

**Republic of the Philippines  
Supreme Court  
Manila**

En Banc

**NATIONAL UNION OF JOURNALISTS  
OF THE PHILIPPINES (NUJP),  
PHILIPPINE PRESS INSTITUTE (PPI),  
CENTER FOR MEDIA FREEDOM AND  
RESPONSIBILITY, ROWENA  
CARRANZA PARAAN, MELINDA  
QUINTOS-DE JESUS, JOSEPH ALWYN  
ALBURO, ARIEL SEBELLINO AND THE  
PETITIONERS IN THE e-PETITION  
<http://www.nujp.org/no-to-ra10175/>  
*Petitioners,***

- versus -

G.R. No. \_\_\_\_\_

**THE EXECUTIVE SECRETARY, THE  
SECRETARY OF JUSTICE, THE  
SECRETARY OF THE INTERIOR AND  
LOCAL GOVERNMENT, THE  
SECRETARY OF BUDGET AND  
MANAGEMENT, THE DIRECTOR  
GENERAL OF THE PHILIPPINE  
NATIONAL POLICE, THE DIRECTOR  
OF THE NATIONAL BUREAU OF  
INVESTIGATION, THE CYBERCRIME  
INVESTIGATION AND  
COORDINATING CENTER, AND ALL  
AGENCIES AND INSTRUMENTALITIES  
OF GOVERNMENT AND ALL  
PERSONS ACTING UNDER THEIR  
INSTRUCTIONS, ORDERS,  
DIRECTION IN RELATION TO THE  
IMPLEMENTATION OF REPUBLIC ACT  
NO. 10175,**

For: Certiorari,  
Prohibition and  
Injunction with  
Application for  
Immediate Restraining  
Order and Other  
Extraordinary Legal and  
Equitable Reliefs

*Respondents.*

X -----X

**P E T I T I O N <sup>1</sup>**

PETITIONERS, by counsel, respectfully state that:

**I. PRELIMINARY STATEMENT**

<sup>1</sup> This is filed also as an e-Petition, which is incorporated by reference into this conventional Petition, is accessible at <http://www.nujp.org/no-to-ra10175/>.

“From our sadness, we awakened to a shaft of light cutting through the darkness...”<sup>2</sup>

In this case of first impression, this Court is asked to rule on a statute that, if allowed to stand, will set back decades of struggle against the darkness of “constitutional dictatorship” and replace it with “cyber authoritarianism”. It is fitting that the words of the President’s own platform be the backdrop against which the looming darkness is to be dispelled.

Petitioners ask this Court to rule on Republic Act No. 10175, a law that establishes a regime of “cyber authoritarianism” and undermines all the fundamental guarantees of freedoms and liberties that many have given their lives and many still give their lives work to vindicate, restore and defend. It is a law that unduly restricts the rights and freedoms of netizens<sup>3</sup> and impacts adversely on an entire generation’s way of living, studying, understanding and relating.

It is no exaggeration to point out that the rapid growth of technology has created a specific way of thinking, relating and living. Social media and the internet has allowed people to draw closer to each other even while retaining personal privacy, that remains deeply valued. Online resources have allowed progressive notions of transparency and accountability; revolutions, such as the Arab Spring, were started on the wings of technology when bloggers took to cyberspace and “broadcast” what was happening--in real time. In a growing consensus, the United Nations Human Rights Council has passed a non-binding resolution to “continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies, as well as of how the Internet can be an important tool for development and for exercising human rights, in accordance with its programme of work”<sup>4</sup>—a huge step towards recognizing access to the internet as a basic human right.

---

<sup>2</sup> From “A Social Contract With The Filipino People”, Benigno S. Aquino III, Platform of Government; accessible at <http://www.gov.ph/about/gov/exec/bsaiii/platform-of-government>; last accessed October 1, 2012, 2:30 AM.

<sup>3</sup> A netizen is defined as an active participant in the online community of the Internet. See Merriam-Webster Online Dictionary; accessible at <http://www.merriam-webster.com/dictionary/netizen>; last accessed on September 29, 2012, 8:30 PM. The Urban Dictionary defines it as “a variant on citizen. A person who interacts with others on the internet. In effect, anyone who uses the internet becomes a netizen.” See Urban Dictionary, accessible at <http://www.urbandictionary.com/define.php?term=netizen>; last accessed on September 30, 2012, 11:26 PM.

<sup>4</sup> <http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf>; last accessed October 1, 2012, 2:45 PM.

Republic Act No. 10175 threatens this entire way of thinking, of relating, of doing business and of expressing oneself with its repressive perspective on personal freedoms and regressive view of technology. Far from complying with the State policy in Article II, section 24 of the 1987 Constitution that “recognizes the vital role of communication and information” and advancing the use of technology to expand the space for creative, imaginative, and progressive use of information and communications technology (ICT), the law demonizes technology, views cynically the space for democratic expression using social media and establishes an authoritarian regime within the space that was, until the passage of Republic Act No. 10175, the freest and most democratic. The law, if allowed to stand, will usher in yet another darkness.

For these and the other reasons set forth below, this Court must shine a light through this darkness. For these and other reasons set forth below, the law must fall.

## **A. Nature of the Action**

1.1. This is a petition for Certiorari,<sup>5</sup> Prohibition<sup>6</sup> and Injunction<sup>7</sup> with an application for urgent relief by way of an Immediate<sup>8</sup> Restraining Order (IRO) filed with this Court to annul and/or restrain the implementation of specific portions of Republic Act No. 10175 for being unconstitutional. The specific provisions are the following:

- a. Sec. 4(c)(4) (*Libel*);
- b. Sec. 5(a) (*Aiding or Abetting in the Commission of Cybercrime*);
- c. Sec. 6 (inclusion of all felonies and crimes within coverage of the law);
- d. Sec. 7 (*Liability under Other Laws*);
- e. Sec. 12 (*Real-Time Collection of Traffic Data*);
- f. Secs. 14 (*Disclosure of Computer Data*), 15 (*Search, Seizure and Examination of Computer Data*), 19 (*Restricting or Blocking Access to Computer Data*), and 20 (*Non-Compliance*), where these provisions unlawfully delegate to police officers the authority to issue orders properly within the scope and sphere of judicial powers and where non-compliance is penalized as a crime;
- g. Sec. 24 (*Cybercrime Investigation and Coordinating Center*) and 26(a) (*Powers and Functions*), where both sections 24 and 26(a) give the Cybercrime Investigation and Coordinating Center the power to formulate a national cybersecurity plan, which should properly fall within the power of Congress and not an administrative agency;

1.2. Apart from the specific grounds for unconstitutionality of these sections, sec. 28 of Republic Act No. 10175 is also sought to be restrained as it delegates to respondents SOJ and SILG the authority to promulgate Implementing Rules and Regulations within ninety days from approval of the law without clear and definite standards to guide the respondents in crafting such rules and regulations. Such a delegation, if allowed to stand, will be an unlawful delegation of legislative powers and result in arbitrariness.

1.3. Despite section 29 (*Separability Clause*), petitioners submit that with these provisions of the law being declared unconstitutional, the entire law is

<sup>5</sup> Rule 65, sec. 1, Rules of Court.

<sup>6</sup> Rule 65, sec. 2, Rules of Court.

<sup>7</sup> Rule 57, Rules of Court.

<sup>8</sup> Because any restraining order issued by the Court is effective until lifted, the true characterization of any restraining order, as distinguished from an injunction, is "immediate" as opposed to "temporary."

rendered without meaning and not capable of implementation. For that reason, the entire law must be struck down.

1.4. In view of the number of sections challenged as unconstitutional and the possibility of the entire law being declared unconstitutional, section 27 (*Appropriations*) is also sought to be restrained as the release of the public money appropriated under the law would result in wastage if these provisions are ultimately annulled or the implementation restrained.

1.5. This petition is filed, partly as an electronic document, because some of the petitioners are based outside of Metro Manila, with others based outside the Philippines. Considering that the law has become effective as of October 3, 2012, the nature of the reliefs prayed for are urgent and, thus, cannot await the physical presence of the petitioners for purposes of signing the petition. The nature of electronic filing has allowed the petitioners to the e-Petition access to this Court.

1.6. The e-Petition contains partial statement of parties and their respective statement of legal standing<sup>9</sup> as well as the statement of material antecedents, statement of reasons warranting reliefs and the statement of reliefs prayed for are contained in the signed e-Petition, which forms an integral part of this Petition. The e-Petition is accessible at <http://www.nujp.org/no-to-ra10175> and is incorporated by reference into this Petition.

## **B. Averments Supporting Jurisdiction**

1.7. Under Article VIII, sec. 1, par. 2 of the 1987 Constitution, this Court has both the power and the duty to inquire into the attendance of grave abuse of discretion on the part of any branch or instrumentality of government. There is no question of power, authority and duty to review the Cybercrime law.

1.8. The law was signed by the President on September 12, 2012. Petitioners have sixty (60) days within which to seek nullification and/or restraint under Rule 65, secs. 1 and 2. This Petition is thus timely filed.

1.9. The pernicious sweep of the Cybercrime law—penalizing all felonies and crimes with double the original penalties had they been committed in the conventional fashion and not using an Information and Communication

---

<sup>9</sup> It is partial only because some of the petitioners are identified in this conventional Petition (as opposed to e-Petition); for purposes of ensuring a determinable number of petitioners, the signing of the e-Petition was closed as of October 3, 2012, 8:00 in the morning, Philippine time. As of that date and time, the number of petitioners signing in the e-Petition totaled \_\_\_\_.

Technology (ICT) device under sections 4(c)(4), (5(a), and (6); the removal of the protection afforded by the double jeopardy clause under sec. (7) and the real time collection of traffic data under sec. 12—pose a clear and present threat to petitioners' freedom of expression and leave them with no clear, adequate and effective remedy in law.

1.10. For these reasons, there is basis for this Court to pass upon the constitutionality of Republic Act No. 10175 or the Cybercrime Law.

## II. THE PARTIES

### 2.1. Petitioners --

2.1.1. **National Union of Journalists of the Philippines (NUJP)** is a lateral guild committed to securing the interests of the Filipino working press. It binds journalists to a covenant to ethical conduct and commitment to the public trust and seeks to promote and safeguard the economic interest and social well-being of the working press, upgrade professional skills, raise the standards of journalistic ethics, carry out welfare program for its members, and foster fraternal solidarity with all journalists everywhere. The union stands on three legs: unity, integrity and dignity for the working press.

2.1.2. **Philippine Press Institute (PPI)** The Philippine Press Institute (PPI) is a non-stock, non-profit private organization duly registered with the Securities and Exchange Commission whose principal mandate is to defend press freedom and promote ethical standards for the professional development of the Filipino journalist. Also known as the national association of newspapers, it represents the interests and concerns of the newspaper sector in media and in all forums. Its membership includes the major national and provincial daily/weekly newspapers in the country. The institute conducts training programs and organizes educational activities for Filipino journalists, seeks to protect their rights and freedoms in the pursuit of their practice, creates and introduces opportunities for the development of the journalist as a practitioner.

2.1.3. **Center for Media Freedom and Responsibility (CMFR)** media advocacy group organized in 1989 by journalists and media practitioners for the purpose of defending and enhancing press freedom and free expression through the responsible and ethical practice of journalism. It publishes PJR Reports, which monitors media

performance and advocates responsible reporting and comment, as well as several other publications of circulated in the Philippines and other Asian countries. It maintains a website and a blog, In Medias Res, through which its executive officers comment on media developments. It stands to suffer direct and immediate injury by reason of the operation of RA 10175.

2.1.4. **Melinda Quintos-De Jesus** is a taxpayer, a citizen, a journalist. She is the Executive Director of the Center for Media Freedom and Responsibility (CMFR). She is also a netizen, contributing to a three-person blog, "In Media Res", which can be accessed at <http://www.cmfr-phil.org/inmediasres>.

2.1.5. **Rowena Carranza Paraan** is a citizen, a taxpayer and a journalist. She is the Secretary General of the NUJP. For purposes of legal standing, she is a taxpayer, a citizen of the Philippines and also a netizen who stands to suffer direct and immediate injury by reason of the operation of Republic Act No. 10175.

2.1.6. **Ariel Sebellino** is a citizen and a taxpayer; he is also the Executive Director of the Philippine Press Institute.

2.1.7. **Alwyn Alburo** is a citizen and a taxpayer and is a program manager at GMA Network Inc. He is vice chair of the National Union of Journalists of the Philippines (NUJP).

2.1.8. Co-petitioners are those who have signed the e-Petition (collectively "e-Petitioners"), accessible at <http://www.nujp.org/no-to-ra10175>, the contents of which are incorporated by reference into this Petition.

All petitioners, including e-Petitioners, may be served with pertinent notices of this Court through counsel at the contact details provided below.

## 2.2. Respondents –

2.2.1. **Executive Secretary** is the cabinet secretary in charge of the Office of the President ("OP"), which has general power of supervision over all agencies and instrumentalities of the executive branch of government. The OP is the office to which the respondent Cybercrime Investigation and Coordinating Center (CICC) is attached. Respondent OP may be served with official notices and pertinent processes through the Executive Secretary at his official station at Malacanang Palace, Manila.

2.2.2. **Secretary of Justice** is tasked with enforcement of Republic Act No. 10175; he is the public officer who has supervision and

control over the National Prosecution Service and, in that capacity, has authority over the conduct of the criminal prosecutions mandated under the pertinent challenged section of the statute. Under Republic Act No. 10175, respondent SOJ is vested with sweeping powers and broad authority including the power to restrict or block access to computer data under section 19. Respondent SOJ may be served with official notices and pertinent processes at her official station at the Department of Justice, Padre Faura Street, Ermita, The City of Manila.

2.2.3. **Secretary of the Interior and Local Government** is tasked with enforcing Republic Act No. 10175; he is vested with the power and authority to formulate implementing rules and regulations to effectively implement Republic Act No. 10175, together with co-respondent Secretary of Justice; he is also the public official tasked with supervision and control of the Philippine National Police (PNP). Respondent SILG may be served with official notices and pertinent processes at his official station at the Department of the Interior and Local Government at A. Francisco Gold Condominium II, EDSA corner Mapagmahal Street, Quezon City.

2.2.4. **Secretary of Budget and Management** is tasked with funding and disbursing the amount of Fifty Million Pesos (P50,000,000.00) allocated by Republic Act No. 10175 for the implementation of the statute. Respondent SBM may be served with official notices and pertinent processes at his official station at the Department of Budget and Management at the Malacanang Palace Compound, Manila.

2.2.5. **Director General, Philippine National Police (PNP)** is tasked with enforcing Republic Act No. 10175, particularly section 12 thereof on the real time collection of traffic data. He may be served with official notices and pertinent processes at his official station at the Philippine National Police Headquarters, Camp Crame, Quezon City.

2.2.6. **Director, National Bureau of Investigation (NBI)** is tasked with enforcing Republic Act No. 10175, particularly section 12 thereof on the real time collection of traffic data. He may be served with official notices and pertinent processes at his official station at the National Bureau of Investigation Headquarters, Taft Avenue, The City of Manila.

2.2.7. **Cybercrime Investigation And Coordinating Center, through the Executive Director of the Information** is tasked with



enforcing Republic Act No. 10175, particularly the formulation of the national cybersecurity plan under sec. 26(a). Respondent CICC may be served with official notices and pertinent processes at its official station at the NCC Building, C.P. Garcia Avenue, UP Diliman Campus, Quezon City.

For purposes of this Petition, all other agencies, instrumentalities and persons acting under the instructions, directives and orders of respondents in relation to the enforcement and implementation of Republic Act No. 10175 are also impleaded.

### III. MATERIAL ANTECEDENTS

3.1. On September 12, 2012, Republic Act No. 10175 entitled “An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and The Imposition of Penalties Therefor and For Other Purposes” or the “Cybercrime Prevention Act of 2012” (“Cybercrime Law”) was signed into law by the President of the Philippines.

3.2. Pursuant to section 31, the Cybercrime Law was published in two (2) newspapers of general circulation<sup>10</sup> and took effect fifteen (15) days thereafter, or on October 3, 2012.

3.3. Pertinent to this Petition, the following provisions are now effective, **even in the absence of any implementing rules and regulations:**

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

x x x

(c) Content-related Offenses:

x x x

(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.

SEC. 5. *Other Offenses.* — The following acts shall also constitute an offense:

<sup>10</sup> It must be noted that the full text of the Cybercrime Law was uploaded to the online Official Gazette (accessible at <http://www.gov.ph/2012/09/12/republic-act-no-10175>; last accessed September 30, 2012, 10:35 PM) on September 12, 2012, the same day it was signed. However, pursuant to *Tanada v. Tuvera*, G.R. No. L-63915 April 24, 1985, and Executive Order No. 200 (s. 1986), the effectivity date was reckoned from publication in two newspapers of general circulation and not the online Official Gazette.

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

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.

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.

3.4. The effectivity of the Cybercrime Law also makes the creation of the Cybercrime Investigation and Coordinating Center (CICC) within thirty (30) days an imminent reality; in turn, the national cybersecurity plan that the CICC is mandated to formulate and enforce will follow as a matter of course.

#### **IV. REASONS WARRANTING RELIEFS**

**- A -**

**SECTIONS 4(c)(4), 5(a), 6, AND 7 VIOLATE FREEDOM OF EXPRESSION.**

**- B -**

**SECTION 4(c)(4), 5(a), AND 6, WHICH CRIMINALIZE THE USE OF “INFORMATION AND COMMUNICATIONS TECHNOLOGIES” (ICT), RENDER REPUBLIC ACT NO. 10175 A BILL OF ATTAINDER; FURTHER, SEC. 20, WHICH MAKES NON-COMPLIANCE WITH ORDERS OF LAW ENFORCEMENT AUTHORITIES PUNISHABLE CRIMINALLY ALSO RENDERS THE LAW A BILL OF ATTAINDER.**

**- C -**

**SECTION 7 VIOLATES THE CONSTITUTIONAL GUARANTEE OF PROTECTION AGAINST DOUBLE JEOPARDY.**

**- D -**

**SECTIONS 6, 7 AND 19 VIOLATE DUE PROCESS AND EQUAL PROTECTION.**

**- E -**

**SECTIONS 14, 15, 19, 24 AND 26(a) VIOLATE SEPARATION OF POWERS AS JUDICIAL POWERS ARE UNDULY DELEGATED TO THE SECRETARY OF JUSTICE, THE PNP AND THE NBI.**

**- F -**

**SECTION 12 VIOLATES THE RIGHT OF PRIVACY OF COMMUNICATION AND CORRESPONDENCE AS IT ALLOWS THE REAL-TIME COLLECTION OF TRAFFIC DATA AND EFFECTIVELY SURVEILLANCE WITHOUT A WARRANT.**

**- G -**

**THE CYBERCRIME LAW IS EFFECTIVE EVEN WITHOUT THE IMPLEMENTING RULES AND REGULATIONS; UNLESS THE IMPLEMENTATION OF THE LAW IS RESTRAINED, PETITIONERS STAND TO SUFFER GRAVE AND IRREPARABLE INJURY WITH NO SPEEDY OR ADEQUATE REMEDY AT LAW.**

## **V. ARGUMENT**

### **A. SECTIONS 4(c)(4), 5(a), 6, AND 7 VIOLATE FREEDOM OF EXPRESSION.**

1. That the transposed felony of libel in the Cybercrime Law falls under the heading “(c) Content-related Offenses” is immediately instructive, as to its nature and the Court’s way forward. By punishing libel as a cybercrime simply because it is “committed through a computer system”, the clear intent of section 4(c)(4) is to single out netizens in their chosen medium of expression. It is clearly a prior restraint that infringes on the freedom of expression guaranteed under Article III, section 4 of the 1987 Constitution.

2. Freedom of expression has long enjoyed the distinction of being a preferred right and thus, “a weighty presumption of invalidity vitiates measures of prior restraint upon the exercise of such freedoms.” (*Ayer Productions v. Hon. Capulong and Juan Ponce Enrile*, G.R. No. 82380, April 29, 1988) The burden lies on the State to justify the prior restraint that section 4(c)(4) works on the freedoms of speech and expression. “(W)hen the prior restraint partakes of ...(a) content-based regulation, ...(it) bears a heavy presumption of invalidity and is measured against the clear and present danger rule...(where) (t)he 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; editorial modifications supplied)

3. Respondents bear the burden and the duty of justification in this regard. No favorable presumption—of validity of the law nor regularity of official action—may be indulged in favor of the law. As it stands, by its mere characterization in the law itself as a “(c)ontent-related (offense)”, section 4(c)(4) is facially void. Petitioners, thus, respectfully reserve their right to comment on or rebut any putative justification that the State may offer in this regard.

4. Section 5(a) punishes “(a)ny person who willfully abets or aids in the commission of any of the offenses enumerated in this Act.” Read together with section 4(c)(4), section 5(a) clearly constitutes a prior restraint on free expression. In the first place, section 5(a) fails to define exactly what acts are punished within the scope of the words “abets or aids” and, **in the distinct context of social media and online journalism**, operates as a chilling factor that undermines, restricts and abridges freedom of expression. The criminalization of the yet-undefined acts that fall under “abets or aids” under section 5(a) causes any person using a computer and the internet to consider if the mere act of “forwarding”, “sharing”, “liking”, “re-tweeting” would constitute an act that “abets or aids” the content-related offense of cyber libel under section 4(c)(4).

5. Section 6 incorporates by reference, jot for jot, “all crimes defined and penalized by the Revised Penal Code...and special laws” and makes all of these punishable as cybercrimes “if committed by through, and with the use of information and communications technologies” and imposes a penalty one degree higher than that provided for by the Revised Penal Code and special laws, as the case may be. This section undermines outright any constitutional protection afforded to freedom of expression. Section 6 must be read in relation to section 2 of the Cybercrime Law which sets forth the legislative policy that the law seeks to advance. The relevant portion of section 2 provides that:

SEC. 2. *Declaration of Policy.* -- xxx The State also recognizes the importance of **providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or**

**conducts.** 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.<sup>11</sup>

The policy declaration in section 2 shows that the wholesale importation of **ALL** felonies and crimes as cybercrimes in section 6 is unjustified. Clearly, there must be a rational basis for converting specific crimes, previously punished when committed by conventional rather than through ICT means, into cybercrimes; this, especially, becomes vital when section 6 creates a new qualifying circumstance that is not governed by Article 14 of the Revised Penal Code—that of “use of information and communications technologies.” There is, however, no rational basis for concluding that the “use of information and communications technologies” in relation to **all** felonies and crimes would constitute a circumstance so perverse as to convert an existing felony or a crime into a separate offense altogether. The absence of any rational basis for section 6, especially when read in relation to section 2, renders it an act of prior restraint especially in relation to the “use of information and communications technologies” and clearly in violation of freedom of expression.

6. Section 7 allows a separate prosecution for cybercrime notwithstanding any prosecution for the same act punished under the Revised Penal Code or special penal laws. Under the rationale that section 6 specifies for the wholesale incorporation of all felonies and crimes, it is the “use of information and communications technologies” that is key. The distinct nature of information and communications technologies is such that these would constitute means of expression; section 3 of the law concedes as much when it defines “(c)ommunication” as referring “to the transmission of information through ICT media, including voice, video and other forms of data.” The tie between ICT and freedom of expression cannot thus be easily severed and any provision of law that would impose a burden on the use of ICT must be viewed as a prior restraint. The prospect of being punished twice for one act that might be considered a felony or a crime but also a cybercrime simply because one chooses to use an ICT device is sufficient to create a chill on freedom of expression and thus undermine and abridge the constitutional protection afforded.

7. Section 19 gives respondent Secretary of Justice the power to restrict or block access to computer data simply on the basis of a *prima facie* finding

---

<sup>11</sup> Emphasis supplied.

that the computer data is in violation of the Cybercrime Law. Read together with section 4(c)(4), respondent Secretary of Justice may, on the basis of a *prima facie* finding, order the “take down” of supposedly libelous computer data—without benefit of a judicial determination or even a formal charge. Moreover, because the law provides for no standards for the exercise of this power, any order may be unlimited in scope, duration and character and would clearly infringe on the right to free expression.

**B. SECTIONS 4(c)(4), 5(a), AND 6, WHICH CRIMINALIZE USE OF “INFORMATION AND COMMUNICATIONS TECHNOLOGIES” (ICT), RENDER REPUBLIC ACT NO. 10175 A BILL OF ATTAINDER; FURTHER, SEC. 20, WHICH MAKES NON COMPLIANCE WITH ORDERS OF LAW ENFORCEMENT AUTHORITIES PUNISHABLE CRIMINALLY ALSO RENDERS THE LAW A BILL OF ATTAINDER.**

8. The Constitution prohibits a bill of attainder in Article III, sec. 22. A bill of attainder is a legislative act that inflicts punishment without trial. “The singling out of a definite class, the imposition of a burden on it, and a legislative intent, suffice to stigmatize a statute as a bill of attainder.” (*People of the Philippines v. Ferrer*, G.R. Nos. L-32613-4, April 30, 1974; Teehankee, *j.*, dissenting)

9. One thing is common to sections 4(c)(4), 5, 6 and 7—the legislative determination that the use of ICT in the performance of an act that has already been characterized as a felony or crime, when committed by conventional means, makes the act a much graver crime—seen by the imposition of a new penalty that is one (1) degree higher than that provided for the felony or crime committed by conventional means.<sup>12</sup>

10. Manifestly, a class is singled out—those who use ICT or are inhabitants of online communities, i.e., netizens. This is clear in section 6.

11. The use of ICT as the measure by which the penalty is doubled cannot be offset by any mitigating circumstance as the same is not provided in Article 14 of the Revised Penal Code. The practical effect is to render the use of ICT as an indefeasible special circumstance that not only converts a conventional offense into a cybercrime but also increases the penalty by a hundred percent.

---

<sup>12</sup> Rep. Act No. 10175, sec. 6.

12. Section 6 also fails to require *mens rea* when it considers the use of ICT as a special qualifying circumstance. Thus, the mere use—even if innocent—of ICT would suffice to make the offense a cybercrime. It, thus, unduly increases the burden on one who uses ICT and it does so in such a way as to cover even incidental or innocent use. Section 6 taints all the penal provisions of Republic Act No. 10175—sections 4, 5, and 7—and suffices to render Republic Act No. 10175 a bill of attainder.

13. Further, section 20, where it provides for punishment for non-compliance with the orders issued by the law enforcement authorities with a term of imprisonment and/or a fine for each and every non-compliance, is clearly a provision that singles out a specific class of offenders for punishment based on a legislative determination of guilt.

### **C. SECTION 7 VIOLATES THE CONSTITUTIONAL GUARANTEE OF PROTECTION AGAINST DOUBLE JEOPARDY.**

14. Article III, sec. 21 of the Constitution expressly guarantees the protection of the double jeopardy clause by commanding that “(n)o person shall be twice put in jeopardy of punishment for the same offense.” Rule 117, section 7 of the Rules on Criminal Procedure provide that double jeopardy would bar subsequent prosecutions “for the offense charged, or for any attempt to commit the same or a frustration thereof, or for any offense which necessarily includes or is necessarily included in the offense charged in the former complaint or information.” It is the identity of offenses that determines the operation of the prohibition against double jeopardy; thus, one of the exceptions under Rule 117, section 7 provides for the viability of a subsequent prosecution only if it is based on a different offense, i.e., “the graver offense developed due to supervening facts arising from the same act or omission constituting the former charge.”

15. Section 7, read in relation to section 6, however proceeds on the premise that the offenses punished by the Revised Penal Code and special penal laws which are incorporated into the Cybercrime Law as cybercrimes are identical, jot for jot. For this reason, there is no justification for exceptional treatment and the constitutional guarantee against double jeopardy ought to apply. In providing for a prosecution for cybercrime “without prejudice to any

liability for any violation” of the Revised Penal Code or special laws, sections 7 and 6 violate the prohibition against double jeopardy.

**D. SECTIONS 6, 7 AND 19 VIOLATE DUE PROCESS AND EQUAL PROTECTION.**

16. Article III, section 1 of the 1987 Constitution guarantees that “(n)o 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.**” This command is simple and straightforward: treat all persons similarly situated similarly.

17. While Congress is not precluded from coming up with a classification, any classification must be reasonable and must, when it involves the exercise of a fundamental right or freedom, survive strict scrutiny.

18. Sections 6 and 7 create a class of persons who: (a) are considered to have committed criminal acts simply because they use ICT and are punished with a penalty double that of the same felony or crime committed without use of ICT, and (b) are not entitled to invoke the constitutional guarantee of double jeopardy.

19. Immediately, it may be seen that Article III, section 1 is directly implicated by sections 6 and 7. Not only is the classification suspect, dependent as it is simply on the use of ICT, such that the law violates equal protection but it also imposes a penalty twice that for the same felony or crime committed without use of ICT where the qualifying circumstance is infeasible, in violation of the fundamental right to not be deprived of liberty without due process.

20. The guarantee of due process is incompatible with a situation where the mere use of ICT under section 6—regardless of malice or *mens rea*—is considered as an infeasible circumstance that would ensure the imposition of a penalty twice that for the same felony or crime committed through more conventional means, i.e., without use of ICT. In the same manner that there should be no irrevocable laws, there should also be no infeasible circumstances. Contending otherwise would make due process—that notion of a sporting chance to be heard and to have one’s side considered—a cruel joke.

21. Additionally, the blanket increase of penalties across the board by one degree for all felonies and crimes under section 6, regardless of the



nature of the felony or crime and regardless of their relation to the public policy set forth in section 2, discriminates against those who use ICT. That the mere use of ICT would constitute an infeasible circumstance in what may be considered a cybercrime unduly burdens that class of persons who use ICT, as a matter of preference or as a matter of necessity.

22. The “take down” clause under Section 19, on the other hand, violates due process as well as equal protection. Not only does it allow the Secretary of Justice to seize property without due process in direct violation of Article III, section 1, it also allows an executive determination of what should be a judicial finding and, then, on an extremely low standard. Effectively, the Secretary of Justice is a one-person tribunal, anathema to the constitutional guarantee of due process and every notion of fundamental fairness.

23. Finally, the “take down” clause under Section 19 violates equal protection because it treats persons who should be similarly situated differently. The incorporation of all felonies and crimes under section 6 provides for a situation where the “take down” power of the Secretary of Justice could result in a determination that a cybercrime exists on a lower quantum of evidence—*prima facie*—than it would if it were not a cybercrime. Section 19 also gives respondent Secretary of Justice the power to “take down” based simply on a *prima facie* finding and without benefit of a warrant.

**E. SECTIONS 14, 15, 19, 24 AND 26(a) VIOLATE SEPARATION OF POWERS AS JUDICIAL AND LEGISLATIVE POWERS ARE UNDULY DELEGATED TO THE SECRETARY OF JUSTICE, THE PNP AND THE NBI.**

24. Congress, in enacting the Cybercrime Law, delegates substantial power to respondents Secretary of Justice, PNP and NBI. The delegation is, however, unconstitutional as Congress has delegated powers that it itself does not possess.

25. Respondent Secretary of Justice is delegated the power to **restrict or block access to computer data** under section 19 on the basis simply of a *prima facie* finding. The power to “restrict or block access to computer data” amounts to a seizure of property which is reserved to a judge under Article III, section 2; notably, it is also a power that can only be exercised after the issuance of a warrant.

26. Respondents PNP and NBI, collectively referred to as “law enforcement authorities”, are delegated judicial powers under section 14 to issue “order(s) requiring any person or service provider to disclose or submit subscriber’s information, traffic data or relevant data in his/its possession or control within seventy two (72) hours from receipt of the order in relation to a valid complaint.” Notably, such an order would partake of the nature of a subpoena, which is a judicial process.

27. Respondent CICC is given the power to formulate and implement the national cybersecurity plan under section 24. Notably, there are no parameters nor standards to guide respondent CICC in formulating the same. Such a delegation is unconstitutional as it amounts to an abdication of the legislative power to formulate policy in favor of an administrative agency which would only be mandated to enforce any such policy.

**F. SECTION 12 VIOLATES THE RIGHT OF PRIVACY OF COMMUNICATION AND CORRESPONDENCE AS IT ALLOWS THE REAL-TIME COLLECTION OF TRAFFIC DATA AND EFFECTIVELY SURVEILLANCE WITHOUT A WARRANT.**

28. Section 12 of the law authorizes respondents PNP and NBI, collectively referred to as “law enforcement authorities” 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” without a warrant or any other judicial order, and certainly without probable cause as the law only provides for the nebulous standard of “due cause.” By “traffic data” is meant “the communication’s origin, destination, route, time, date, size, duration, or type of underlying service, but not content nor identities.”

29. This directly violates Article III, section 3 of the 1987 Constitution which guarantees that “(t)he 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.” That Congress recognized the need for a warrant in situations covered by the right to privacy is made manifest by the third paragraph of section 19, which expressly provides that “(a)ll other data to be collected or seized or disclosed will require a court warrant.” That the real-time traffic data to be seized under section 12 is not

justified by requirements of public safety or order is also made manifest by section 19 which does not justify the seizure on these grounds but only on the nebulous standard of “due cause.”

30. Patently, section 12 of the Cybercrime Law impermissibly intrudes into the privacy of communication and correspondence without any justification. This Court has already previously ruled that privacy is a fundamental right and any intrusion by State action may only be “justified by some compelling state interest” that is narrowly drawn. (*Ople v. Torres*, G.R. No. 127685, July 23, 1998). The Cybercrime Law fails to provide for any indication that there is a compelling state interest in the real time collection of data.

31. The grant of power to law enforcement authorities under section 12 is also excessive and capricious. No parameters or boundaries are set, no durations prescribed nor standards given. It is a roving license given to PNP and NBI to intrude into a fundamental right that the Constitution guarantees and protects. Section 12 cannot stand.

**G. THE CYBERCRIME LAW IS EFFECTIVE EVEN WITHOUT THE IMPLEMENTING RULES AND REGULATIONS; UNLESS THE IMPLEMENTATION OF THE LAW IS RESTRAINED, PETITIONERS STAND TO SUFFER GRAVE AND IRREPARABLE INJURY WITH NO SPEEDY OR ADEQUATE REMEDY AT LAW.**

32. The law has taken effect and, despite the absence of implementing rules and regulations, will already bring about consequences.

33. Unless immediately restrained, petitioners stand to suffer irreparably and irretrievably. For this reason, an Immediate Restraining Order must be issued by this Court enjoining: (a) respondents from implementing the law in its entirety, (b) respondent Secretary of Budget and Management from releasing the allocated funds, and (c) respondents Secretary of Justice, PNP and NBI from implementing the provisions of section 12 and section 19, in relation to sections 4(c)(4), 5, 6, 7 and 20.

**VI. RELIEFS**

WHEREFORE, premises considered, petitioners respectfully pray that, immediately upon receipt of this Petition (together with the integrated e-

Petition), an Immediate Restraining Order be issued directing respondents from implementing Republic Act No. 10175 or the Cybercrime Prevention Act of 2012. Further, it is also prayed that an Immediate Restraining Order be issued directing respondent Secretary of the Department of Budget and Management not to release the amount of Fifty Million Pesos (P50,000,000.00) until such time that the Court orders otherwise.

Petitioners thereafter pray that, upon submission of the respective comment from respondents, that this Petition (with the corresponding e-Petition integrated by reference into this Petition) be given due course and that judgment be rendered, thus:

- 1) Declaring Republic Act No. 10175 in its entirety null and void, for being unconstitutional; or
  - a. In the alternative, declaring sections 4(c)(4), 5, 6, 7, 12, 19, 21, 24 and 26(a) null and void, for being unconstitutional;
- 2) Prohibiting all respondents and those who act under their instructions, orders and/or directives from implementing Republic Act No. 10175 in its entirety, to include the formulation of Implementing Rules and Regulations under section 28; or
  - a. In the alternative, prohibiting all respondents and those who act under their instructions, orders and/or directives from implementing sections 4(c)(4), 5, 6, 7, 12, 19, 21, 24 and 26(a) and all provisions in Republic Act No. 10175 that are inherently related to these sections;

Petitioners also pray for all other just and equitable *interim* or permanent reliefs, as may be warranted including, but not limited to, scheduling this case for oral argument before the Court to allow the parties to more fully articulate their respective positions before the Court.

Quezon City for The City of Manila; October 3, 2012.

**FREE LEGAL ASSISTANCE GROUP  
(FLAG)**

Counsel for all Petitioners  
Room 201, Malcolm Hall, University of the Philippines  
Diliman, Quezon City

**JOSE MANUEL I. DIOKNO  
PABLITO V. SANIDAD**

**RICARDO A. SUNGA III**  
**THEODORE O. TE**

BY:

**THEODORE O. TE**  
PTR No. 4610200, 1/7/11, QC  
IBP No.848002, 1/10/11, Makati  
MCLE Exemption III-000942  
Tel. No. 9205514, local 405; Mobile: 09175202295  
Email: [theodore.te@gmail.com](mailto:theodore.te@gmail.com)

**VERIFICATION & CERTIFICATION AGAINST FORUM SHOPPING**

I, ROWENA CARRANZA PARAAN, of legal age, Filipino citizen and Netizen, do hereby state under oath that: they are among the petitioners who have caused this Petition (and the accompanying e-Petition, incorporated by reference within this petition) to be prepared; they have read and understood all the allegations in the Petition/e-Petition; they affirm that all the factual averments are true and correct, to the best of their own personal knowledge and based on authentic records at hand; they certify that they have not commenced any action against the same persons involving the same issues pleaded in this Petition/e-Petition before any court or tribunal or agency and that no such other action is pending; should any such other action come to their knowledge, they undertake to inform this Court of said fact within five (5) days from their actual knowledge thereof.

TO THE TRUTH OF THE FOREGOING, she has signed this Verification and Certification this \_\_ day of October 2012.

**ROWENA CARRANZA PARAAN**  
PASSPORT # EB4178446  
Issued on November 29, 2011  
at Manila, Philippines

SUBSCRIBED AND SWORN TO before me this \_\_ day of October 2012, affiant having presented to me competent proof of identity as indicated above.

Doc. No.  
Page No.  
Book No.  
Series of 2012.

**VERIFICATION & CERTIFICATION AGAINST FORUM SHOPPING**

I, MELINDA QUINTOS-DE JESUS, of legal age, Filipino citizen and Netizen, do hereby state under oath that: they are among the petitioners who have caused this Petition (and the accompanying e-Petition, incorporated by reference within this petition) to be prepared; they have read and understood all the allegations in the Petition/e-Petition; they affirm that all the factual averments are true and correct, to the best of their own personal knowledge and based on authentic records at hand; they certify that they have not commenced any action against the same persons involving the same issues pleaded in this Petition/e-Petition before any court or tribunal or agency and that no such other action is pending; should any such other action come to their knowledge, they undertake to inform this Court of said fact within five (5) days from their actual knowledge thereof.

TO THE TRUTH OF THE FOREGOING, she has signed this Verification and Certification this \_\_ day of October 2012.

**MELINDA QUINTOS-DE JESUS**

PASSPORT # EB1406502

Issued on/at Nov. 18, 2010, Manila,  
Philippines

SUBSCRIBED AND  
SWORN TO before  
me this \_\_ day of  
October 2012,  
affiant having  
presented to me  
competent proof of identity as indicated above.

Doc. No.  
Page No.  
Book No.  
Series of 2012.

**VERIFICATION & CERTIFICATION AGAINST FORUM SHOPPING**

I, JOSEPH ALWIN T. ALBURO, of legal age, Filipino citizen and Netizen, do hereby state under oath that: they are among the petitioners who have caused this Petition (and the accompanying e-Petition, incorporated by reference within this petition) to be prepared; they have read and understood all the allegations in the Petition/e-Petition; they affirm that all the factual averments are true and correct, to the best of their own personal knowledge and based on authentic records at hand; they certify that they have not commenced any action against the same persons involving the same issues pleaded in this Petition/e-Petition before any court or tribunal or agency and that no such other action is pending; should any such other action come to their knowledge, they undertake to inform this Court of said fact within five (5) days from their actual knowledge thereof.

TO THE TRUTH OF THE FOREGOING, he has signed this Verification and Certification this \_\_ day of October 2012.

**JOSEPH ALWIN T. ALBURO**

SSS # 03-9228398-8

Issued on/at Quezon City

SUBSCRIBED AND SWORN TO before me this \_\_ day of October 2012, affiant having presented to me competent proof of identity as indicated above.

Doc. No.  
Page No.  
Book No.  
Series of 2012.



**VERIFICATION & CERTIFICATION AGAINST FORUM SHOPPING**

I, ARIEL SEBELLINO, of legal age, Filipino citizen and Netizen, do hereby state under oath that: they are among the petitioners who have caused this Petition (and the accompanying e-Petition, incorporated by reference within this petition) to be prepared; they have read and understood all the allegations in the Petition/e-Petition; they affirm that all the factual averments are true and correct, to the best of their own personal knowledge and based on authentic records at hand; they certify that they have not commenced any action against the same persons involving the same issues pleaded in this Petition/e-Petition before any court or tribunal or agency and that no such other action is pending; should any such other action come to their knowledge, they undertake to inform this Court of said fact within five (5) days from their actual knowledge thereof.

TO THE TRUTH OF THE FOREGOING, he has signed this Verification and Certification this \_\_ day of October 2012.

**ARIEL SEBELLINO**  
TIN # 172-948-819  
Issued on/at Dec. 22, 1994, Davao City

SUBSCRIBED AND SWORN TO before me this \_\_ day of October 2012, affiants having presented to me competent proof of identity as indicated above.

Doc. No.  
Page No.  
Book No.  
Series of 2012.

Copy furnished:

**THE EXECUTIVE SECRETARY**  
Malacanang Palace, Manila

**THE SECRETARY OF JUSTICE**  
Department of Justice  
Padre Faura Street, Ermita, Manila

**THE SECRETARY OF THE INTERIOR**

**AND LOCAL GOVERNMENT**

Department of the Interior and Local Government  
A. Francisco Gold Condominium II  
EDSA corner Mapagmahal Street  
Quezon City

**THE DIRECTOR GENERAL  
PHILIPPINE NATIONAL POLICE**

Headquarters, Philippine National Police  
Camp Crame, Quezon City

**THE DIRECTOR, NATIONAL BUREAU  
OF INVESTIGATION**

Headquarters, National Bureau of Investigation  
Taft Avenue, Manila

**THE CYBERCRIME INVESTIGATION  
AND COORDINATING CENTER**

c/o The Executive Director,  
Information and Communications Technology Office  
NCC Building, C.P. Garcia Avenue  
Diliman, Quezon City

**THE SOLICITOR GENERAL**

134 Amorsolo Street, Legaspi Village  
Makati City

**EXPLANATION FOR SERVICE BY REGISTERED MAIL**

This Petition was served on the respondents by registered mail because of time, personnel and geographical concerns and constraints; the distance involved as well as lack of manpower to cause service by personal delivery constrained counsel to cause service by registered mail.

**THEODORE O. TE**

**AFFIDAVIT OF SERVICE**

I, (Name), of legal age, do hereby state under oath that: On (date), I served copies of the Petition in "National Union of Journalists of the Philippines, Philippine press Institute, Center for Media Freedom and Responsibility, Rowena Carranza Paraan, Melinda Quintos-De Jesus, Joseph Alwyn Alburo, Ariel Sebellino, et al. v. The Executive Secretary, et al." by registered mail on the following, as shown by the respective registry receipt details:

**THE EXECUTIVE SECRETARY**

Malacanang Palace, Manila

REG. RECEIPT NO.

POST OFFICE:

Date:

**THE SECRETARY OF JUSTICE**

Department of Justice  
Padre Faura Street, Ermita, Manila

REG. RECEIPT NO.

POST OFFICE:

Date:

**THE SECRETARY OF THE INTERIOR  
AND LOCAL GOVERNMENT**

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

REG. RECEIPT NO.

POST OFFICE:

Date:

**THE DIRECTOR GENERAL  
PHILIPPINE NATIONAL POLICE**

Headquarters, Philippine National Police  
Camp Crame, Quezon City

REG. RECEIPT NO.

POST OFFICE:

Date:

**THE DIRECTOR, NATIONAL BUREAU  
OF INVESTIGATION**

Headquarters, National Bureau of Investigation, Taft  
Avenue, Manila

REG. RECEIPT NO.

POST OFFICE:

Date:

**THE CYBERCRIME INVESTIGATION  
AND COORDINATING CENTER**

c/o The Executive Director, Information and  
Communications Technology Office, NCC Building, C.P.  
Garcia Avenue, Diliman, Quezon City

REG. RECEIPT NO.

POST OFFICE:

Date:

**THE SOLICITOR GENERAL**

134 Amorsolo Street, Legaspi Village  
Makati City

REG. RECEIPT NO.

POST OFFICE:

Date:

Quezon City, \_\_ October 2012.

\_\_\_\_\_  
TIN #

Issued on/at

SUBSCRIBED AND SWORN TO before me this \_\_ day of October 2012, affiant having presented to me competent proof of identity as indicated above.

Doc. No.

Page No.

Book No.

Series of 2012.