406 Amberland Place
Jade Drive, Ortigas Center
Pasig City 1605
Philippines

Comments on the Draft Implementing Rules and Regulations* of the Cybercrime Prevention Act of 2012 (RA 10175)

Democracy.Net.PH presents the following comments and recommendations on the draft Implementing Rules and Regulations (IRR) of the Cybercrime Prevention Act.

1. Cyberbullying

Republic Act No. 10627, or the Anti-Bullying Act of 2013†, already has Implementing Rules and Regulations on the prohibited act of "cyberbullying," as well as defined administrative penalties for the commission of the prohibited act. As such, Democracy.Net.PH recommends that:

- Sections 3 (d) and 4 on cyberbullying should be deleted.
- Any reference in the IRR to criminal prosecution of any modes of cyberbullying not provided by RA 10627 must refer to the Revised Penal Code or a special criminal law enacted for this purpose, and not to the Anti-Bullying Act.

2. Use of Hash Values

The duties of a service provider under Republic Act No. 9775, or the Anti-Child Pornography Act of 2009, in relation to in child pornography cases is clear: "All ISPs shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered."

The draft IRR for the Cybercrime Prevention Act proposes that "An Internet Service Provider (ISP)/ Internet Content Host shall install available technology, program or software such as but not limited to system/ technology that produces hash value or any similar calculation, to ensure that access to or transmittal of any form of child pornography will be blocked or filtered."

The draft IRR itself proposes a definition of hash value as a "digital fingerprint" or "digital DNA" for information.

The provisions of RA 9775 provide specifically and only for blocking or filtering of child pornography data, and not the attachment of identification to digital data, systems, or infrastructure, which may constitute unreasonable and warrantless search. We propose the deletion of the hash value definition (Section 3(s) of the draft IRR) and the entire phrase "such

* Dated 28 March 2014.

† Republic Act No. 10627, "An Act Requiring All Elementary and Secondary Schools to Adopt Policies to Prevent and Address the Acts of Bullying in Their Institutions" (Anti-Bullying Act of 2013) http://www.gov.ph/2013/09/12/republic-act-no-10627/

406 Amberland Place
Jade Drive, Ortigas Center
Pasig City 1605
Philippines

as but not limited to system/ technology that produces hash value or any similar calculation" from the Rule 8 provision.

3. Definition of Service Provider

The draft IRR for the Cybercrime Prevention Act proposes an extremely broad definition of "Service Provider." The definition ensures that restaurants, churches, places of business, places of assembly government offices with waiting areas, and other similar facilities providing free or paid Wi-Fi connectivity to its employees, customers, and guests are classed as service providers. This definition is so unreasonably broad that it will be difficult for law enforcement officers to distinguish between what is and is not s service provider that may be subject to prosecution under the IRR.

4. Definition of the National Cybersecurity Plan

We propose that in the sentence, "[I]t is a top-down approach to cybersecurity that contains broad policy statements and establishes a set of national objectives and priorities that should be achieved in a specific timeframe," the reference to a "top-down approach to cybersecurity" be deleted. This would, in effect, prevent even local government units from contributing to the National Cybersecurity Plan.

5. Definition of Original Author

"Original Author" under Section 3 is defined as, "Original author refers to the person who created or is the origin of the assailed electronic statement or post using the computer system." We propose that the phrase "origin of the assailed electronic statement" be deleted as this may contemplate a situation where the person who originally made the statement but not via the Internet or with the use of ICT may be subject to prosecution as well for online libel. More importantly, RA 101075 did not provide that the offense of online libel shall include an origin of the assailed electronic statement.

6. Period Covered by Order to Disclose Computer Data

Section 14 states that after the issuance of a warrant, the law enforcement authority may issue an order to any person/service provider, requiring the disclosure/submission of subscriber information, traffic data, and other relevant information. The section should specifically state that the information to be covered by this disclosure/submission shall be information gathered after the issuance of the warrant. Otherwise, it would be tantamount to data collection without a warrant, which is a violation of the right against unreasonable searches and seizures.