true in all its factual particulars."[105] Moreover,

> [u]nder such a rule, would-be critics of official conduct may be deterred from voicing their criticism, even though it is believed to be true and even though it is in fact true, because of doubt whether it can be proved in court or fear of the expense of having to do so. They tend to make only statements[,] which 'steer far wider of the unlawful zone.' The rule thus dampens the vigor and limits the variety of public debate. It is inconsistent with the First and Fourteenth Amendments.[106]

Six years after *New York Times Co.*, the Philippine Supreme Court — in *Lopez v. Court of Appeals*[107] — adopted the actual malice doctrine[108] and has since adhered to the *New York Times Co.* doctrine to dismiss both civil and

---

101. *Id.* at 429 (citing New York Times Co. v. Sullivan, 376 U.S.254 (1964)).

102. *Disini, Jr.*, 716 SCRA at 430. (citing *New York Times Co.*, 376 U.S. at 271-72).

103. *New York Times Co.*, 376 U.S. at 376.

104. *Id.*

105. *Id.*

106. *Id.* at 375.

107. Lopez v. Court of Appeals, 34 SCRA 116, 126 (1970)). This case decided by the Philippine Supreme Court formally adopted the actual malice rule in the Philippines as against the presumed malice rule as embodied in the Revised Penal Code. *Id.*

108. *Disini, Jr.*, 716 SCRA at 431 (J. Carpio, concurring and dissenting opinion) (citing *Lopez*, 34 SCRA at 126).

criminal libel complaints.[109] The actual malice rule has three specific principles, to wit:

> (a) Malice is not presumed even in factually false and defamatory statements against public officers and public figures[.] [I]t must be proven as a fact for civil and criminal liability to lie;
>
> (b) Report on official proceedings or conduct of an officer may contain fair comment, including factually erroneous and libelous criticism; and
>
> (c) Truth[,] or lack of reckless disregard for the truth[,] or falsity of a defamatory statement is an absolute defense against public officers and public figures.[110]

On the other hand, the principles behind the libel provisions of the Revised Penal Code are the following:

> (a) Malice is presumed in every defamatory imputation, even if true (unless good intention and justifiable motives are shown);
>
> (b) Report on official proceedings or conduct of an officer must be made without comment or [remarks] or, alternatively, must be made without malice; [and]
>
> (c) In defamatory allegations made against a public official, truth is a defense only if the imputed act or omission constitutes a crime or if the imputed act or omission relates to official duties.[111]

As observed by Associate Justice Carpio, the actual malice rule and the libel provisions of the Revised Penal Code cannot be reconciled as regards "(1) the necessity of proof of malice in defamatory allegations against public proceedings or the conduct of a public officer or [a] public figure and (2) the availability of truth as a defense in defamatory imputations against public officers or public figures."[112]

Here, "[t]he former requires proof of malice and allows truth as a defense unqualifiedly, while the latter presumes malice and allows truth selectively."[113] It is, then, clear that the actual malice rule, which has already been enshrined in Philippine constitutional law through jurisprudential doctrines in freedom of speech cases, and the libel provisions in the Revised Penal Code, specifically Article 354, are irreconcilable.

---

109. *Id.*

110. *Id.* at 432 (emphasis omitted).

111. *Id.* at 432–33 (citing REVISED PENAL CODE, art. 361).

112. *Id.* at 433.

113. *Id.*

Considering that the online libel provision of the Cybercrime Prevention Act of 2012 relies upon the libel provisions of the Revised Penal Code for its efficacy and enforceability — and considering that, as illustrated above, the latter is clearly repugnant to the actual malice rule and, hence, is irreconcilable with recognized constitutional interpretations of the right to free speech, then it is but right to strike down these provisions for being unconstitutional. Indeed, "[a]llowing a criminal statutory provision clearly repugnant to the Constitution, and directly attacked for such repugnancy, to[,] nevertheless[,] remain in the statute books is a gross constitutional anomaly[,] which, if tolerated, weakens the foundation of constitutionalism in this country."[114] To craft a new law based on an unconstitutional criminal statute exacerbates this anomaly. To make things worse, libel, if committed online, shall be penalized by a penalty one degree higher than that provided for by the Revised Penal Code.[115]

The Philippine Supreme Court should have taken this opportunity to strike down the libel provisions of both the Revised Penal Code and the Cybercrime Prevention Act of 2012 as unconstitutional. The Authors strongly recommend that the online libel provision be deleted from the Cybercrime Prevention Act of 2012, if amendments are to be done in the future. Considering that the Revised Penal Code is currently undergoing revisions,[116] the criminal libel statute should be amended to incorporate the actual malice rule instead of the presumed malice rule.

D. On Real-Time Collection of Traffic Data

The Cybercrime Prevention Act of 2012 provides —

> Sec. 12. *Real-Time Collection of Traffic Data.* — Law enforcement authorities, with due cause, shall be authorized to collect or record[,] by technical or electronic means[,] traffic data in real-time associated with specified communications transmitted by means of a computer system.
>
> Traffic data refer only to the communication's origin, destination, route, time, date, size, duration, or type of underlying [service] but [neither content] nor identities.
>
> All other data to be collected[,] [ ]seized[,] or disclosed will require a court warrant.

114. *Disini, Jr.*, 716 SCRA at 433-34.

115. *See* Cybercrime Prevention Act of 2012, § 6.

116. Department of Justice, Criminal Code Committee, Department Circular No. 19 [DOJ. Circ. No. 19-11] (Apr. 20, 2011).

> Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.
>
> The court warrant required under this section shall only be issued or granted upon written application[,] [ ] the examination under oath or affirmation of the applicant and the witnesses he may produce[,] and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated [herein] has been committed, or is being committed, or is about to be committed; (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, [ ] to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.[117]

Lastly, the petitioners in *Disini, Jr.* also claimed that giving law enforcement agencies the authority to collect or record traffic data in real-time tends to "curtail civil liberties or provide opportunities for official abuse."[118] The petitioners invoked the right of every individual to privacy.[119]

The Philippine Supreme Court ruled in favor of the petitioners on this issue and declared that the "authority that Section 12 gives law enforcement agencies is too sweeping and lacks restraint."[120] Though the Philippine Government has a compelling interest in providing law enforcement agencies with the tools necessary to spot, prevent, and investigate crimes,[121] the Philippine Supreme Court declared that there are certain constitutional guarantees that ensure the existence of zones of privacy where governmental powers may not intrude without a court warrant[122] and that there exists an independent constitutional right of privacy.[123]

The Philippine Government cited *Smith v. Maryland*,[124] a case decided by the U.S. Supreme Court to further its doomed arguments. According to the Philippine Supreme Court, *Smith* "reasoned that telephone users in the [1970s] must realize that they necessarily convey phone numbers to the

117. Cybercrime Prevention Act of 2012, § 12.

118. *Disini, Jr.*, 716 SCRA at 336.

119. *Id.* at 336-37.

120. *Id.* at 343.

121. *Id.* at 337.

122. *Id.* at 307.

123. *Id.*

124. Smith v. Maryland, 442 U.S. 735 (1979).

telephone company in order to complete a call."[125] The Philippine Supreme Court further stated that, in *Smith*, "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.'"[126] Indeed, *Smith* reiterates the proposition that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[127] The Philippine Supreme Court, however, concluded that

> when seemingly random bits of traffic data are gathered in bulk, pooled together, and analyzed, they reveal patterns of activities[,] which can[,] then[,] be used to create profiles of the persons under surveillance. With enough traffic data, analysts may be able to determine a person's close associations, religious views, political affiliations, [and] even sexual preferences. Such information is likely beyond what the public may expect to be [disclosed] and clearly falls within matters protected by the right to privacy.[128]

This, coupled with the fact that real-time collection of traffic data may be done by authorities "with due cause,"[129] which was seen by the Philippine Supreme Court as granting the Philippine Government a constitutionally-prohibited general search warrant,[130] was reason enough for the provision on real-time collection of traffic data to be struck down as void and unconstitutional.[131]

Though the conclusion is sound, it would have been helpful if the Philippine Supreme Court used *State v. Hunt*,[132] a New Jersey Supreme Court case that involved the issue of the "constitutionality of the warrantless search and seizure of defendants' telephone toll billing records."[133] In that case,

> [t]he telephone caller is 'entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.' Similarly, he is entitled to

125. *Disini, Jr.*, 716 SCRA at 343-44.

126. *Id.* at 408 (C.J. Sereno, concurring and dissenting opinion) (citing *Smith*, 442 U.S. at 743-44) (emphasis omitted).

127. *Smith*, 442 U.S. at 743-44.

128. *Disini, Jr.*, 716 SCRA at 342.

129. Cybercrime Prevention Act of 2012, § 12.

130. *Disini, Jr.*, 716 SCRA at 343.

131. *Id.* at 354.

132. State v. Hunt, 91 N.J. 338 (N.J. 1982) (U.S.).

133. *Id.* at 340-41.

> assume that the numbers he dials in the privacy of his home will be recorded solely for the telephone company's business purposes. From the viewpoint of the customer, all the information[,] which he furnishes with respect to a particular call[,] is private. The numbers dialed are private. The call is made from a person's home or office, locations entitled to protection under the Fourth Amendment[.]
>
> ...
>
> It is unrealistic to say that the cloak of *privacy* has been shed because the telephone company and some of its employees are aware of this information. Telephone calls cannot be made except through the telephone company's property and without payment to it for the service. This disclosure has been necessitated because of the nature of the instrumentality, but more significantly[,] the disclosure has been made for a limited business purpose and not for release to other persons for other reasons. The toll billing record is a part of the *privacy* package.[134]

Hunt criticized *Smith* and cited examples of other cases promulgated by courts of other states rejecting the same.[135] Moreover, it held that

> a telephone subscriber has a reasonable expectation that the calls he makes will be utilized only for the accounting functions of the telephone company and that he cannot anticipate that his personal life, as disclosed by the calls he makes and receives, will be disclosed to outsiders without legal process.[136]

Hunt is an excellent case that upholds the privacy rights of citizens in traffic data. Though traffic data does not reveal much of the content of conversations — specifically in electronic mails and other electronic communications, if in the contemplation of the Cybercrime Prevention Act of 2012 — still, if aggregated and interpreted, traffic data can reveal facts about an individual that falls within one's sphere or privacy.[137] Information, which, traditionally, may only be obtained under court-issued processes,[138] may be sought and discovered by putting together bits of traffic data if the provision on real-time collection of data was upheld. Accordingly, it was right for the Philippine Supreme Court to invalidate that provision on real-time collection of data in the Cybercrime Prevention Act of 2012. However,

---

134. *Id.* at 346-47 (citing Katz v. United States, 389 U.S. 347, 352 (1967); U.S. CONST. amend. IV; & N.J. CONST. art. VII, ¶ 1) (emphasis supplied).

135. *Id.* at 348.

136. *Id.* (citing People v. Blair, 25 Cal. 3d. 646, 653 (1979) (U.S.)).

137. *See Disini, Jr.*, 716 SCRA at 451-52 (J. Carpio, concurring and dissenting opinion).

138. *Id.*

citing *Hunt*, instead of *Smith*, to justify its conclusions would have been helpful in buttressing the Philippine Supreme Court's discussion.

III. CONCLUSION

American jurisprudence has long aided the Philippine Supreme Court in resolving contentious and novel issues, especially in situations where there is no available Philippine jurisprudence, which the Philippine Supreme Court can resort to for construction. This Article has shown how, in *Disini, Jr.*, American jurisprudence could be used and how the Philippine Supreme Court's discussions and conclusions could have been justified in a better manner.

From among several possible issues presented by the Cybercrime Prevention Act of 2012, this Article chose four of the most contentious to evaluate in light of applicable American jurisprudence.

First, regarding the ruling on the provision on cyber-squatting as valid. The Authors submit that the Philippine Supreme Court could have used this opportunity to clarify what acts could qualify as abusive. The "bad faith" requirement in the provision could have been clarified by adopting the Factors used in *Lamparello*. Also, the Philippine Supreme Court could have established that literary devices, such as satire, parody, and fair comment, could be used as a defense in a charge of cyber-squatting, as what American courts have done.

Second, regarding the ruling on the provision on cybersex as valid. The Authors argue that this conclusion is erroneous because the provision is overbroad. Though there is a legitimate government interest involved, the means to prevent online prostitution and to protect children online unduly encroach into protected space — private, consensual, and sexual acts of adults. The rule of strict scrutiny used in *Brown* and other American and Philippine jurisprudence should have been used in analyzing the validity of this provision.

Third, regarding the ruling on online libel as valid. The Authors submit that *Disini, Jr.* was the opportune time to strike down a statute rendered unconstitutional by the evolution of American and Philippine jurisprudence on the issue of free speech vis-à-vis defamation.[139] Indeed, *New York Times*

139. The declaration of a statute originally valid and constitutional as void and unconstitutional was referred to by the Philippine Supreme Court as the process of "relative unconstitutionality," to wit —

> [t]he constitutionality of a statute cannot, in every instance, be determined by a mere comparison of its provisions with applicable

Co., together with *Lopez*, established the actual malice rule for conviction to arise in libel cases. Hence, the presumption of malice rule in the Revised Penal Code and adopted by the Cybercrime Prevention Act of 2012 is rendered extant and should, thus, be declared unconstitutional.

Last, regarding the ruling on real-time collection of data as unconstitutional. The Philippine Supreme Court rightfully rejected the conclusion in *Smith*, which ruled that an individual has no privacy interest in the phone numbers that one voluntarily dials. However, it would have been more prudent for the Philippine Supreme Court to have cited cases, such as *Hunt*, that explicitly declared that there is a privacy right in traffic data, such as telephone numbers. In *Disini, Jr.*, *Hunt* could have been construed as recognizing privacy rights to traffic data that do not show the content of communications, but reveal other information when they are pieced together, such as the origin, source, destination, time, and size of electronic communications.

Undeniably, American jurisprudence on Internet law issues will prove to be a useful aid in resolving Philippine disputes that will involve its newly-enacted Cybercrime Prevention Act of 2012.

> provisions of the Constitution, since the statute may be constitutionally valid as applied to one set of facts and invalid in its application to another.
>
> A statute valid at one time may become void at another time because of altered circumstances. Thus, if a statute in its practical operation becomes arbitrary or confiscatory, its validity, even though affirmed by a former adjudication, is open to inquiry and investigation in the light of changed conditions.

Central Bank Employees Association, Inc. v. Bangko Sentral ng Pilipinas, 446 SCRA 299, 347-48 (2004) (citing Medill v. State, 477 N.W.2d 703 (Minn. 1991) (U.S.); In Re Cook, 138 B.R. 943 (Minn. Bankr. D. 1992) (U.S.); Nashville, C. & St. L. Ry. v. Walters, 294 U.S. 405 (1935); Atlantic Coast Line R. Co. v. Ivey, 148 Fla. 680 (1941) (U.S.); Louisville & N. R. Co. *v.* Faulkner, 7 S.W.2d 196 (Ky. 1957) (U.S.); Vernon Park Realty *v.* City of Mount Vernon, 307 N.Y. 493 (1954) (U.S.); & Murphy v. Edmonds, 325 Md. 342 (1992) (U.S.)) (emphasis omitted).