CHINA

SUBMISSION TO THE NPC STANDING COMMITTEE'S LEGISLATIVE AFFAIRS COMMISSION ON THE DRAFT "CYBER SECURITY LAW"

AMNESTY INTERNATIONAL

Amnesty International Publications

First published in 2015 by
Amnesty International Publications
International Secretariat
Peter Benenson House
1 Easton Street
London WC1X 0DW
United Kingdom
www.amnesty.org

Index: ASA 17/2206/2015
Original Language: English
Printed by Amnesty International, International Secretariat, United Kingdom

Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

AMNESTY
INTERNATIONAL

Amnesty International welcomes the Chinese Government's practice of conducting public consultation before promulgating laws, and we are submitting the following comments regarding the People's Republic of China (PRC) Draft Cyber Security Law (hereafter Draft Law), issued by the Standing Committee of the National People's Congress (NPC) on 6 July 2015 after initial review at its 15th meeting.[1] Amnesty International would appreciate any opportunity to present further information, in writing or in person, to the Legislative Affairs Commission of the Standing Committee.

As part of our work, Amnesty International promotes the adoption of legal instruments that protect internationally recognized human rights. This submission contains Amnesty International's concerns about selected provisions of the Draft Law, which appear to be incompatible with China's international human rights obligations, whether embodied in treaties and other instruments, or under customary international law. Our organization hopes that these comments will ultimately contribute to the enhancement of the protection of human rights in China.

After careful examination of the provisions of the Draft Law, Amnesty International's position is that many provisions of the Draft Law would run counter to China's national and international obligations to safeguard the right to freedom of expression and the right to privacy. The Draft Law would legalize censorship and surveillance in the name of national security beyond the requirements set out in international law, including strict tests of necessity and proportionality.

In the Report on the work of the Standing Committee of the NPC on the third Session of the 12th NPC held in March 2015, Zhang Dejiang, chairman of the Committee, said that to "uphold the rule of law in our efforts to advance national security", they would formulate a National Security Law, an Anti-terrorism Law, a law on the management of international NGOs in China, and a Cyber Security Law[2]. This set of laws is clearly linked in a newly articulated national security architecture, giving legal bases to what has often been practice before, and on which Amnesty International has raised similar concerns about the same poorly defined and vague concepts in these law, and called upon the Chinese government to withdraw or repeal these too due to the risk of human rights violations and because of the high risk of misuse.[3]

The issues and provisions cited below are illustrative and not exhaustive examples of problems

[1] *People's Republic of China Draft Cyber Security Law*, 《中华人民共和国网络安全法（草案）》, http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm, accessed 20 July 2015.

[2] *Report on the work of the Standing Committee of the National People's Congress delivered at the third session of the 12th National People's Congress on 8 March 2015 delivered by Zhang Dejiang, Chairman of the Standing Committee of the National People's Congress*, http://www.npc.gov.cn/englishnpc/Special_12_3/2015-03/20/content_1930867.htm, accessed 20 July 2015.

[3] For Amnesty International's comments on the National Security Law, the draft Anti-terrorism Law, and the draft Foreign NGOs Management Law, see https://www.amnesty.org/en/latest/news/2015/07/china-scrap-draconian-new-national-security-law/; https://www.amnesty.org/en/latest/news/2015/03/china-draconian-anti-terror-law/; and https://www.amnesty.org/en/documents/asa17/1776/2015/en/, all accessed 3 August 2015.

with the Draft Law, and do not purport to constitute a comprehensive human rights analysis of the Draft Law. In this submission, Amnesty International in particular submits concerns and recommendations with regard to the principle of legality; far-reaching restrictions of the right to freedom of expression and the right to privacy; and the assertion by the authorities of the concept of "cyberspace sovereignty".

Amnesty International urges the Chinese government to withdraw the present Draft Law. Should the government decide that a "Cyber Security" law is truly needed, it should introduce a new draft that is compatible with China's human rights obligations and amend or repeal similar provisions in the whole set of interrelated laws.

I. GENERAL CONCERNS

Terminology

Article 1 of the Draft Law states that the law is formulated among other reasons "to ensure network security, to preserve cyberspace sovereignty, national security and societal public interest". Article 9(2) goes on to state that any person or organization using the network "must not use the network to engage in activities harming national security, propagating terrorism and extremism, including ethnic hatred and ethnic discrimination …upsetting social order [and] harming the public interest …". These terms lack clarity and precise definition such that it is difficult for individuals to predict what behaviour will run foul of the law. Amnesty International has documented that some governments have used concepts such as "public security", "national security", "terrorism" and "extremism" as misplaced justification to repress political opposition, human rights defenders and critical media reporting, and otherwise restrict the right to freedom of expression, association and religion. In existing law and practice in China "national security" and maintaining "social order" have been prioritized over individual human rights, to an extent that is not in compliance with international law and standards.

Similarly, these terms are either not defined or only defined broadly and vaguely in other related laws. The definition of "national security" found in the National Security Law Article 2 is virtually limitless, covering "the welfare of the people, sustainable economic and social development, and other major national interests". The draft Anti-Terrorism Law Article 104 broadly defines "extremism" as "the distortion of religious doctrine and advocacy of religious extremism, as well as other thought, speech, or behaviour which advocates violence, hatred against society, or opposition to human beings".

Amnesty International is concerned that the proposed terminology would breach China's obligations under international human rights law by failing to satisfy the necessary requirements of clarity, accessibility and foreseeability as prescribed by the principle of legality, a core general principle of law, enshrined, *inter alia*, in Article 15 of the International Covenant on Civil and Political Rights (ICCPR) and Article 11 of the Universal Declaration of Human Rights (UDHR). With regard to criminalization, the principle of legality requires that the law must classify and describe offences in precise and unambiguous language that narrowly defines the punishable behaviour. This means that all criminal laws, including counter-terrorism laws, must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly, and must not confer unfettered discretion on authorities, but rather provide sufficient guidance to those charged with their application to enable them to

ascertain the sort of conduct that falls within their scope.[4]

National Security and Freedom of Expression

Internationally recognized human rights standards, as reflected, for instance, in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (hereafter "Johannesburg Principles")[5] allow governments to restrict the exercise of some rights, including freedom of expression, on the ground of national security in order to "protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force", whether from an internal or external force.[6] However, the same Principles emphasize that such restrictions are not legitimate if "their genuine purpose or demonstrable affect is to protect interests unrelated to national security", including to protect a government from embarrassment or exposure of wrong-doing, or to entrench a particular ideology.[7]

Freedom of expression includes all forms of electronic and internet-based modes of expression.[8] Any restrictions of the right to freedom of expression must be prescribed by law which is clear and accessible, in pursuit of a legitimate purpose, and must be necessary and proportionate to achieve that purpose. Any restriction must not only be adequate to the pursuit of the legitimate purpose, but must also be the least intrusive measure among those available. The burden is on the state to demonstrate the necessity and proportionality of the restriction. Restrictions must be consistent with all other human rights recognized in international law; may not impair the essence of the right affected; and may not be applied in a discriminatory or arbitrary manner.

The UN Human Rights Committee, the body mandated with interpreting the ICCPR, has pointed out that it is incompatible with this treaty, which China signed in 1998 and has repeatedly stated the intention to ratify, to invoke national security laws to suppress or withhold

---

[4] Report, UN High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism, UN document A/HRC/28/28 of 19 December 2014, para28. See also, *inter alia*, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN document E/CN.4/2006/98 of 28 December 2005, para46; UN Human Rights Committee, *"General Comment No. 34 on Article 19 of International Covenant on Civil and Political Rights*" (2001), para25, http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf, accessed 20 July 2015.

[5] *Johannesburg Principles on National Security, Freedom of Expression and Access to Information (Johannesburg Principles)*, adopted on 1 October 1995 by a group of experts in international law, national security, and human rights convened by Article 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of the Witwatersrand in Johannesburg, http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf, accessed 4 August 2015.

[6] *Johannesburg Principles*, Principle 2(a).

[7] *Johannesburg Principles*, Principle 2(b).

[8] General Comment no. 34 on Article 19 (2001), para12

from the public information of legitimate public interest that does not harm national security.[9]

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (hereafter Special Rapporteur on freedom of expression) expressed concerns, in his 2011 report, regarding regulations similar to those contained in the Draft Law, that "legitimate online expression is being criminalized in contravention of States' international human rights obligations … Such laws are often justified as being necessary to protect individuals' reputation, national security or to counter terrorism. However, in practice, they are frequently used to censor content that the Government and other powerful entities do not like or agree with."[10] The Special Rapporteur further underscored that "the protection of national security or countering terrorism cannot be used to justify restricting the right to expression unless it can be demonstrated that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence."[11]

Missing Safeguards

Article 23 of the Draft Law is problematic as it requires network operators to provide to investigating organs "necessary technological support and assistance in accordance with laws and regulation" for the needs of national security and criminal investigations. This provision, without any corresponding safeguards and used in connection with the vague and overly broad definitions in other laws mentioned above, could be used by authorities to curtail freedom of expression and persecute human rights defenders. For example, Amnesty International documented the detention of approximately 100 individuals simply for exercising their right to freedom of expression in support of the Hong Kong pro-democracy protests in 2014, many of them for simply posting their photos holding placards with slogans supporting the Hong Kong protests.[12] Many of these individuals were criminally detained on suspicion of "picking quarrels and provoking trouble" or "inciting subversion". There are no safeguards in the draft law to monitor the authorities' power to require private information from service providers and network operators, such as a mechanism of having the order approved by an independent and impartial court. Article 16 of the draft Anti-Terrorism Law likewise requires Internet service providers to provide technical support, including decryption, to public security organs and state security

[9] General Comment no. 34 on Article 19 (2001), para30.

[10] Frank La Rue, *"Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (hereafter "Report of the Special Rapporteur on freedom of expression"),* para72, 16 May 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, accessed 20 July 2015.

[11] *Report of the Special Rapporteur on freedom of expression),* para73.

[12] Amnesty International, "*China: Release supporters of Hong Kong protests",* 1 October 2014, http://www.amnesty.org/en/for-media/press-releases/china-release-supporters-hong-kong-protests-2014-10-01, and "*Chinese activists detained for supporting Hong Kong protests"*, 7 November 2014, updated 24 November 2014, http://www.amnesty.org/en/news/chinese-activists-detained-supporting-hong-kong-protests-2014-11-07, both accessed 20 July 2015.

organs preventing and investigating "terrorist" activities.

The Special Rapporteur on freedom of expression has pointed out: "Any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as administration of criminal justice, should be done through an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences."[13]

Amnesty International calls on the Standing Committee to withdraw or repeal the Draft Law and all other relevant draft laws recently introduced to serve the stated purpose of protecting national security, including the National Security Law, the Anti-Terrorism Law and the Foreign NGO Management Law. The Chinese Government should ensure that laws introduced to protect national security should have provisions that are clearly and strictly defined and conform to international human rights law and standards.

II. PRIVACY AND CENSORSHIP

Concerns about Privacy

Article 18 of the Draft Law expressly states that where network providers' "products and services have functions gathering users' information, this shall be expressed to users and their consent obtained", and other provisions such as Articles 34 to 39 likewise give a nod to strengthening the protection of personal data. Article 17(1) of the ICCPR states: "No one shall be subject to arbitrary or unlawful interference with his privacy … or correspondence …".[14] The right to privacy is important for the realization of the right to freedom of expression, to hold opinions, peaceful assembly, and association.[15] Under international human rights standards, every individual should have the right of access to information, including what personal data is stored, for what purposes, and which public authority or private entity controls these files.[16] Any surveillance of communications, whether of content or metadata, must be authorized in accordance with domestic laws, which set out in sufficient detail the extent and scope, and the manner of exercise, of any discretion granted to the relevant authorities to authorize and implement surveillance, as well as adequate and effective safeguards against arbitrary use and abuse.

However, the right to privacy is greatly undermined in Article 20 of the Draft Law by the requirement that network operators "shall require users to provide real identity information when signing agreements with users or confirming provision of services" and Article 31 which requires that infrastructure operators "shall store citizens' personal information and other important data gathered … within the mainland territory of the People's Republic of China.

[13] *Report of the Special Rapporteur on freedom of expression*, para75.

[14] See also Article 12 UDHR.

[15] See, e.g., UN Human Rights Council, *The right to privacy in the digital age*, resolution 28/16, UN document A/HRC/RES/28/16, 1 April 2015, preamble para13.

[16] General Comment no. 34 on Article 19 (2001), para18

Real-name registration and the requirement to keep the information stored in mainland China may increase the risk to human rights defenders, activists, and anyone engaging in discussions on topics officially deemed "sensitive", and will likely have a chilling effect on on-line discourse and social media activism. In contrast, the Special Rapporteur on freedom of expression has labelled the "relative anonymity" of the Internet as one of its "unique characteristics" contributing to its "vast potential and benefits."[17] The Human Rights Committee has stated further that States have to take effective measures to ensure that information concerning a person's private life is never used for purposes incompatible with the ICCPR.[18]

Obligations of Service Providers

The Draft Law requires:

a) network operators to immediately stop transmission of "information that the law or administrative regulations prohibits the publication or transmission of", delete such information, prevent it from "spreading", save relevant records, and report to the relevant departments (Article 40);

b) Distribution and software service providers, when the same type of information is discovered, to stop the provision of services and delete the information, store relevant records and report to relevant departments (Article 41(2)); and

c) Authorities to request network operators to also stop transmission of, delete, store and report such information; and where such information comes from outside of mainland China, to notify the relevant organization to adopt measures to block its transmission (Article 43).

These provisions appear designed to give a legal base to already existing, and highly problematic, practices in mainland China. There is already stringent control over the Internet in China in a manner that violates the right to freedom of expression, including the freedom "to seek, receive and impart information and ideas" of all kinds and regardless of frontiers (Article 19 UDHR and Article 19(2) of the ICCPR). Through technology colloquially known as "the Great Firewall", numerous foreign websites are inaccessible, including news sites like the New York Times, the BBC, Reuters, as well as independent Chinese news media like Boxun, China Elections and Governance, and Epoch Times. Popular social media platforms like Youtube, Facebook, and Instagram are blocked, as well as email services such as Gmail.

Xinhua, China's state news agency reported that on 6 November 2014 the Cyberspace Administration of China issued a "voluntary pledge" to be adopted by 29 of the main Internet portals, instructing them on how to censor comments made on their websites. The "voluntary

[17] *Report of the Special Rapporteur*, para23.

[18] UN Human Rights Committee, *"General Comment No. 16: Article 17 (Right to Privacy)"* (1988), para10, http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en, accessed 3 August 2015

pledge" prescribed a ban on information related to 18 topics, and included such vague and inherently subjective provisions as:

> 2) harming national security, divulging state secrets, subversion, damaging national unification ;
>
> 3) harming the nation's honour and interests;
>
> 6) damaging the nation's religious policies, propagating cults and superstition;
>
> 7) spreading rumors, disturbing public order, damaging social stability;
>
> 15) using language not normally used in the website to give comments;
>
> 17) intentionally using character combinations to avoid censorship;
>
> 18) disseminating other information that is banned by rules and regulations.[19]

The inherently wide scope and arbitrary nature of the censorship requirements under current practice goes far beyond the narrowly permitted purposes for which freedom of expression may be lawfully curtailed. Article 19(3) of the ICCPR allows restrictions – if sufficiency clear in law, necessary and proportionate – for the purpose of "national security"; however, internationalstandards limit this to the ability to "protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force", whether from an internal or external force.[20] Furthermore, the UN Special Rapporteur on freedom of expression has stated that "censorship measures should never be delegated to private entities, and that intermediaries should not be held liable for refusing to take action that infringes individuals' human rights"[21].

Amnesty International is also concerned that articles of the Draft Law (such as Articles 40, 41 and 43) and the penalties on service providers who fail to fulfil their respective obligations, may encourage these service providers to self-censor or over censor in order to avoid fines, suspension or termination of business or closing down of websites, and thereby would not be able to respect others' right to freedom of expression.

The UN Special Rapporteur on the freedom of expression has called upon "States that currently block websites to provide lists of blocked websites and full details regarding the necessity and justification for blocking each individual website. An explanation should also be provided on

---

[19] Xinhua, "29《跟帖评论自律管理承诺书》家网站签署" (29 Internet Companies Signed the 'Pledge to Self Regulate Internet Comments on Posts'"), 6 November 2014, http://news.sina.com.cn/c/2014-11-06/223631106669.shtml, accessed 20 July 2015.

[20] See, e.g., *Johannesburg Principles*, Principle 2(a).

[21] *Report of the Special Rapporteur on the freedom of expression,* para75.

the affected websites as to why they have been blocked."[22] He further pointed out that "any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as administration of criminal justice, should be done through an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences."[23]

Concerns about Restriction of Service

Article 50 of the Draft Law stipulates: "To fulfil the need to protect national security and social public order, and respond to major social security incidents, the State Council, or the governments of provinces, autonomous regions and municipalities with approvals by the State Council, may take temporary measures regarding network communications in certain regions, such as restricting it".

The UN Human Rights Committee has stated that any interference with the operation of websites, blogs or other internet-based, electronic or other dissemination systems, including respective supporting systems, must be in compliance with Article 19(3) of the ICCPR, which lays out permissible restrictions to the freedom of expression; such restrictions must be content-specific, rather than generically covering certain sites, and may not be based solely on the fact that the content is critical of the government.[24]

Amnesty International documented the cutting off of Internet access and its suspension for several months in the Xinjiang Uighur Autonomous Region (XUAR) in northwest China as a result of the July 2009 protests,[25] and is concerned that Article 50 of the Draft Law will provide legal authority for various government authorities to disproportionately restrict Internet access in violation of international human rights law and standards. While blocking and filtering measures denying users access to specific content on the Internet may be justifiable, cutting off users from Internet access entirely, regardless of the justification provided, is considered disproportionate and thus a violation of Article 19(3) of the ICCPR, according to the Special Rapporteur on freedom of expression.[26] States should ensure that Internet access is maintained at all times, including during times of political unrest.[27]

Flowing from the vaguely worded provisions and the subjective nature of charges in all the above-mentioned national security related laws, provisions in this Draft Law that oblige Internet service providers to censor, block, record and report to the authorities transmission of information that "the law or administrative regulations prohibits" lack legal predictability and

[22] *Report of the Special Rapporteur*, para70.

[23] *Report of the Special Rapporteur on freedom of expression*, para75.

[24] General Comment no. 34 on Article 19 (2001), para43.

[25] Amnesty International, *"Justice, justice": the July 2009 protests in Xinjiang, China,* 2010, https://www.amnesty.org/en/documents/asa17/027/2010/en/, accessed 28 July 2015.

[26] *Report of the Special Rapporteur on freedom of expression*, para78.

[27] *Report of the Special Rapporteur on freedom of expression*, para79.

could be used as a pretext to attack freedom of expression, association and religious beliefs.

Amnesty International calls on the Standing Committee of the National People's Congress to ensure that any limitations on the right to freedom of expression are limited strictly to applications in compliance with the tests of necessity and proportionality to achieve a legitimate aim, and that they are reviewed and approved after an independent and impartial judicial review, thereby giving effect to the suggestions of the Special Rapporteur.

III. CYBERSPACE SOVEREIGNTY

Amnesty International is deeply concerned that one of the other purposes of the Draft Law stated in Article 1, the preservation of "cyberspace sovereignty", would further serve to legalize the Government's online censorship practices and persecution of people freely expressing their opinion through the Internet. The term "cyberspace sovereignty", first referenced in Article 25 of the National Security Law[28], which came into effect on 1 July 2015, and mentioned in the Draft Law as a core purpose but with no definition, is a challenge to what the Special Rapporteur on freedom of expression has called "[t]he vast potential and benefits of the Internet [...] rooted in its unique characteristics such as its speed, worldwide reach and relative anonymity."[29] The Director of China's State Internet Information Office of the Cyberspace Administration of China, Lu Wei, published an Op-ed in 2014, entitled "Cyber Sovereignty Must Rule Global Internet", further detailing what the government means with the term "cyberspace sovereignty".[30] The concept however is not based on any international human rights laws or standards and therefore cannot be used as grounds to legitimize restrictions on Internet freedom and should not be promoted as a model for global regulation.[31]

Ensuring respect for human rights, including freedom of expression, is a vital component in the discussion of internet monitoring. Modern communication networks such as the Internet

---

[28] It stated that " The State establishes a national network and information security safeguard system, raising the capacity to protect network and information security; increasing innovative research, development and use of network and information technologies; to bring about security core techniques and key infrastructure for networks and information, information systems in important fields, as well as data; increasing network management, preventing, stopping and lawfully punishing unlawful and criminal activity on networks such as network attacks, network intrusion, cyber theft, and dissemination of unlawful and harmful information; maintaining cyberspace sovereignty, security and development interests."

[29] *"Report of the Special Rapporteur"*, para23.

[30] "U.S. companies operating in China show that those who respect the Chinese law can seize the opportunity of China's Internet innovation and create immense value, while those who chose opposition will be isolated by themselves and finally abandoned by the Chinese market." Lu Wei, "*Cyber Sovereignty Must Rule Global Internet*", 15 December 2014, http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html, accessed 3 August 2015.

[31] Amnesty International, "*Internet freedom faces new attack as China seeks to shape global web rules",* 18 November 2014, https://www.amnesty.org/en/latest/news/2014/11/internet-freedom-faces-new-attack-china-seeks-shape-global-web-rules/, accessed 3 August 2015

have proved invaluable to the development of human rights – revolutionizing access to information and improving transparency and accountability.[32] The Human Rights Committee has observed developments in information and communications technologies, providing a global network for exchanging ideas and opinion, and that States should foster the independence of these new media and ensure individuals' access.[33] The UN Human Rights Council has recognized the global and open nature of the Internet, and that related technological advancement is "a driving force … towards development".[34]

According to Article 2 of the Universal Declaration of Human Rights, everyone is entitled to the enjoyment of human rights, which includes the rights to freedom of expression and privacy. The concept of "cyberspace sovereignty" cannot be used to legitimize the infringement of freedom of expression and privacy beyond the bounds set by international law and standards.

Article 56 of the Draft Law, together with provisions in other laws, such as Articles 15, 16 and 94(3) of the Anti-Terrorism Law, which oblige companies to provide authorities with Internet technological interfaces and decryption support, would have the consequence that the authorities could obtain from all "critical information infrastructure" operators in mainland China information provided by these companies' users, living inside and outside of the territory of mainland China, under conditions that would violate the users' human rights. Article 94(3) of the draft Anti-Terrorism Law would allow the authorities to fine or give detention to directly responsible persons at the telecommunications and Internet service providers which do "not provide public security organs with telecommunications and internet technological interfaces or de-encryption technology support in accordance with law". No provision for sufficient oversight, judicial or otherwise, is made in these laws with regard to the making of such requests, or opportunities to challenge any subsequent penalties upon refusal to comply.

Provisions in the Draft Law could in fact impose China's domestic Internet rules beyond its territory, to Internet users worldwide who use platforms based in mainland China, or international companies that feel they have to comply with Chinese standards without differentiating their services for other markets. Amnesty International is concerned about the possible misuse of the Draft Law and the concept of "cyberspace sovereignty" initiated by the Chinese Government to compel Internet companies operating in China to be in compliance with the authorities' censorship directives, and compromise their responsibility to respect human rights, especially the right to freedom of expression under Article 19(2) of the ICCPR, of Internet users living inside and outside of the mainland territory of China. Rather than forcing Internet companies into a position in which they potentially abuse users' human rights, States in fact have a duty to protect the human rights of people subject to their jurisdiction from interference by private persons or entities, including business enterprises; this positive duty

[32] See Report, Special Rapporteur on extrajudicial, summary or arbitrary executions, *Use of information and communications technologies to secure the right to life*; UN document A/HRC/29/37 of 24 April 2015.

[33] General Comment no. 34 on Article 19 (2001), para15

[34] UN Human Rights Council, *The right to privacy in the digital age*, resolution 28/16 (2015), para2

applies in particular to the right to privacy, among others.[35]

The principle that companies have a responsibility to respect human rights is now well-established under international business and human rights standards as well. The Human Rights Council unanimously endorsed this principle when it approved the "Guiding Principles on Business and Human Rights: Implementing the 'Protect, Respect, Remedy' Framework" on 16 June 2011.[36] These Guiding Principles specify that companies have a responsibility to respect human rights that, "…exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations".[37] Contrary to the present provision in the Draft Law, the international human rights framework obliges States to require business enterprises to put in place due diligence processes to ensure they do not cause or contribute to abuses of human rights throughout their operations.[38] It appears that the present Draft Law would force companies to choose between complying with Chinese rules and regulations and fulfilling their obligation to respect their users' human rights.

Amnesty International calls on the Standing Committee of the National People's Congress to remove any provisions in law that have the effect of compelling corporations to cause or contribute to abuse of human rights and ensure that laws and regulations governing the Internet in China require corporations to respect human rights in line with international standards including the UN Guiding Principles on Business and Human Rights.

---

[35] United Nations Human Rights Committee, *"General Comment No. 31: The Nature of the General Legal Obligations Imposed on States Parties to the Covenant"* (2004), para8

[36] United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights,* 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf, accessed 3 August 2015.

[37] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, *UN Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework,* UN document A/HRC/17/3 (2011), Principle 11, and Commentary to Principle 11; see also, UN Human Rights Council, *The right to privacy in the digital age*, resolution 28/16 (2015), preamble para17

[38] *UN Guiding Principles on Business and Human Right*s, Principles 17-21

AMNESTY
INTERNATIONAL

www.amnesty.org