INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW
1126 16th Street NW, Suite 400
Washington, DC 20036 USA

Submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. David Kaye.

ICNL is pleased to present the following submission to Mr. David Kaye, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. ICNL's submission will primarily focus on "issue-spotting" with national examples, where appropriate.

Through this submission, ICNL is providing input on the first and second issue areas identified by the Special Rapporteur: the actors within the ICT sector that implicate freedom of opinion and expression, and legal and policy issues concerning the ICT sector, respectively. For the first issue area, ICNL has provided a summarized description of "how the internet works," which identifies the variety of actors necessary for Internet communications, all of which affect the freedom of expression. Regarding the second issue area, ICNL has provided a bullet-point list of legal issues related to the freedom of expression. ICNL notes that this is not a complete list, but rather illustrative of what ICNL believes to be the biggest threats to the freedom of expression.

How the Internet works

At the outset, ICNL has found that many people have a hard time grasping the issues related to the freedom of expression on the Internet because they are not aware of all the things that happen when one types a website into their web browser. While a full understanding of how the Internet works is unnecessary for most individuals, ICNL has found that a brief explanation of the actions that take place "behind the scenes" helps people understand the actors that constitute the Internet. Such explanation also helps identify points at which governments are able to restrict the free flow of ideas. Therefore, ICNL proposes that the Special Rapporteur consider publishing a brief overview of how the Internet works. ICNL has prepared a brief summary based on the summary provided in *Center for Democracy & Technology v. Pappert*, 337 F.Supp.2d 606, E.D.P.A. (2004).

Most people access the Internet through Internet Service Providers (ISPs), and increasingly through mobile telephone providers. In essence, mobile telephone operators act in a nearly identical fashion as ISPs and therefore, for clarity, mobile phone operators will be considered ISPs.

Individual Internet users generally contract on a monthly or annual basis with an ISP and will access that ISP's network over a high-speed connection wire such as a cable or digital subscriber line ("DSL"). A typical ISP's network is in turn connected, directly or indirectly (through a larger ISP), to the network of an Internet backbone provider (a very large ISP with high-speed transcontinental or global data lines), and through the backbone to other backbones, ISPs, and

networks that, collectively, comprise the global Internet. Similarly, businesses usually contract with an ISP to provide Internet access to their employees or to connect their internal computer network to the ISP's network, which is in turn connected to the global Internet. Some businesses connect to their ISP's networks (and the Internet) over dedicated high-speed connections, while others access the Internet over dial-cable circuits, or DSL circuits.

A communication over the Internet will commonly travel up the "tree" or hierarchy of networks of one or more backbone providers and then back down to its destination. A hypothetical communication (from an employee of a corporation) might originate on the user's computer, travel through the corporation's network, then through a regional ISP's network, then to a backbone provider, then to another backbone provider, then back down to a regional ISP, then, in some cases, through the network of a smaller ISP, and then to the corporate network of the destination, and finally to the computer of the intended recipient of the communication.

Communications on the Internet are usually divided into small "packets" that are separately sent over the Internet and reassembled on the receiving end. Separate packets that make up a given communication on the Internet are not required to travel over the same path from the sender to the recipient of the communication but can be routed over different paths within an ISP's network, or in the middle of the Internet, based on a variety of factors such as congestion on the network.

Publishing to the World Wide Web

Individuals, businesses, governments, and other institutions that want to make content broadly available over the Internet (web publisher) can do so by creating a web site. To make a web site available on the World Wide Web, a web publisher must place the content or web pages onto a computer running specialized web server software. This computer, known as a Web Server, transmits the requested web pages in response to requests sent by users on the Internet.

Web publishers have two common options for making a web site available over a Web Server. First, a web publisher can own and operate a Web Server on the web publisher's premises (including, possibly, the web publisher's home or business). In that case, the web publisher would contract with an ISP for Internet access and would thereby connect the Web Server to the Internet. Second, a web publisher may contract with a web hosting company (web host) to own and operate the necessary Web Server on the web host's premises (or third party premises arranged by the web host). A web host will typically operate one or more Web Servers that can store web pages for customers and make those web pages generally available to users on the Internet. Many ISPs offer web hosting services, but many web hosts operate independently of ISPs.

A web host offers a web publisher the ability to post a web page or a web site to the Internet. There are a variety of forms of web hosting, including arrangements where a web hosting company: (1) provides a Web Server to service a single web site of a customer, (2) provides a Web Server the customer can use to run multiple web sites, or (3) provides space on a Web Server that services the web sites of many different customers. The third form of web hosting is commonly called virtual web hosting.

Posting blog or posting to social media works the same way. The web publisher (Blogger, Twitter or Facebook user, for example) accesses that particular service or content provider (Blogger, Twitter or Facebook) via their ISP to the content providers servers. The web publisher then "publishes" his/her content by uploading the content to the content provider's servers. The content provider stores the publisher's pages, posts, etc. and generally makes that content available to other users on the service or the whole Internet depending on that particular service.

To access web pages on a web site, an Internet user utilizes a client computer program called a web browser, like Chrome, Firefox, Safari, etc. The web browser sends a request to a Web Server, which responds by sending the requested web page, which upon receipt is formatted and displayed by the web browser.

To access content on the Internet, the most common sequence is for a user to request content from a web site (via his/her web browser), and for the web site to return web pages to the user. This sequence is illustrated as follows, with the initial request shown by the arrows on the left, and the response shown by the arrows on the right:

↓	User	↑
↓	User's ISP	↑
↓	"Backbone" ISP	↑
↓	Web Site's ISP	↑
↓	Web Site	↑

As one can see, there are numerous actors, pieces of equipment and infrastructures that must be utilized in order for an individual to access the Internet. Private companies own 90% of the Internet's backbone. Private companies are not obligated to comply with international human rights standards in the same manner States are, and are susceptible to pressure from States because they often need a State's permission to operate within that country.

Main legal issues for freedom of opinion and expression within the ICT Sector

Taking everything discussed, it's useful to think of various levels that are needed to communicate over the Internet as layers.[1] One can categorize the various levels of Internet communications as either being part of the Infrastructure Layers (comprised of OSI Layers 1-3 since these layers include functions that must be implemented in each portion of the network) or the Application Layers (comprised of OSI Layers 4-7).[2] ICNL will categorize issues in the Infrastructure Layers or Application Layers, as appropriate.

[1] The Open Systems Interconnection model (OSI model) is a conceptual model of the Internet comprising 7 layers stacked on top of each other, where information is passed from one layer to the next, starting at the application layer and proceeding to the bottom layer, the physical layer, and then moving back up the hierarchy. The seven layers in the OSI model are: 1) the Physical Layer, 2) the Data Link Layer, 3) the Network Layer, 4) the Transport Layer, 5) the Session Layer, 6) the Presentation Layer, and 7) the Application Layer. Although there are other conceptual models comprised of a different number of layers, the OSI model seems to be the most-widely adopted model at the present time.

[2] Scott Jordan, *A Layered Network Approach to Net Neutrality,* International Journal of Communication 1, 427 at 443 (2007).

Infrastructure Layers

The infrastructure layers define how data is physically sent through networks, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, wifi, etc. Since the physical layer is the backbone and hardware of Internet communications, it is crucial that policies be established so that everyone has the ability to access the Internet.

- Monopolies: Accessibility is becoming a larger issue, especially as efforts to connect the next 3 billion people gain momentum. Establishing the actual infrastructure layer is expensive and labor intensive. Indeed, we have seen that due to this high barrier to entry, countries rely upon a small number of carriers to provide Internet services. This high barrier to entry means that there is risk of monopolies or oligopolies controlling the infrastructure in countries. The result of such a monopoly or oligopoly may lead to high costs for Internet access or a refusal by companies to enter non-lucrative markets, i.e. there is no incentive to lay fiber optic cable in rural or remote areas. This would result in less accessibility, which therefore prevents individuals from exchanging ideas and forming opinions. ICNL has concerns that monopolizing the Internet infrastructure will result in less accessibility and therefore a decreased ability to openly and freely exchange ideas.

- Net Neutrality: Internet users are entitled to service that does not discriminate on the basis of source, destination, or ownership of Internet traffic. Many are worried that without regulations mandating net neutrality, ISPs may block access to websites based the website's content, like political speech. The Council of Europe recently stated, "The principle of network neutrality underpins non-discriminatory treatment of Internet traffic and the users' right to receive and impart information and to use services of their choice. It reinforces the full exercise and enjoyment of the right to freedom of expression."[3] Internet content should not be subject to discriminatory practices for cultural, political or monetary reasons. The Internet should remain open with equal opportunities of use and access for all users.

- "Cyber-sovereignty": This concept, championed by the Chinese government in recent years, effectively cedes all control over the Internet and related networks to national governments; in other words, States enjoy the same sovereign rights in cyberspace as they do in physical space. Also known as "Internet sovereignty," this policy specifies that each nation has the unconditional right to regulate the Internet infrastructure and cyber activities within its borders, and this includes the right to censor and restrict information from entering its territory as well as through its territory.[4] This policy is wholly contradictory to the idea and philosophy that the Internet be a global community,

[3] Committee of Ministers of the Council of Europe, *Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality*, adopted on January 13, 2016.

[4] See e.g., Dan Levin, *At U.N., China Tries to Influence Fight Over Internet Control*, New York Times, December 16, 2015 (available at: http://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html).

connecting individuals across physical borders. The more control exercised by governments over the Internet infrastructure will lead to increased censorship and a reduced ability to exchange ideas. Indeed, China is already seeking to prosecute a German national for comments he made on the Internet while in Germany.[5] Rather than "cyber-sovereignty," the existing multi-stakeholder approach to Internet governance should be continued.

Applications Layer

- Privacy of user data: Currently, many companies, including ISPs, but also email services, financial services and social media, have access to vast amounts of user data. Revealing this data to governments may result in human rights defenders, dissidents and others being subjected to governmental harassment, surveillance or imprisonment. Yahoo infamously revealed the names and IP addresses of writers and dissidents using its services to the Chinese government, resulting in the arrest, detention and possible torture of these individuals.[6] Similarly, governments, such as Russia, are requiring ISPs to install equipment from intelligence agencies onto their networks, which allows for the government to access user data. Kazakhstan appears to have mandated the country's telecommunications operators to intercept citizens' Internet traffic using a government-issued certificate starting on January 1, 2016. Kazakhtelecom JSC announced that it will begin intercepting all mobile communications in January 2016 by requiring citizens to install a new "national security certificate" on their devices.[7] The certificate will function as an effective backdoor, allowing officials to intercept (and potentially block) a user's communications and browsing of foreign websites. Companies and organizations with access to user data should adhere to transparent privacy policies that protect and respect privacy rights as established in international human rights law.

- Storage of user data: In addition to keeping user data private, companies should not be required to physically store data and/or servers in specific countries. For example, some countries are requiring all entities conducting business on the Internet to keep, house and maintain their servers within that country's borders.[8] By requiring Internet servers and similar devices that are vital to a company's Internet operations to housed within a country's territory, government agencies are able to easily access stored information, including user data, via a search warrant or similar judicial instrument. In countries that lack an independent judiciary, obtaining search warrants can be accomplished easily and

[5] Didi Kirsetn Tatlow, *A German's Video Likens Mao to Hitler, and China Wants Him Punished*, New York Times, January 8, 2016 (available at: http://www.nytimes.com/2016/01/09/world/asia/china-mao-hitler.html).
[6] *Yahoo plea over China rights case*, BBC, August 28, 2007 (available at: http://news.bbc.co.uk/2/hi/asia-pacific/6966116.stm).
[7] Bill Buddington and Eva Galperin, *Kazakhstan Considers a Plan to Snoop on all Internet Traffic*, Electronic Frontier Foundation, December 15, 2015 (available at: https://www.eff.org/deeplinks/2015/12/kazakhstan-considers-plan-snoop-all-internet-traffic).
[8] See, Federal Law No. 242-FZ, Russia, July 21, 2014, requiring operators of personal data to store such data in Russia.

premised on arbitrary rationales, which is likely to have a stifling effect on free speech and the right to privacy. Therefore, companies should not be required to store their servers within a particular country and should be free to choose the best locations for their servers and other data storage devices.

- Intermediary Liability: There have been numerous examples of countries imposing intermediary liability on service providers. These restrictions potentially place ISPs and other telecom providers in a difficult situation. In some cases, they are forced to take on a quasi-law-enforcement function in order to avoid liability. In other cases, they are forced to comply with questionable orders even if those orders are illegal or unconstitutional and then risk being punished for acting illegally, or they refuse to comply with the orders and are fined, prosecuted and/or have their business license confiscated. Other times, they are forced to prove their innocence and their lack of involvement in a crime. For example, Tanzania's Cybercrime Act of 2015 shifts the burden of proof onto the service provider to prove that it was not involved in the illegal disclosure of data; service providers must prove: (1) that a third-party, or user, acted without the knowledge of the service provider and (2) that "the service provider exercised due care and skill to prevent…" such disclosure.[9] The Act violates the presumption of innocence,[10] which may negatively impact service providers' ability to work and invest in Tanzania in a way that promotes freedom of expression and the free flow of ideas and information. Internet intermediaries should not be liable for content posted by their users as this would likely lead to intermediaries – in an effort to avoid liability – banning and removing all types of content that should be protected under international human rights standards.

- Monitoring of Social Media: States increasingly monitor social media sites, and prosecute people for statements made online. In many cases, States can monitor these sites fairly easily, since much of this information is public and many users use their real names. However, States have also drafted laws that provide them with greater surveillance powers. These laws often violate the right to privacy, which includes the right for individuals to ensure that their communications "remain private, secure and, if they choose, anonymous." Cambodia is one of many countries that have been aggressively prosecuting individuals for comments made on social media and has created an agency tasked solely with monitoring social media.[11] Individuals have been arrested in Turkey, Tanzania, Myanmar, to name but a few, over social media posts in recent months. The heavy monitoring of social media combined with laws that restrict protected speech – for example, laws prohibiting "insults" – result in the freedom of expression being stifled and self-censorship becoming a norm. Investigations and subsequent prosecutions for speech made on Social Media should comply with the standards set forth in Article 19 of the ICCPR.

[9] Tanzania, The Cybercrimes Act, 2015, Article 39(3), (available at: http://www.parliament.go.tz/polis/PAMS/docs/1-2015-4.pdf).
[10] ICCPR, Article 14(2).
[11] See e.g., Taing Vida, *Monitoring the Internet*, Phnom Penh Post, September 8, 2015 (available at: http://www.phnompenhpost.com/national/monitoring-internet).

- Blocking access to the mobile messaging applications: There are numerous examples of governments or telecom providers blocking access to mobile messaging applications, such as Viber, WhatsApp, and Skype. These sites have historically provided a more secure and cheaper means of communication, particularly for groups or individuals who seek to remain connected with their counterparts in other countries. However, authorities are increasingly seeking to subsume them under national regulations. For example, in January 2016, users in Morocco reported difficulty in using free applications such as WhatsApp, Viber and Skype using 3G and 4G Internet. According to reports, these sites were blocked because they do not have license permits to operate as "telecom providers."[12] Without license permits, Moroccan telecom providers have the legal right to restrict the use of VoIP services through these applications.[13] Blanket blocking of mobile messaging applications has an enormous, detrimental impact on the freedom of expression, and therefore should only occur in emergency situations,[14] and in compliance with Article 19 of the ICCPR.

- Blocking access to websites: Several countries have blocked access to social media websites, including You Tube, Facebook, etc. For example, in 2014, Turkish officials blocked access to Twitter and YouTube. The Turkish government claimed that both Internet sites were threats to Turkish national security, relying on controversial new amendments to Turkey's Internet law that took effect in 2014. The amendments expanded the government's censorship powers by enabling authorities, without court order, to block access to websites based on the subjective allegation that a posting violates an individual's private life.[15] The UN Human Rights Committee has said that generic bans on the operation of certain sites and systems are not compatible with Article 19, paragraph 3 and various national Courts have also overturned laws that permitted bans on social media sites, including Turkey's Constitutional Court.[16] Despite these judicial rulings, many states continue to block access to websites. The blocking of websites should only occur once all the requirements from Article 19 of the ICCPR are met.

- Blocking access to Virtual Private Networks (VPNs): VPNs are an effective way to communicate securely and privately over the Internet. In simple terms, VPNs are a group

[12] Mona Abisourour, *Moroccan Telecom Providers Block Use of Whatsapp, Viber and Skype*, Moroccan World News, January 5, 2016 (available at: http://www.moroccoworldnews.com/2016/01/176863/moroccan-telecom-providers-block-use-of-whatsapp-viber-and-skype/).

[13] According to Article 1 of the National Telecommunications Regulatory Agency (ANRT/DG/N° 04-04) in regards to the protocol of VoIP services, the commercial provision of VoIP services to the public can only be done by telecom operators with a license.

[14] However, it should be noted that emergency situations are precisely the time when all such services should be fully operational as communication tools are necessary to locate and speak with family, friends, those injured or hurt and authorities so that proper assistance can be dispatched quickly and efficiently.

[15] *See*, Decision of the Constitutional Court of Turkey on Omnibus Bill No. 6552 amending the Law of Regulation of Publication on the Internet and Suppression of Crimes Committed by Means of Such Publication, No. 5651 (Internet Law), (summary of the decision available at https://globalfreedomofexpression.columbia.edu/cases/the-turkish-twitter-case-of-2014/).

[16] UN Human Rights Committee, General Comment 34, para 43, Sept. 12, 2011 (available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f34&Lang=en).

of computers networked together over the Internet. VPNs allow a computer to behave as if it is based in another country; this is particularly important for businesses as they use VPNs to connect remote datacenters and to allow individual employees to access network resources when they are not physically on the same local area network. Additionally, many individuals use VPNs to get around government filters. It is of little surprise then that Iran[17] and China,[18] block access to VPNs. VPNs are a powerful tool to promote privacy, security and expression, and individuals should be free to use VPNs as they see fit.

- Prohibiting encryption: As a result of individuals seeking more security in their communications, States are presently grappling with prohibiting software and hardware companies from encrypting communications over their networks or applications.[19] This prohibition could also include forcing companies like Apple or Juniper Networks to create "backdoors" into their software so that encrypted communications can be unencrypted by law enforcement. There are reports that China has already enacted a law requiring companies to provide encryption keys to government authorities.[20] Encrypting one's communications is vital in efforts to be secure in one's communications, which is part of the right to privacy and the freedom of expression. Limitations of the use of privacy-enhancing tools that can be used to protect communications, such as encryption, amounts to a restriction on the right to privacy in one's communications.[21]

- Real-name requirements: Recently some States and social media companies have begun requiring Internet users to register for services using their real names and other, real personal data; Facebook[22] and Brazil[23] are the two latest examples. Brazil's proposed law would require all Internet users in Brazil to provide their full name, home address and taxpayer ID to every website they use, and require every website and application, including those with no presence in Brazil, to store users' personal details for up to three years and provide access to police or other "competent authorities." There are two main risks of requiring such personal data to use the Internet and applications. First, the

[17] Yeganeh Torbati, *Iran blocks use of tool to get around internet filter*, Reuters, March 10, 2013, available at: http://www.reuters.com/article/us-iran-internet-idUSBRE9290CV20130310

[18] *China blocks virtual private network use*, BBC, January 26, 2105 (available at: http://www.bbc.com/news/technology-30982198).

[19] See, e.g., Tom Whitehead, *Internet firms to be banned from offering unbreakable encryption under new laws*, The Telegraph, November 15, 2015 (available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11970391/Internet-firms-to-be-banned-from-offering-out-of-reach-communications-under-new-laws.html).

[20] Mark Willson, *China passes law requiring tech firms to hand over encryption keys*, Beta News (available at: http://betanews.com/2015/12/27/china-passes-law-requiring-tech-firms-to-hand-over-encryption-keys/); Ferenstein Wire, *China Passes Law to Require Encryption Keys from Tech Companies, Cites American Precedent*, Breitbart, December 27, 2015 (available at: http://www.breitbart.com/big-government/2015/12/27/china-passes-law-require-encryption-keys-tech-companies-cites-american-precedent/).

[21] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 71, UN Doc. # A/HRC/23/40, (April 2013).

[22] Facebook has since improved upon this policy; *see*: Access Now, "Facebook: Nameless Coalition demands fixes to real name policy," October 5, 2015 (available at: https://www.accessnow.org/facebook-nameless-coalition-demands-fixes-to-real-name-policy/).

[23] Matt Sandy, *Brazilian Lawmakers Threaten to Crack Down on Internet Freedom*, Time, January 20, 2016 (available at: http://time.com/4185229/brazil-new-internet-restrictions/).

gathering of this data becomes a treasure trove of information for governments and hackers alike, which will likely lead to an increased risk of private information being stolen. Second, while using one's real name may be beneficial in some instances or for some social media hubs, many individuals cannot use their real name when using the Internet, especially if they wish to publish statements critical of governments or are using web sites or services prohibited in their country of residence. Individuals should not be required by their governments to register with their real-names or other identifying information before accessing the Internet. Similarly, web services should allow for individuals to use aliases either as a rule or as an exception to user policies.

- Duplicative crimes: As more countries adopt "cybercrime legislation," the risk of duplicative crimes increases. These cybercrime laws – in addition to criminalizing legitimate speech - often recriminalize actions already criminalized in penal codes or other legislation. This can result in similar conduct being treated differently and inconsistently. For example, Cambodia's draft Cybercrime Law outlines penalties for child pornography when produced or disseminated over the Internet that are weaker than the penalties for producing or distributing child pornography in the Law on Suppression of Human Trafficking and Sexual Exploitation. To the greatest extent possible electronic crimes laws, or cybercrime laws, should mirror penal codes and other criminal laws, and ideally should focus on actions genuinely and directly related to computer information and systems.

ICNL remains available to provide additional information, including additional country-specific examples, or assistance, as appropriate.
Respectfully submitted
January 29, 2016