

REPUBLIC OF THE PHILIPPINES
SUPREME COURT
MANILA

SUPREME COURT
RECEIVED
BY: _____

2012 SEP 25 PM 3: 27

JOSE JESUS M. DISINI, JR.,
ROWENA S. DISINI, LIANNE IVY
P. MEDINA, JANETTE TORAL and
ERNESTO SONIDO, JR.,

Petitioners,

- versus -

G.R. NO 203335

THE SECRETARY OF JUSTICE,
THE SECRETARY OF THE
DEPARTMENT OF THE INTERIOR
AND LOCAL GOVERNMENT, THE
EXECUTIVE DIRECTOR OF THE
INFORMATION AND
COMMUNICATIONS
TECHNOLOGY OFFICE, THE
CHIEF OF THE PHILIPPINE
NATIONAL POLICE and THE
DIRECTOR OF THE NATIONAL
BUREAU OF INVESTIGATION,

Respondents.

X-----X

PETITION FOR CERTIORARI AND PROHIBITION

WITH PRAYER FOR A TEMPORARY RESTRAINING ORDER

PETITIONERS, through the undersigned counsel, unto this
Honorable Supreme Court, most respectfully state:

PREFATORY STATEMENT

The present petition is a taxpayer suit that raises issues of transcendental importance and provides the opportunity for this Honorable Court to affirm, once and for all, that the Bill of Rights and the freedoms protected by the Constitution apply with full force to acts and speech conducted in an online environment such as the Internet. The petition seeks to nullify certain parts of the Cybercrime Prevention Act of 2012. Independently, these provisions are Constitutionally infirm. Taken together, they restrict the fundamental rights to free speech and the freedom of the press with respect to online content in the same way a totalitarian state would do so – through unrestricted and unregulated censorship.

I.

NATURE OF PETITION

This is a Petition for CERTIORARI, and PROHIBITION under Rule 65 of the 1997 Rules of Civil Procedure to:

1. NULLIFY Sections 4(c)(4), 6, 7, 12 and 19 of Republic Act No. 10175 otherwise known as the “Cybercrime Prevention Act of 2012” (hereafter referred to as the “Cybercrime Act”) for violating the fundamental rights protected under the Constitution; and
2. PROHIBIT the Respondents, singly and collectively, from enforcing the afore-mentioned provisions of the Cybercrime Act.

II.

THE PARTIES

1. Petitioners are taxpayers. They may be served with summons and other processes of the Honorable Supreme Court through undersigned counsel.
2. The Respondent SECRETARY OF JUSTICE is a public officer tasked with the enforcement of the Cybercrime Act and whose office directs the prosecution of crimes through the National Prosecution Service. The SECRETARY OF JUSTICE may be served with summons at the Department of Justice, Padre Faura St., Ermita, Manila 1000.
3. The Respondent SECRETARY OF THE INTERIOR AND LOCAL GOVERNMENT is a public official tasked with the implementation of the Cybercrime Act. The Secretary may be served with summons at the A. Francisco Gold Condominium II, EDSA cor. Mapagmahal St., Diliman, Quezon City.
4. The Respondent EXECUTIVE DIRECTOR OF THE INFORMATION COMMUNICATIONS TECHNOLOGY OFFICE (ICTO) is a public official tasked with the implementation of the Cybercrime Act. The Executive Director may be served with summons at the NCC Building, C.P. Garcia Ave., Diliman, Quezon City.

5. The Respondent CHIEF OF THE PHILIPPINE NATIONAL POLICE (PNP) is the head of the PNP, named as a law enforcement authority authorized to engage in real-time collection of traffic data under the Cybercrime Act. The Respondent may be served with summons at the PNP National Headquarters, Camp General Crame, Quezon City, Metro Manila.

6. The Respondent DIRECTOR OF THE NATIONAL BUREAU OF INVESTIGATION (NBI) is the head of the NBI, named as a law enforcement authority authorized to engage in real-time collection of traffic data under the Cybercrime Act. The Respondent may be served with summons at the NBI Building, Taft Avenue, Ermita, Manila.

III.

AVERMENT AS TO JURISDICTION

7. Petitioners herein aver that Sections 4(c)(4), 6, 7, 12 and 19 of the Cybercrime Act collectively violate the Petitioners' Constitutionally-protected rights to freedom of expression, due process, equal protection, privacy of communications, as well as the Constitutional sanctions against double jeopardy, undue delegation of legislative authority and the right against unreasonable searches and seizure.

- a. Sections 6 and 7 of the Cybercrime Act more than doubles the liability for imprisonment for any violation of existing penal laws simply because the same was committed by, through and with the use of information and communications technologies (ICTs). These violate the Petitioners' right against Double Jeopardy. To the extent that a group of violators are identified as a class without justification, the afore-mentioned provisions also infringe the Petitioners' right to equal protection.
- b. Section 12 of the Cybercrime Act permits the NBI and the PNP "with due cause" to engage in real time collection of traffic data without the benefit of the intervention of a judge. This unwarranted authority to engage in wholesale surveillance of all cellular, data, mobile, Internet and computer communications violates the Petitioners' Constitutionally-protected right to be free from unreasonable searches and seizure as well as the right to the privacy of communications.
- c. Section 19 of the Cybercrime Act authorizes the Respondent Secretary of the Department of Justice (DOJ) to block or restrict access to any content upon a *prima facie* finding that the same violates the law. This provision contains an undue delegation of legislative authority, infringes upon the judicial power of the judiciary, and violates the Petitioners' Constitutionally-protected right to due process and freedom of expression.

d. Section 4(c)(4) of the Cybercrime Act defines libel as a cybercrime and in relation to Section 6 the law, increased the penalty from 6 months to 4 years and 2 months¹ to the greater period of 6 years to 10 years². Moreover under Section 12, a *prima facie* finding by the Secretary of the DOJ can trigger an order directed at service providers to block access to the said material without the benefit of a trial or a conviction. It should be stressed that in the Revised Penal Code, the courts have no authority to censor libelous materials even after conviction. In this regard, the Cybercrime Act therefore infringes upon the right to freedom of expression and also restricts the freedom of the press. The increased penalties, plus the ease by which allegedly libelous materials can be removed from access, work together as a “chilling effect” upon protected speech.

8. Petitioner further avers that there is no other plain, speedy, or adequate remedy in the course of law, and that this Petition is therefore cognizable by the Supreme Court’s judicial power under Article VIII, Sec. 1 par. 2 of the Constitution and pursuant to Rule 65, Sec. 1 of the 1997 Rules of Civil Procedure, as amended.

¹ Article 355 of the Revised Penal Code punishes Libel with *prision correccional* in its minimum and medium periods

² Sec. 6 of the Cybercrime Act imposes a penalty on libel committed using information and communication technologies, one degree higher or *prision mayor* in its minimum and medium periods.

IV.

ANTECEDENT FACTS

1. On September 12, 2012, the President of the Philippines approved Republic Act No. 10175, otherwise known as the “Cybercrime Prevention Act of 2012” (the “Cybercrime Act”).
2. Section 4(c)(4) of the Cybercrime Act defines libel as a cybercrime.

It provides:

“SEC. 4. *Cybercrime Offenses.* — The following acts constitute the offense of cybercrime punishable under this Act:

xxx	xxx	xxx
-----	-----	-----

(c) Content-related Offenses

xxx	xxx	xxx
-----	-----	-----

(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.”

3. In addition to the cybercrimes defined in Section 4 thereof, Section 6 of the Cybercrime Act refers to **all existing laws with penal provisions** and if violations thereof were committed by, through, and with the use of ICTs, higher penalties will be imposed, to wit:

“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” (emphasis and underscoring supplied).

4. Section 7 of the Cybercrime Act provides for the independent liability for violations of the Revised Penal Code or special laws and violations of the Cybercrime Act. It provides:

“SEC. 7. *Liability under Other Laws.* — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.”

5. Section 12 of the Cybercrime Act, in pertinent part, authorizes the PNP and the NBI to engage in real time surveillance of **all** traffic data in **all** telecommunications facilities **without the benefit of a search warrant**:

“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 not content, nor identities.”

6. Section 19 of the Cybercrime Act authorizes the Respondent DOJ Secretary to require service providers to restrict or block access to any content upon a *prima facie* showing that the same violates the Act:

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

V.

ARGUMENTS

A. *The Cybercrime Act Violates Free Speech*

1. On its face, the present Petition strikes down independent provisions of the Cybercrime Act as being violative of Constitutional freedoms, and collectively, these provisions inter-operate with each other to create a “chilling effect” upon the freedom of expression.
 - a. First, Section 4(c)(4) defines libel as a cybercrime, and pursuant to Section 6, the penalty for libel committed “by, through, and with the use” of information and communication technologies (ICTs) or “online libel” is punished *one degree higher* than the Revised Penal Code, that is, from the minimum and medium periods of *prision correccional* to the minimum and medium periods of *prision mayor*. The Cybercrime Act therefore imposes heavier penalties for online libel than paper-based libel.
 - b. Second, Section 7 provides that online libel will not only attract the penalties provided in the Cybercrime Act but also those imposed in the Revised Penal Code. In other words, a single act of online libel will result in two (2) convictions penalized separately under the Revised Penal Code and the Cybercrime Act.

2. Prior to the enactment of the Cybercrime Act, online libel would have

attracted a penalty from 6 months to 4 years 2 months³. With the new law, **in addition to a prosecution under the Revised Penal Code for libel, online libel will attract a penalty of 6 to 10 years⁴.**

3. Furthermore, since the accused can be prosecuted under both laws, a conviction under both will disqualify the accused from applying for probation. Note that even a singular prosecution for online libel under the Cybercrime Act will have the same effect since the penalty exceeds six (6) years.
4. In other words, online libel under the Cybercrime Act will ensure the imprisonment of the accused and for a much longer period. Surely, these changes will result in a chilling effect upon the freedom of speech.
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.
6. On August 22, 2012 and September 7, 2012, Petitioner Sonido posted 2 blogs entitled “Sotto Voce: Speaking with Emphasis”⁵ and “Sotto

³ These are the minimum and medium periods of *prision correccional*.

⁴ These are the minimum and medium periods of *prision mayor* which is one degree higher than *prision correccional*.

⁵ <http://baratillo.net/2012/08/sotto-voce-speaking-with-emphasis/>

and Lessons on Social Media”⁶ 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] RH Bill. Ganun ang strategy nun and **unfortunately, di pa napipirmahan 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.⁷

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 such 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.

⁶ <http://baratillo.net/2012/09/sotto-and-lessons-on-social-media/>

⁷ <http://rp1.abs-cbnnews.com/nation/08/30/12/sotto-warns-critics-beware-cybercrime-law>

10. With the passage of the Cybercrime Act, the threat that was issued by Senator Sotto against his online critics has become real.
11. Worse, the threat of criminal prosecution under the Cybercrime Act, whether warranted or not, will work to preclude people such as Petitioners from posting social commentaries online, thereby creating a “chilling effect” upon the freedom of expression.
12. But the attack on the freedom of expression and the press does not stop there. Section 19 of the Cybercrime Act authorizes the Respondent Secretary of the DOJ, upon a mere *prima facie* showing that a particular Internet article constitutes online libel, to issue an order directing Internet service providers (such as duly enfranchised telecommunications companies) to block or restrict access to such material.
- a. This provision constitutes the Respondent DOJ Secretary as an omnipotent censor and regulator of online content available in the Philippines.
 - b. What’s worse is that the blocking of access to online content can be achieved without any hearing of any kind, and without respect for the author’s freedom of expression.
 - c. The *prima facie* standard is so low that virtually any request forwarded to the Respondent DOJ Secretary may trigger the issuance of a “blocking” order.

- d. The blocking order itself can encompass all types of content whether local or international, since the Respondent DOJ Secretary can order Philippine Internet service providers to block access to entire sites on a wholesale basis.
- e. The blocking order is also permanent since the law does not prescribe an expiration period nor does the Cybercrime Act require the complaining party to initiate criminal proceedings to ensure that the accused is indeed guilty beyond reasonable doubt.
- f. It should be stressed that under the Revised Penal Code, real-world or offline libel cannot be censored by the courts *even after the conviction of the accused*. Under the Cybercrime Act, a mere *prima facie* showing entitles the complainant to these remedies. Effectively, the Respondent DOJ Secretary becomes the judge, jury and executioner – indeed, the final authority on all matters of online speech.
- g. Since the Cybercrime Act does not distinguish, the Respondent DOJ Secretary can restrain and block access to content whether authored by private citizens or the organized press.

13. It is undeniable that the Cybercrime Act in this context is a content-based regulation, that is, one that seeks to restrict speech that *at first blush* appears to violate the Cybercrime Act. Jurisprudence instructs that the law should be subject to strict scrutiny. This Honorable Court has had occasion to hold:

“(A) governmental action that restricts freedom of speech or of the press **based on content** is given the **strictest scrutiny** in light of its inherent and invasive impact. Only when the challenged act has overcome the **clear and present danger rule** will it pass constitutional muster, with the government having the burden of overcoming the presumed unconstitutionality.

Unless the government can overthrow this presumption, the **content-based** restraint will be struck down.

With respect to **content-based** restrictions, the government must also show the type of harm the speech sought to be restrained would bring about — especially the gravity and the imminence of the threatened harm — otherwise the prior restraint will be invalid. Prior restraint on speech based on its content cannot be justified by hypothetical fears, “but only by showing a substantive and imminent evil that has taken the life of a reality already on ground.” As formulated, “the question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent. It is a question of proximity and degree.”

The regulation which restricts the speech content must also serve an important or substantial government interest, which is unrelated to the suppression of free expression.

Also, the incidental restriction on speech must be no greater than what is essential to the furtherance of that interest. A restriction that is so broad that it encompasses more than what is required to satisfy the governmental interest will be invalidated. The regulation, therefore, must be reasonable and narrowly drawn to fit the regulatory purpose, with the least restrictive means undertaken.

Thus, when the prior restraint partakes of a **content-neutral regulation**, it is subjected to an intermediate review. A **content-based regulation**, however, bears a heavy presumption of invalidity and is measured against the **clear and present danger rule**. The latter will pass constitutional muster only if justified by a compelling reason, and the restrictions imposed are neither overbroad nor vague” (*Chavez v. Gonzales*, G.R. No. 168338, February 15, 2008).

14. Undeniably, therefore, it is the duty of the Respondents to demonstrate how the Cybercrime Act fares under strict scrutiny.

- a. The Petitioners submit that the *prima facie* standard in Section 19 of the Cybercrime Act is effectively a prior restraint since

the speech can be easily blocked or taken down. Moreover, the order of the Respondent DOJ Secretary becomes permanent. Hence, the Respondents have to demonstrate that such prior restraint is necessary because the speech creates a clear and present danger that will bring about substantive evils that Congress seeks to restrain.

- b. The Petitioners further submit that the absence of any limitation upon the Respondent DOJ Secretary's power in terms of time or the duty to pursue a criminal prosecution, demonstrates that the incursion into the Freedom of Expression is not narrowly tailored to satisfy a valid governmental interest nor is it the least restrictive means possible to pursue such interest.

15. Apart from collectively operating to infringe the freedom of expression and the press, Sections 6, 7, 12 and 19 of the Cybercrime Act independently violate relevant provisions of and fundamental rights protected by the Constitution.

B. Sections 6 and 7 of the Cybercrime Act violate the Double Jeopardy and Equal Protection Clauses of the Constitution.

7. *Double Jeopardy.* Section 6 of the Cybercrime Act defines all criminal offenses, whether punishable under the Revised Penal Code

or special laws, as cybercrimes for which a higher penalty will be imposed. Section 7 of the Cybercrime Act specifies that the penalty imposed in the Act shall be independent of the prosecution of the accused under the Revised Penal Code or special laws, as the case may be. These provisions state:

“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.

SEC. 7. *Liability under Other Laws.* — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.”

8. In effect, the same set of acts that constitute a violation of the Revised Penal Code or of a special law will attract an even greater penalty under the Cybercrime Act (if the law was violated “by, through, and with the use” of ICTs). Hence, persons who commit crimes using ICTs face the possibility of being imprisoned more than double the imprisonment laid down in the Revised Penal Code or special law, simply by the passage of the Cybercrime Act.

9. It is submitted that the above-quoted provisions violate Section 21, Article III of the Constitution which reads:

“Section 21. No person shall be twice put in jeopardy of punishment for the same offense. If an act is punished by a law and an ordinance, conviction or acquittal under either shall constitute a bar to another prosecution for the same act.”

10. In the context of simultaneous prosecutions under the Revised Penal Code and special laws, this Honorable Court has defended the imposition of double penalties upon the theory that the offenses are different. Hence,

“Although *Tac-an* and *Tiozon* relate more to the issue of whether there is a violation of the constitutional proscription against double jeopardy if an accused is prosecuted for homicide or murder and for aggravated illegal possession of firearm, they at the same time laid down the rule that these are separate offenses, with the first punished under the Revised Penal Code and the second under a special law; hence, the constitutional bar against double jeopardy will not apply. We observed in *Tac-an*:

It is elementary that the constitutional right against double jeopardy protects one against a second or later prosecution for the *same offense*, and that when the subsequent information charges another and different offense, although arising from the same act or set of acts, there is no prohibited double jeopardy. In the case at bar, it appears to us quite clear that the offense charged in Criminal Case No. 4007 is that of unlawful possession of an unlicensed firearm penalized under a special statute, while the offense charged in Criminal Case No. 4012 was that of murder punished under the Revised Penal Code. It would appear self-evident that these two (2) offenses in themselves are quite different one from the other, such that in principle, the subsequent filing of Criminal Case No. 4012 is not to be regarded as having placed appellant in a prohibited second jeopardy.

And we stressed that the use of the unlicensed firearm cannot serve to increase the penalty for homicide or murder; however, the killing of a person with the use of an unlicensed firearm, by express provision of P.D. No. 1866, shall increase the penalty for illegal possession of firearm.

In *Tiozon*, we stated:

It may be loosely said that homicide or murder qualifies the offense penalized in said Section 1 because it is a circumstance which increases the penalty. It does not, however, follow that the homicide or murder is absorbed in the offense; otherwise, an anomalous absurdity results whereby a more serious crime defined and penalized in the Revised Penal Code is absorbed by a statutory offense, which is just a *malum prohibitum*. The rationale for the qualification, as implied from the exordium of the decree, is to effectively deter violations of the laws on firearms and to stop the "upsurge of crimes vitally affecting public order

and safety due to the proliferation of illegally possessed and manufactured firearms, . . ." In fine then, the killing of a person with the use of an unlicensed firearm may give rise to separate prosecutions for (a) violation of Section 1 of P.D. No. 1866 and (b) violation of either Article 248 (Murder) or Article 249 (Homicide) of the Revised Penal Code. The accused cannot plead one as a bar to the other; or, stated otherwise, the rule against double jeopardy cannot be invoked because the first is punished by a special law while the second, homicide or murder, is punished by the Revised Penal Code.

In *People vs. Doriguez* [24 SCRA 163, 171], We held:

It is a cardinal rule that the protection against double jeopardy may be invoked only for the same offense or identical offenses. A simple act may offend against two (or more entirely distinct and unrelated provisions of law, and if one provision requires proof of an additional fact or element which the other does not, an acquittal or conviction or a dismissal of the information under one does not bar prosecution under the other. Phrased otherwise, where two different laws (or articles of the same code) defines two crimes, prior jeopardy as to one of them is not obstacle to a prosecution of the other, although both offenses arise from the same fact, if each crime involves some important act which is not an essential element of the other.

In *People vs. Bacolod* [89 Phil. 621], from the act of firing a shot from a sub-machine gun which caused public panic among the people present and physical injuries to one, informations of physical injuries through reckless imprudence and for serious public disturbance were filed. Accused pleaded guilty and was convicted in the first and he sought to dismiss the second on the ground of double jeopardy. We ruled:

The protection against double jeopardy is only for the same offense. A simple act may be an offense against two different provisions of law and if one provision requires proof of an additional fact which the other does not, an acquittal or conviction under one does not bar prosecution under the other.

Since the informations were for separate offense[s] — the first against a person and the second against public peace and order — one cannot be pleaded as a bar to the other under the rule on double jeopardy" (*People v. Quijada*, G.R. Nos. 11508-09, July 24, 1996).

11. The same doctrine was echoed by this Honorable Court in the case of the dual prosecution for violations of Batas Pambansa Blg. 22 and

Estafa. In *People v. Reyes* (G.R. Nos. 101127-31, November 18, 1993), this Honorable Court held:

“We re-affirm at the outset the established doctrine that:

While the filing of the two sets of Information under the provisions of Batas Pambansa Bilang 22 and under the provisions of the Revised Penal Code, as amended, on estafa, may refer to identical acts committed by petitioner, the prosecution thereof cannot be limited to one offense, because a single criminal act may give rise to a multiplicity of offenses and where there is variance or differences between the elements of an offense in one law and another law as in the case at bar there will be no double jeopardy because what the rule on double jeopardy prohibits refers to identity of elements in the two (2) offenses. Otherwise stated, prosecution for the same act is not prohibited. What is forbidden is prosecution for the same offense. Hence, the mere filing of the two (2) sets of information does not itself give rise to double jeopardy (*People v. Miraflores*, 115 SCRA 570).

The gravamen of the offense punished by BP 22 is the act of making and issuing a worthless check or a check that is dishonored upon its presentment for payment. The law has made the mere act of issuing a bad check a *malum prohibitum*, an act proscribed by the legislature for being deemed pernicious and inimical to public welfare.

According to Chief Justice Pedro L. Yap in the landmark case of *Lozano v. Martinez*:

The effects of the issuance of a worthless check transcends the private interests of the parties directly involved in the transaction and touches the interest of the community at large. The mischief it creates is not only a wrong to the payee or holder, but also an injury to the public. The harmful practice of putting valueless commercial papers in circulation, multiplied a thousandfold, can very well pollute the channels of trade and commerce, injure the banking system and eventually hurt the welfare of society and the public interest.”

12. In the case of the Cybercrime Act however, the cybercrimes defined and punished under Section 6 of the Act **are absolutely identical** to the crimes defined in the Revised Penal Code and special laws. Indeed, the acts are identical and the essential elements of both offenses are also identical, except that the penalty under the

Cybercrime Act is one degree higher. Therefore, this raises the possibility that an accused will be punished twice for the same offense in violation of the Constitution.

13. *Equal Protection*. Section 1, Article III of the Constitution provides as follows:

“Section 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws.”

14. The Equal Protection Clause simply requires that all persons similarly situated must be treated in the same manner by the law. While Congress is permitted to classify persons, the Equal Protection Clause demands that the classification be reasonable. In *Biraogo v. The Philippine Truth Commission of 2010* (G.R. No. 192985, December 7, 2010), this Honorable Court explained the rules governing valid classifications:

“An early case, *People v. Cayat*, articulated the requisites determinative of valid and reasonable classification under the equal protection clause, and stated that it must

- (1) rest on substantial distinctions;
- (2) be germane to the purpose of the law;
- (3) not be limited to existing conditions only; and
- (4) apply equally to all members of the same class.”

15. Moreover, in that case, this Honorable Court held that when a classification interferes with the exercise of a fundamental right, the strict scrutiny standard must be used. Hence:

“The most exacting of the three tests is evidently the *strict scrutiny test*, which requires the government to show that the challenged classification serves a *compelling state interest* and that the classification is necessary to serve that interest. Briefly stated, the strict scrutiny test is applied when the challenged statute either:

(1) classifies on the basis of an inherently suspect characteristic; or

(2) **infringes fundamental constitutional rights.**

In these situations, the usual presumption of constitutionality is reversed, and **it falls upon the government to demonstrate that its classification has been narrowly tailored to further compelling governmental interests**; otherwise, the law shall be declared unconstitutional for violating the equal protection clause.”

16. Applying the above doctrines to the case at bar, it is immediately clear that through Sections 6 and 7 of the Cybercrime Act, Congress created a class of offenders who commit crimes “by, through or with the use” of ICTs. Because the Cybercrime Act is a penal statute, the fundamental right to liberty is necessarily implicated. Hence, it behooves the Respondents to demonstrate that the classification has been narrowly tailored to further compelling governmental interests. Failing that, then the Cybercrime Act violates the Equal Protection Clause and is Constitutionally infirm.

C. The Real Time Collection of Traffic Data Violates the Right to Privacy and the Right Against Unreasonable Searches and Seizure

17. Section 12 of the Cybercrime Act permits the NBI and PNP to collect traffic data without a warrant. It 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 not content, nor identities.

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

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

18. Real time collection of traffic data under the Cybercrime Act authorizes the PNP and the NBI to install devices at the networks of telecommunications, mobile and Internet service providers to capture data about communications. It is conceivable that the PNP or NBI can monitor *all traffic* since the law does not establish standards for the exercise of the authority to collect data.

- a. For mobile phone communications, the traffic data collected will include the originating cell phone number, the destination number, the date and time of the communication and the duration of the communication. This can include voice calls, SMS or text including mobile data usage.
- b. While the law does not permit the PNP and NBI to secure subscriber data from the service providers without a warrant,

such information is available through other means. In other words, if the PNP and NBI were to discover a particular person's cellphone number (through such person's friends or business associates), the NBI and PNP can use this information to search through the collected "real time traffic data" to know all the details of such person's communications - that is, voice calls, SMS/text, and mobile Internet/data usage (except the content thereof).

- c. From there, it is possible for the NBI and PNP to learn other information about the subject such as the phone numbers and identities of the persons who communicate with the subject.
- d. This amounts to nothing less than surveillance without a warrant.

19. Sections 2 and 3, Article III of the Constitution provides:

"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.

Section 3.

1. The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.

2. Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding."

20. In *Ople v. Torres* (G.R. No. 127685, July 23, 1998), this Honorable Court recognized privacy as a fundamental right and held that State action that impinges upon the right to privacy must be “justified by some compelling state interest and that it is narrowly drawn.”

21. In the case of the Cybercrime Act, there is no compelling state interest that justifies real time collection of data. Neither does the statute narrowly draw the authority granted to the PNP and the NBI. Indeed, the authority vested to collect data is not bounded by any reasonable standard except “due cause” which presumably, the PNP and NBI will determine for itself.

22. It should be noted that in the Human Security Act, the privacy of suspected terrorists are protected by the intervention of the Court of Appeals before surveillance operations are conducted⁸. In the Cybercrime Act, the privacy of *all citizens* may be infringed without judicial participation.

23. Moreover, neither the NBI nor the PNP is required to justify the incursion into the right to privacy. These law enforcement authorities are not required to show that the collection of traffic data is necessary to a pending criminal investigation. They are not required to report their findings or use the same in any criminal prosecution.

⁸ See Secs. 7-11, Republic Act No. 9327.

24. Finally, no limits are imposed upon either the PNP or the NBI since they can lawfully collect traffic data *at all times without interruption.*

It is conceivable that the PNP and the NBI can at **all times** possess **all** traffic data on **all** Internet, mobile, fixed line and related communications.

25. There is no stated justification for this warrant-free unlimited incursion into the privacy of citizens.

D. The Respondent DOJ Secretary's Take Down Authority under Section 19 of the Cybercrime Act violates Due Process and is an Undue Delegation of Legislative Authority.

26. Section 19 of the Cybercrime Act authorizes the Respondent DOJ Secretary to order the restriction or blocking of access to certain content, in this wise:

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

27. This power authorizes the Respondent DOJ Secretary to compel the take down of any Internet or on-line content upon a mere *prima facie* finding without any need for a judicial determination. As demonstrated earlier, a party complaining of libel needs to show only a *prima facie* case and the libelous content will be blocked from

access – a remedy not otherwise available to victims of real-world libel even after a judicial conviction of the accused.

28. The Cybercrime Act therefore contemplates that the Respondent DOJ Secretary will be “judge, jury and executioner” of all cybercrime-related complaints. Note that nowhere in the law is the authority of the Respondent DOJ Secretary limited by time or burdened with the requirement that such blocking order be followed up with a criminal prosecution.

29. When one considers that all penal provisions in all special laws are cybercrimes under Section 6, it follows that:

- a. Complaints filed by intellectual property rights owners may be acted upon by the Respondent DOJ Secretary to block access to websites and content upon a mere *prima facie* showing of an infringement; or
- b. Foreign sites like Amazon.com, offering goods on retail to Philippine citizens may be blocked for violating the Retail Trade Law; or
- c. Foreign service providers such as Skype may be blocked from offering voice services without securing a license from the National Telecommunications Commission; or
- d. YouTube videos may be blocked for presumably violating the IP Code.

30. The takedown authority of the Respondent DOJ Secretary is indeed overwhelming since it can be used to shape the way all Filipinos experience the Internet in the same manner the Chinese government established the “Great Firewall of China.”

31. These overwhelming powers have been granted with a very low hurdle – a *prima facie* showing of a violation of law, and the Respondent DOJ Secretary is not required to hear or give due course to the targets of the request for the takedown order – in clear violation of their Constitutionally protected right to due process.

32. *Undue Delegation*. The legislature is permitted to delegate its authority to the executive but the same must set the standards for the exercise of the delegated authority.

33. In *Abakada Guro Party List v. Purisima*, G.R. No. 166715, August 14, 2008, this Honorable Court described these standards as follows:

“Two tests determine the validity of delegation of legislative power: (1) the completeness test and (2) the sufficient standard test. A law is complete when it **sets forth therein the policy to be executed, carried out or implemented** by the delegate. It lays down a **sufficient standard** when it provides adequate guidelines or limitations in the law to map out the boundaries of the delegate's authority and **prevent the delegation from running riot**. To be sufficient, the standard must specify the **limits of the delegate's authority, announce the legislative policy and identify the conditions under which it is to be implemented**” (emphasis supplied).

34. The Petitioners submit that Section 12 of the Cybercrime Act fails both tests.

a. First, nowhere in the Cybercrime Act's declaration of policy does it lay down the legislative policy with respect to the blocking of content. Section 2 of the Cybercrime Act provides, in part, that:

"In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation."

Nowhere in the above-quoted portion, or indeed, the entirety of Section 2, does the legislature provide the policy that justifies the resort to extrajudicial remedies, such as the takedown power. Worse, the Respondent DOJ Secretary is enjoined to "detect, investigate and prosecute" cybercrimes within the judicial system.

b. Second, there are no limits upon the takedown power of the Respondent DOJ Secretary. Once the order is issued, it does not expire. The Respondent DOJ Secretary is not even required to take any further action on the complaint or require the complaining party to litigate the matter before the regular courts. As demonstrated above, the *prima facie* standard is not enough to prevent the Respondent DOJ Secretary from exercising infinite discretion and becoming the supreme authority in the Philippine Internet landscape.

**GROUND FOR THE ISSUANCE OF A
TEMPORARY RESTRAINING ORDER**

35. As explained above, the Respondents will implement Sections 4(c)(4), 6, 7, 12 and 19 of the Cybercrime Act in clear violation of the Constitution and of various fundamental rights protected therein.

36. Pending action by this Honorable Court upon this Petition, the Petitioners are entitled to have the Respondents enjoined from implementing the afore-mentioned provisions of the Cybercrime Act.

37. Unless the implementation of these unconstitutional provisions is enjoined, the Petitioners stand to suffer irreparable injury that cannot be estimated.

PRAYER

WHEREFORE, in light of all the foregoing, the Petitioners respectfully pray that judgment be rendered by this Court:

- a. Declaring null and void, for being unconstitutional, Sections 4(c)(4), 6, 7, 12 and 19 of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012;
- b. Prohibiting all Respondents from implementing Sections 4(c)(4), 6, 7, 12 and 19 of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012; and

- c. Pending resolution of this case, issuing a Temporary Restraining Order enjoining the Respondents from implementing Sections 4(c)(4), 6, 7, 12 and 19 of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012.

Other reliefs, just and equitable in the premises, are likewise prayed for.

Quezon City for the City of Manila, September 24, 2012.

DISINI & DISINI LAW OFFICE

Counsel for Petitioners

320 Philippine Social Science Center
Commonwealth Avenue
Diliman, Quezon City 1100
Metro Manila

Phone: (+632)426-0486

Fax: (+632)454-5442 ext. 102

Email:docket@disini.ph

By:



JOSE JESUS M. DISINI, JR.

Roll of Attorneys No. 38949

PTR No. 6117995/1.13.12/QC

IBP No. 879967/1.06.12/QC

MCLE Compliance No. III-0008990



ROWENA S. DISINI

Roll of Attorneys No. 39342

PTR No. 6117994/1.13.12/QC

IBP Lifetime No. 01331/QC

MCLE Compliance No. III-0008989



LIANNE IVY PASCUA-MEDINA

Roll of Attorneys No. 52047

PTR No. 3199312/1.17.12/QC

IBP No. 879966/1.06.12/QC

MCLE Compliance No. IV-0002372

Copy Furnished:

Hon. Leila M. De Lima
Secretary
Department of Justice
Padre Faura Street, Ermita
City of Manila

Hon. Manuel A. Roxas II
Secretary
Department of the Interior and Local Government
A. Francisco Gold Condominium II
EDSA corner Mapagmahal Street
Diliman, Quezon City

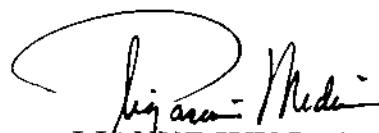
Hon. Louis C. Casambre
Executive Director
Information and Communications Technology Office
NCC Building, C.P. Garcia Avenue
Diliman, Quezon City

Dir. Gen. Nicanor Bartolome
Chief
Philippine National Police
PNP National Headquarters
Camp General Crame, Quezon City

Dir. Nonnatus Caesar R. Rojas
Director
National Bureau of Investigation
NBI Building, Taft Avenue
Ermita, Manila.

EXPLANATION FOR SERVICE BY REGISTERED MAIL

The undersigned counsel was constrained to serve copies of the foregoing PETITION upon the parties by registered mail as evidenced by the attached Affidavit of Service, due to time constraints, and considering further, the lack of available manpower to effect service by personal delivery.



LIANNE IVY PASCUA-MEDINA

VERIFICATION AND CERTIFICATION OF NON-FORUM SHOPPING

We, **JOSE JESUS M. DISINI, JR., ROWENA S. DISINI, LIANNE IVY P.MEDINA, JANETTE TORAL and ERNESTO SONIDO, JR.**, of legal age, Filipinos, after having been duly sworn in accordance with law, hereby depose and state that:

1. We are the petitioners in the instant case entitled, "*Jose Jesus M. Disini, Jr., et al. vs. The Secretary of Justice, et al.*" that was filed before this Honorable Court.

2. We caused the preparation of the foregoing *Petition for Certiorari and Prohibition with Prayer for a Temporary Restraining Order*.

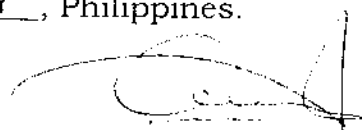
3. We have read the said pleading and hereby aver that the allegations therein are true and correct of our personal knowledge or based on authentic records.


4. We have not commenced any other action or filed any claim involving the same issues in any court, tribunal or quasi-judicial agency and, to the best of our knowledge, no such other action or claim is pending therein.

5. If we should hereafter learn that the same or similar action or claim has been filed or is pending before the Supreme Court, Court of Appeals, or any other tribunal or agency, we shall report such fact within five (5) days therefrom to this Honorable Court.

IN WITNESS WHEREOF, we have hereunto set our hand this 24th day of September 2012 in QUEZON CITY, Philippines.


JOSE JESUS M. DISINI, JR.
Affiant


ROWENA S. DISINI
Affiant


LIANNE IVY P. MEDINA
Affiant



JANETTE TORAL
Affiant


ERNESTO SONIDO, JR
Affiant

SUBSCRIBED AND SWORN to before me this SEP 24 2012 day of September 2012 at QUEZON CITY, affiants exhibiting to me the following competent proofs of their identification:

Name	Identification Card	Issued on/Valid until
Jose Jesus M. Disini, Jr.	Driver's License No. N01-85-009543	Valid Until April 27, 2015
Rowena S. Disini	Postal I.D. No. 2313583	Valid until July 13, 2015
Lianne Ivy P. Medina	Postal I.D. No. 23135335	Valid until July 4, 2015
Janette Toral	Passport No. XX0428328	Issued on January 26, 2008
Ernesto Sonido, Jr.	Passport No. CC4839286	Issued on October 26, 2009

Doc. No. 16 ;
Page No. 4 ;
Book No. I ;
Series of 2012.


EMERSON S. BAÑEZ
Notary Public for Quezon City
Adm. Matter No. NI-112, until Dec. 31, 2012
Rol. No. 36723
IBP No. 888800, 02-09-12 - Makati City
PTE No. 695069, 02-09-12 - Quezon City
320 PSSC Bldg., Commonwealth Avenue
Delmonte, Quezon City

AFFIDAVIT OF SERVICE

I, **MA. VICTORIA B. CLEMENTE**, of legal age, Filipino, with postal address at Room 320 Philippine Social Science Center, Commonwealth Avenue, Diliman, Quezon City, after having been duly sworn to in accordance with law, depose and say:

On September 25, 2012, I served copies of the following pleading/paper:

PETITION FOR CERTIORARI AND PROHIBITION
WITH PRAYER FOR A TEMPORARY RESTRAINING ORDER

in **G.R. No. _____** entitled "**Jose Jesus M. Disini, Jr. et al. vs. The Secretary of Justice et al.**" pursuant to Rule 13 of the 1997 Rules of Civil Procedure, as follows:

By Registered Mail To:

Hon. Leila M. De Lima
Secretary
Department of Justice
Padre Faura Street, Ermita
City of Manila

Registry Receipt No. 4777
U.P. Diliman, Quezon City Post Office
September 25, 2012

Hon. Manuel A. Roxas II
Secretary
Department of the Interior and Local Government
A. Francisco Gold Condominium II
EDSA corner Mapagmahal Street
Diliman, Quezon City

Registry Receipt No. 4776
U.P. Diliman, Quezon City Post Office
September 25, 2012

Hon. Louis C. Casambre
Executive Director
Information and Communications Technology Office
NCC Building, C.P. Garcia Avenue
Diliman, Quezon City

Registry Receipt No. 4774
U.P. Diliman, Quezon City Post Office
September 25, 2012

Dir. Gen. Nicanor Bartolome
Chief
Philippine National Police
PNP National Headquarters
Camp General Crame, Quezon City

Registry Receipt No. 4778
U.P. Diliman, Quezon City Post Office
September 25, 2012

Dir. Nonnatus Caesar R. Rojas
Director
National Bureau of Investigation
NBI Building, Taft Avenue
Ermita, Manila


Registry Receipt No. 4775
U.P. Diliman, Quezon City Post Office
September 25, 2012

Quezon City, Metro Manila, September 25, 2012.


MA. VICTORIA B. CLEMENTE
Affiant

SUBSCRIBED AND SWORN to before me this 25th day of September 2012, at Quezon City, affiant exhibiting to me her SSS card bearing numbers 33-0059723-6.

Doc. No. 17 ;
Page No. 4 ;
Book No. I ;
Series of 2012.


EMERSON S. BANEZ
Notary Public for Quezon City
Adm. Matter No. NP-368 until Dec. 31, 2012
Rul. No. 9473
[BP] No. 888-000002-0012 / Makati City
[TE] No. 37600-000002-0012 / Quezon City
320 P.S.S.C. Bldg., Commonwealth Avenue
Diliman, Quezon City