

Available online at www.sciencedirect.com
www.compseconline.com/publications/prodclaw.htm

**Computer Law
&
Security Review**



A slippery and inconsistent slope: How Cambodia's draft cybercrime law exposed the dangerous drift away from international human rights standards

Felicity Gerry QC ^{a,*}, Catherine Moore ^{b,**}

^a School of Law, Charles Darwin University, Darwin, Australia

^b Center for International and Comparative Law, University of Baltimore School of Law, Baltimore, USA

A B S T R A C T

Keywords:

Cybercrime
Cambodia
International human rights
Freedom of speech
Privacy rights
Internet

In the late 70's, a Group of Experts on Transborder Data Barriers and Privacy Protection was set up within the OECD. This expert group developed guidelines on basic rules governing the transborder flow and the protection of personal data and privacy. The purpose was to "facilitate a harmonization of national legislations, without this precluding at a later date the establishment of an international Convention." The Guidelines are described as "minimum standards for adoption in domestic legislation . . . and . . . capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level." Decades on, there remains no internationally accepted set of principles, leaving states with piecemeal legislation.²

The draft Cybercrime Law for Cambodia is just the latest in this long line of laws that attempt to resolve this issue. This Article will demonstrate, however, that the draft Cybercrime Law for Cambodia exposed a dangerous drift away from international human rights standards regarding protection of speech and right to privacy on the Internet. We will also propose possible redrafting of the Cambodian law, to bring it in line with their international human rights obligations and provide for easier implementation along with a possible framework for an international construct dealing with this pressing legal issue.

© 2015 Felicity Gerry. Published by Elsevier Ltd. All rights reserved.

* Corresponding author. School of Law, Law Education Business & Arts, Charles Darwin University, Darwin, Northern Territory 0909, Australia.

** Center for International and Comparative Law, University of Baltimore School of Law, 1420 N. Charles St. Baltimore, MD 21201, USA. E-mail address: Felicity.Gerry@cdu.edu.au (F. Gerry QC), cmoore@ubalt.edu (C. Moore).

¹ Both authors contributed equally to the article.

² ILRC comparative research related to Cambodia's Cybercrime Law prepared for the ABA Justice Defenders Programme by Felicity Gerry QC and Catherine Moore and teams of students from Charles Darwin University (Australia) University of Baltimore School of Law (United States).

<http://dx.doi.org/10.1016/j.clsr.2015.05.008>

0267-3649/© 2015 Felicity Gerry. Published by Elsevier Ltd. All rights reserved.

1. Introduction

In April 2014, [ARTICLE 19](#), a London-based human rights organization obtained a copy of a draft Cybercrime law for Cambodia.³ [Article 40](#) of the proposed legislation indicates that it will go into effect 12 (twelve) months after the promulgation. It is therefore due for implementation in or about April 2015. Our recent comparative research project on the draft Cybercrime law for Cambodia started as an analysis of the terms but soon exposed a dangerous global drift by all States from the necessary common human rights standards in the context of global cyber law.⁴ Thus, this article was written with the intent to make clear our own personal recommendations relating to the specific terms of the draft Cybercrime law for Cambodia. Additionally, our comparative research highlighted the need for a more globally comprehensive and uniform approach to cyber law by all States.

The Internet is not a separate community for the world of cyberspace. Yet, the global nature of the connected world creates a new global legal conundrum highlighted here by the proposed Cambodian legislation. Cybercrime laws need to balance international criminal law principles with competing issues of sovereignty in the context of the online global community. The proposed Cambodian Cybercrime law does not address these issues. In addition, it has been drafted in such a way that it is ineffective as a tool to combat online crime. Its terms are misleading, beyond mere issues of translation and it has real potential to restrict the media, communication by social media and individual freedom. The structure and contents are such that rights are inhibited, policing is inappropriate and the legislation, if enacted could be used to target human rights activists/NGOs. The current draft restricts legitimate acts of expression and communication, and violates an individual's right to privacy. This version also fails to properly deal with child exploitation online and other cybercrime. If enacted, it is a dangerous instrument and requires significant amendment to comply with Cambodia's international obligations. This Article makes some practical suggestions and proposes some global solutions to address the larger issue of global compliance of international human rights law pertaining to the Internet and Cybercrime.

Even in the short comparative exercise we were able to conduct with the assistance of some willing students, it was plain that several states have attempted to enact laws to address such Internet related issues with varying degrees of success. Some states directly censor and control the Internet,⁵ while others place the responsibility for enforcing the law in the hands

of the trade organizations who stand to gain from their enforcement.⁶ Our research exposed a dangerous global drift by all States from the necessary common human rights standards in the context of global cyber law. States commitment to common human rights standards requires the formulation of a balanced set of cyber laws and procedures to combat cybercrime and improve cyber security, without compromising human rights in all States. This Article proposes the immediate formulation of a global panel of experts with a view to the creation of uniform global cyber law construct: An international convention envisaged by the OECD in the context of privacy as proposed over three decades ago.

2. The Internet: an environment ripe for state interference and regulation

The Internet is now a global information infrastructure and provider of commercial services as a result of the widespread adoption of browsers making information accessible for users across the globe. Access to the Internet is liberating and educational, however it has also been used a great deal to facilitate cybercrime. The prevalence of cybercrime is then used as a justification for intrusive surveillance and over regulation.⁷ Human Rights Watch has concisely summarized the issues: "Intrusive surveillance and over regulation threaten privacy right of individuals . . . Governments should only be able to call for information relating to an individual's private life for the public interest. Any relevant legislation must specify the precise circumstances for accessing private individual's information. In addition, the right to information requires governments to allow free flow of information . . . A decision to block access to online materials should be subject to the highest level of scrutiny, with a burden on the government to demonstrate that censorship would effectively avert a threat of irreparable, imminent, and weighty harm, and that less extreme measures are unavailable as alternatives to protect the state interest at issue."⁸ The major issue in any cybercrime law (Cambodian or otherwise) is balancing competing interests on an individual, corporate, government and global level.

However, the speed of technological changes outpaces social and legal changes. In a very short space of time, much of the world has moved from telephones to smart phones, desktop computers to laptops to tablets to invention like Google Glass. Now there are cyborgs and artificial intelligence.⁹ The slower pace of changing domestic law means that criminal laws and

³ [ARTICLE 19](#), *Cambodia: Secret Draft Cybercrime Law seeks to undermine free speech online* (Apr. 9, 2014), accessible at <http://www.article19.org/resources.php/resource/37516/en/cambodia-secret-draft-cybercrime-law-seeks-to-undermine-free-speech-online#sthash.F9LjIwql.dpuf> [last accessed Sept. 22, 2014].

⁴ ILRC comparative research related to Cambodia's Cybercrime Law prepared for the ABA Justice Defenders Programme by Felicity Gerry QC and Catherine Moore and teams of students from Charles Darwin University in Australia and the US University of Baltimore.

⁵ S.C.S., *Why South Korea is really an Internet dinosaur*, *THE ECONOMIST* (Feb. 10, 2014), <http://www.economist.com/blogs/economist-explains/2014/02/economist-explains-3>.

⁶ Ed Black, *WCIT, TPP, Russia PNTR: Growing Recognition of Internet Freedom As A Trade Issue*, *FORBES* (Dec. 19, 2012), <http://www.forbes.com/sites/edblack/2012/12/19/wcit-tp-russia-pntr-growing-recognition-of-internet-freedom-as-a-trade-issue/>.

⁷ Felicity Gerry QC and Nadya Berova, *The rule of law online: Treating data like the sale of goods: Lessons for the Internet from OECD and CISG and sacking Google as the regulator*, 30 *CHAR. DAR. UNIV. COMP. L. & SEC. REV.* 489 (2014).

⁸ "Race to the Bottom" - *Corporate Complicity in Chinese Internet Censorship*, *HUMAN RIGHTS WATCH*, 5 (Aug. 10, 2006), <http://www.hrw.org/reports/2006/china0806/3.htm>.

⁹ Frank Swain, *Beyond human: How I became a cyborg*, *BBC* (Jan. 8, 2014), <http://www.bbc.com/future/story/20140107-how-i-became-a-cyborg>.

Download English Version:

<https://daneshyari.com/en/article/466415>

Download Persian Version:

<https://daneshyari.com/article/466415>

[Daneshyari.com](https://daneshyari.com)