Human Rights Watch Submission

World Development Report 2016 – Internet for Development

August 2015

Thank you for meeting with us on May 26, 2015. We appreciate the opportunity to provide input into the World Bank's 2016 World Development Report on Internet for Development. The report represents an opportunity for the World Bank to provide policy guidance to governments in the digital age and ensure that investments in Internet technologies promote social and economic opportunity, civic participation, and good governance.

While affordable Internet access and inclusion remain significant challenges in most of the world, Human Rights Watch welcomes the Banks's recognition that increasing access to Internet and mobile phones is not, by itself, enough to fully realize the benefits of the Internet to development. The Internet and mobile phones have been a boon to independent civil society, human rights activists, and the media. Yet they have also brought new risks for outspoken critics and ordinary citizens alike. Governments are increasingly employing invasive digital surveillance and censorship to counter efforts to demand accountability using these tools.

The full potential of the Internet to support development goals cannot be fully realized unless human rights are protected online. In a landmark 2012 resolution adopted by consensus, the UN Human Rights Council recognized that the same rights that people have offline must also be protected online.[1] The Council also recognized that the global and open nature of the Internet is "accelerating progress towards development in its various forms" and called on all states to ensure protection for freedoms of expression, association, the right to privacy, and other rights online so that it can "continue to be a vibrant force that generates economic, social and cultural development."[2]

We note that the research team for the 2016 report has already recognized in its tentative findings that the Internet has "empowered governments, but often not their citizens."[3] We urge the Bank to document the

[1] UN Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet," Resolution 20 (2012), U.N. Doc A/HRC/20/L.13. This resolution enjoyed broad international backing from more than 70 Human Rights Council member countries and non-members from all regional groups.

[2] UN Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet," Resolution 26 (2014), U.N. Doc A/HRC/26/L.24.

[3] World Bank Group, "World Development Report 2016, Internet for Development Overview Presentation", June 2015, http://www.worldbank.org/content/dam/Worldbank/Publications/WDR/WDR%202016/WDR2016_overview_presentation.pdf (accessed August 26, 2015).

links between human rights online and development, identify barriers to digital participation, and put forward policy recommendations to support governments in reversing this trend.

Specifically, we ask the World Bank to:

- Solicit input from the information and communications technology (ICT) industry and civil society, with particular emphasis on organizations with expertise on the Internet and freedom of expression, privacy, and other human rights online.

- Document in the report's fact finding chapters (chapters 1-3) case studies of ways in which governments have censored expression and limited access to information online and used digital surveillance to target and silence criticism of government policy.

- Recognize in the report's policy analysis chapters (chapters 4-5) that an enabling regulatory environment for development must include strong protections for the right to privacy, freedoms of expression and association, and other human rights online.

1. Human Rights Online and Barriers to Development

The World Bank has increasingly emphasized the importance of civic participation and social accountability for sustainable development. These concepts involve enabling people to provide input into decisions that affect them and hold decision-makers to account, including through civil society organizations and the work of independent media.

The global Internet has become crucial to the work of independent civil society and journalists worldwide. Increasingly affordable, global communications tools allow environmental, anti-corruption, and human rights activists to document abuses and disseminate their findings quickly and on a worldwide scale. Civil society organizations, union leaders, and activists can more easily connect and organize through a range of digital tools to amplify the impact of their work. Social media gives independent voices a platform in places where legacy media is heavily controlled. It is not accidental that the rise in global digital communications has coincided with some of the strongest efforts to end impunity for abuses or expose corruption.

In this context, it is no surprise that some governments see the Internet as a threat and have tried to censor and control its use. Digital technologies have enabled intrusive governmental surveillance that violates the right to privacy on an unprecedented scope and scale. Governments are building their technical surveillance capacity and enacting new laws to expand spying powers and limit anonymity online, with little to no safeguards. Some security agencies employ commercially available intrusion tools (or "spyware") to hack into and compromise the computers of activists and opposition party members. Such surveillance can enable governments to identify journalistic sources, government critics, whistle-

blowers, union organizers, or members of persecuted minority groups and expose such individuals to reprisals.

While the Internet has enabled extraordinary access to knowledge and information on a global scale, governments are also learning how to shape and censor citizens' ability to speak and access information online, violating the right to freedom of expression. Blocking and filtering of Internet content is increasingly common, and often occurs with no judicial oversight, transparency, or due process.

Such censorship is often directed at independent media sources or social media and user generated-content sites used by civil society. Governments often put pressure on private sector Internet intermediaries (like social media companies) to censor content or shut down accounts of activists. In extreme cases, governments have shut down entire networks, as the Egyptian government did in 2011 during the popular Arab uprisings. However, some governments simply opt to arrest and imprison users that post "undesirable" content, which deters others and encourages self-censorship.

Human Rights Watch and others have documented many examples of such abuses, including in many of the countries where the WDR 2016 team held consultations. The following sections provide examples, along with policy implications and recommendations.

To fully address barriers to development, Human Rights Watch urges the World Bank to recognize there must be strong protections for the right to privacy, freedom of expression and association, and other rights online as part of an enabling regulatory environment for the ICT and telecommunications sector.

2. Surveillance, Privacy, and Data Protection

Protections for privacy are an essential component of an enabling environment for development. User trust is at the heart of ICT adoption: people may not use e-commerce, e-government services, mobile banking applications, social media services, and other applications if they do not trust that their communications and personal data will be kept private and won't be misused by abusive government officials or malicious private actors.

As more of our lives are lived online, our communications and activities routinely leave rich digital traces that can be collected, analyzed, and stored at low cost. In parallel, commercial imperatives drive a range of companies to amass vast stores of information about our social networks, health, finances, and shopping habits. The plummeting cost of storage and computing means that such data can be retained for longer and mined for future, unforeseen purposes.

These digital dossiers appeal to governments for a range of purposes, both legitimate and illegitimate. By accessing data held by the private sector, governments can easily uncover patterns of behavior and

associations, both offline and online—whether to thwart security threats or to identify a particularly vocal online critic of government policy. Governments are also able to access data on their own through hacking or interception of communications. Interception can take place on both a targeted basis and on a mass scale by tapping fiber optic cables or centralized network switches.

In a ground-breaking report released in July 2014, the then-UN High Commissioner for Human Rights documented how laws in most countries that regulate surveillance have not kept pace with technological change.[4] Applying old legal frameworks to new forms of highly intrusive or mass spying capabilities often leaves privacy and other human rights unprotected. Former National Security Agency contractor Edward Snowden's revelations of mass surveillance by the US and UK governments illustrate this point.[5] Yet even governments that lack the technological know-how can quickly build surveillance capacity with the help of surveillance systems and training sold by a burgeoning private sector.[6]

A survey of the surveillance laws in 44 countries released by the Telecommunications Industry Dialogue, a group of telecommunications operators, confirmed that "many countries lack a clear and transparent legal framework regarding government restriction of the content of communications and access to communications data. Provisions for adequate, independent oversight of these powers are also often absent. As a condition of operating in certain countries, governments may also require unrestricted direct access into companies' infrastructure."[7]

The expansion of unchecked surveillance of the Internet and mobile phones can have devastating consequences for the work of independent civil society and journalists:

- *Ethiopia*: The Ethiopian government is one of the world's largest jailers of journalists and has sought to systematically silence government critics. To facilitate this goal, the government has started to build its capabilities for overbroad surveillance of Internet and mobile networks, even though penetration rates in the county lag far behind its neighbors. As documented in Human Rights Watch's March 2014 report, *They Know Everything We Do*, the government imposes virtually no restrictions on access to intercepted mobile calls by security agencies, leading to violations of privacy and other rights.[8] The government has subjected individuals to abusive interrogations

[4] See UN Human Rights Council, "The right to privacy in the digital age," A/HRC/27/37, June 30, 2014, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx (accessed August 26, 2015); Joint Civil Society Statement on Privacy in the Digital Age, Submitted to the 27th session of the UN Human Rights Council (September 2014), http://www.hrw.org/node/129031 (accessed August 26, 2015).

[5] See Cynthia Wong, "Internet at a Crossroads: How Government Surveillance Threatens How We Communicate," *World Report 2015* (New York: Human Rights Watch, 2015), https://www.hrw.org/world-report/2015/essays/internet-crossroads.

[6] See Jennifer Valentino-Devries, Julia Angwin, and Steve Stecklow, "Document Trove Exposes Surveillance Methods," *Wall Street Journal*, November 9, 2011, http://www.wsj.com/articles/SB10001424052970203611404577044192607407780 (accessed August 26, 2015).

[7] Annette Fergusson, "Industry Dialogue Releases Resource on 44 Countries' Laws on Freedom of Expression and Privacy in Telecommunications," June 22, 2015, https://www.telecomindustrydialogue.org/industry-dialogue-releases-resource-on-44-countries-laws-on-freedom-of-expression-and-privacy-in-telecommunications/ (accessed August 26, 2015).

[8] Human Rights Watch, *"They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia*, March 25, 2014, https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia.

about their possible union or political activities. In these interrogations, governments often show detainees lists of mobile phone calls they have made or play back intercepted calls. Security agents would interrogate individuals about who they had been in contact with and why. As a result, individuals interviewed by Human Rights Watch reported that they did not view mobile phones as enabling tools for development, but another tool of government control.

- ***Russia***:[9] Security services in Russia have direct access to Internet service provider (ISP) infrastructure through SORM (System of Operative Search Measures), which allows security agents to monitor Internet traffic without any intervention from service providers.[10] While warrants are legally required to intercept communications, in practice security agents aren't required to show the warrant to service providers and Russians enjoy few safeguards for their privacy or redress when surveillance abuses occur. In 2014, Russia enacted a law that requires ICT companies that host user-generated content to retain data about their users and store such data within Russia, which will make it easier for the government to obtain sensitive personal data of users held by companies, without adequate protections for rights.[11] These "data localization" requirements are scheduled to go into effect in September 2015.[12]

- ***Mass surveillance in Central Asia***: Russia's SORM system has been emulated in several other countries in Central Asia and Eastern Europe. In a November 2014 report, Privacy International documented how "efforts to improve telecommunications infrastructure and attract foreign investment in Central Asia have been accompanied by the expansion of state censorship and electronic surveillance."[13] Privacy International interviewed journalists and activists in ***Uzbekistan*** who reported being arrested, detained, or harassed by authorities and shown transcripts of Skype conversations or other communications that could have only been accessed through surveillance or hacking. The report also examined the national legislative frameworks to regulate surveillance in ***Kazakhstan***, ***Kyrgyzstan***, ***Tajikistan***, ***Turkmenistan***, and ***Uzbekistan*** and found that they do

[9] Freedom House, *Freedom on the Net 2014*, "Russia," December 2, 2014, https://freedomhouse.org/report/freedom-net/2014/russia (accessed August 26, 2015).

[10] Andrei Soldatov and Irina Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You," *Wired*, December 21, 2012, http://www.wired.com/2012/12/russias-hand/ (accessed August 26, 2015).

[11] "Russia: Veto Law to Restrict Online Freedom," Human Rights Watch news release, April 24, 2014, https://www.hrw.org/news/2014/04/24/russia-veto-law-restrict-online-freedom (accessed August 26, 2015). Data localization requirements also have broad, negative economic impacts. One study estimated that Russia's localization requirement could lead to a loss of 0.27% of Gross Domestic Product (GDP), or the equivalent of US$5.7 billion. See Matthias Bauer, Hosuk Lee-Makiyama, and Erik van der Marel, "Data Localisation in Russia: A Self-imposed Sanction," European Centre for International Political Economy policy brief No. 6 (2015), http://www.ecipe.org/publications/data-localisation-russia-self-imposed-sanction (accessed August 26, 2015).

[12] Michael Mallow and Pavel Arievich, "Russia's Data Localization Requirement Will Take Effect September 1," DLA Piper, Data Protection, Privacy and Security Alert, July 8, 2015, https://www.dlapiper.com/en/us/insights/publications/2015/07/russia-data-localization-requirement (accessed August 26, 2015).

[13] Privacy International, *Private Interests: Monitoring Central* Asia, November 2014, https://www.privacyinternational.org/?q=node/293 (accessed August 26, 2015).

not adequately safeguard the right to privacy or do not yet regulate new kinds of modern surveillance methods like hacking into devices to ensure such capabilities are not abused.

- ***Turkey***: In April 2014, Turkey passed a new law that greatly expanded the surveillance powers of its National Intelligence Agency (MIT), while shielding it from accountability.[14] The law gave the agency sweeping powers to amass private data, documents, and information about individuals from banks, archives, companies, and other legal entities, all without the need for a court order. Turkey's laws fail to impose any clear limits on how long such data can be retained and how it may be accessed or used in order to protect the right to privacy. The new law also sets new penalties for journalists who publish leaked documents, even where there is a legitimate public interest (for example, where documents reveal corruption), and gives MIT personnel effective immunity from prosecution by allowing the agency's head to block any investigation into allegations of wrongdoing by agency officials.

- ***Increased use of commercially sold hacking/intrusion tools***: Toronto-based research center Citizen Lab has documented increased use of "spyware" by governments worldwide. This kind of surveillance software (also known as "intrusion software") enables governments to surreptitiously access personal computers and mobile phone and monitor all activity on that device. Once spyware is installed on a laptop or phone, it allows a government to copy files; capture passwords typed into the device; record Skype calls; monitor chat, email, and web browsing; and activate the computer's camera or microphone to spy on the user. Citizen Lab's four-year study involving ten civil society organizations documented how use of spyware "undermines [civil society organizations'] core communications and missions in a significant way, sometimes as a nuisance or resource drain, more seriously as a major risk to individual safety."[15]

    - Citizen Lab's research has also uncovered evidence that two such commercially available products, Hacking Team's Remote Control System and FinFisher's FinSpy, may have been in use in over 20 countries in recent years, including ***Ethiopia***,[16] ***Kazakhstan***, ***Uzbekistan***, and ***Turkmenistan***.[17] While some governments have the technical expertise to develop

[14] "Turkey: Spy Agency Law Opens Door to Abuse," Human Rights Watch news release, April 29, 2014, https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse.

[15] Citizen Lab, "Communities @ Risk: Targeted Digital Threats Against Civil Society," November 11, 2014, https://targetedthreats.net/index.html (accessed August 26, 2015).

[16] "Ethiopia: Hacking Team Lax on Evidence of Abuse," Human Rights Watch news release, August 13, 2015, https://www.hrw.org/news/2015/08/13/ethiopia-hacking-team-lax-evidence-abuse.

[17] Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Mapping Hacking Team's 'Untraceable' Spyware," Citizen Lab, February 17, 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/ (accessed August 26, 2015); Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab, March 13, 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ (accessed August 26, 2015). Leaked emails from Italian firm Hacking Team that were released in July 2015 confirmed that Kazakhstan and Uzbekistan had used the company's spyware products. See Ryan Gallagher, "Hacking Team Emails Expose Proposed Death Squad Deal, Secret UK Sales Push and Much More," *The Intercept*, July 8, 2015, https://firstlook.org/theintercept/2015/07/08/hacking-team-emails-exposed-death-squad-uk-spying (accessed August 26, 2015).

such tools themselves, many do not and must turn to the privacy sector to purchase technology and training. Documents that were leaked in July 2015 showed that an Ethiopian security agency paid US$1 million to Italian firm Hacking Team for its software, support, and training services in 2012 alone.

The right to privacy is an enabling right: if users cannot enjoy private spaces to speak and access information online without fear of unjustified monitoring—and the reprisals that can follow—other rights will be unavoidably harmed, including freedom of opinion and expression, association, and assembly. The Bank should urge governments to address these trends in three areas of regulation to ensure access to the Internet supports development:

- **Data protection laws** to regulate the data collection, use, dissemination, and retention practices of the private sector. As we shift more of our social, political, and economic lives online, ICT and telecommunications companies have commercial incentives to collect personal data. Companies may offer ad-driven services for free—which can be crucial for users in less-developed countries—but such services are built on large stores of data that are vulnerable to breach or misuse. Data protection laws should protect users against abuse of their personal data by private firms and provide recourse and redress.[18]

- **Regulation of the government's surveillance powers** to ensure any governmental intrusion into privacy is legal, proportionate, and necessary for a legitimate aim.[19] New capabilities like hacking must also be regulated consistent with human rights requirements. Surveillance and data collection should be subject to approval by an independent judicial authority and oversight by all branches of government. Governments must ensure effective remedy for violations of privacy through digital surveillance. Finally, governments should refrain from requiring ICT companies to retain consumer data in a blanket manner (that is, in the absence of individualized suspicion of wrongdoing), even for law enforcement purposes, because such requirements harm the privacy of all users and are not proportionate.[20]

- **Regulation of governmental data practices** related to personal data collected for public service delivery (online and offline), which, in turn, can support public sector transparency and accountability. Citizens should be able to understand what personal data the government collects

[18] For the European Union's approach to data protection, see European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: European Union, 2014), http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (accessed August 26, 2015)

[19] Mass surveillance is, by nature, disproportionate. For guidance on international human rights standards that apply to surveillance, see OHCHR, "The right to privacy in the digital age," A/HRC/27/37, June 30, 2014, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx (accessed August 21, 2015); Necessary and Proportionate, "International Principles on the Application of Human Rights to Communications Surveillance," https://en.necessaryandproportionate.org (accessed August 21, 2015).

[20] In April 2014, the European Court of Justice invalidated the EU Data Retention Directive, which required telecom providers across the EU to store certain user data for up to two years. See Cynthia Wong, "Dispatches: Victory for Digital Privacy on Data Retention," Human Rights Watch, April 29, 2014, https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse.

to provide public services and how such information will be used or retained. Collection of personal data should be limited only to what is necessary to provide the service for which it was collected, and should be deleted as soon as it is no longer needed. Especially where government-held data can result in adverse determinations—for example, denial of services or benefits—citizens must have the ability to review their data held in government systems and correct any errors. These privacy protections are critical for ensuring efficient, transparent, and accountable public service delivery.[21]

As with any technology, the Internet can also be used for illegitimate purposes. The WDR 2016 research team has already identified some of the risks posed to users and governments in the digital age, including distribution of child abuse images, identify and data theft, and facilitation of cross-border crime (on and offline). Yet increasingly, cybercrime, cybersecurity, or counterterrorism laws adopted by governments to address these threats do not strike a balance with pre-existing obligations to respect fundamental rights and fail to adequately protect privacy and freedom of expression or are misused by governments to target government critics and activists. For example, while many countries have acceded to the Council of Europe Cybercrime Convention or emulated its approach, many governments have removed the convention's safeguards for privacy and due process when implementing the convention in national law.[22] Some countries have also added new, vaguely worded offences for online activity that are not consistent with human rights requirements and impose disproportionate penalties.

- *Thailand*: In addition to hacking and illegal interception, Thailand's Computer Crimes Act criminalizes a range of online expression, including expression considered harmful to national security and public order. These provisions have been abused to target activists and journalists and shut down political discussions and debate online, which the military junta perceives as a threat to stability and national security.[23] Since the 2014 military coup, there has been a sharp increase in use of the Act, often combined with the lèse-majesté law, to punish criticism of the government on social media.[24] The Act also imposes liability on social media and other user-generated content websites for the content posted by users (known as "intermediary liability"), which encourages companies to censor users to avoid liability. One prominent media website, Prachatai, was forced to shut down its web discussion forum to protect users after the website's

[21] For how the United States regulates government data practices, see Electronic Privacy Information Center, "The Privacy Act of 1974," https://epic.org/privacy/1974act/ (accessed August 21, 2015).

[22] Civil society organizations have criticized the convention for not including adequate protections for privacy and due process rights. See Global Internet Liberty Campaign, "Comments of the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International on Draft 27 of the Proposed CoE Convention on Cybercrime," June 7, 2001, http://gilc.org/privacy/coe-letter-0601.html (accessed August 21, 2015).

[23] Human Rights Watch, "Joint Letter to Thai PM on Phuketwan Journalists RE: Drop Charges against Phuketwan Journalists Alan Morison and Chutima Sidasathian," July 9, 2015, https://www.hrw.org/news/2015/07/08/joint-letter-thai-pm-phuketwan-journalists; Human Rights Watch, *World Report 2015,* (New York: Human Rights Watch, 2015), Thailand chapter, https://www.hrw.org/world-report/2015/country-chapters/thailand.

[24] UN Human Rights Council, "Press briefing note on Thailand and Mali," August 11, 2015, http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16310&LangID=E (accessed August 21, 2015).

manager, Chiranuch Premchaiporn, was charged under the Act's intermediary liability provisions for content posted on the forum.[25]

- New or proposed cybercrime laws in ***Kuwait***,[26] ***Egypt***,[27] and ***Pakistan***[28] also contain broadly worded provisions that could be abused to penalize legitimate expression online and through social media sites, especially in the absence of safeguards in these laws for due process and human rights.

While governments have a legitimate interest in investigating and prosecuting cybercrime, the Bank should urge governments to ensure any regulation in the areas of cybercrime and cybersecurity are consistent with human rights requirements (including the protection of privacy) and minimize the risk that such laws are misused.

3. Internet Censorship, Freedom of Expression, and Anonymity

Increasing universal and inclusive access to the Internet for all should be a priority for the World Bank and governments alike. However, as any Internet user behind the Great Firewall of China can attest, not all access to the Internet is equal.

Freedom of expression entails the ability to both speak and receive information. The rise of social media and other user generated content services (YouTube, Twitter, Facebook, chat applications, etc.) have given citizens and journalists extraordinary new tools to communicate, connect, and seek independent sources of information.

The Internet's global, interconnected nature does present a novel challenge for governments: online content that is legal in one jurisdiction may be freely accessible from a jurisdiction where it would be illegal.[29] Yet many governments have attempted to restrict access to online content in illegitimate, disproportionate, or otherwise abusive ways. In some countries, such restrictions are not targeted at content that has been proscribed under democratically enacted laws, but at content that might be critical of government policies or identifies public corruption or waste.

---

[25] "Thailand: Internet Trial a Major Setback for Free Speech," Human Rights Watch news release, May 30, 2012, https://www.hrw.org/news/2012/05/30/thailand-internet-trial-major-setback-free-speech. Chiranuch Premchaiporn was the September 2011 recipient of Human Rights Watch's Hellman/Hammett Award for journalists under threat.

[26] "Kuwait: Cybercrime Law a Blow to Free Speech," Human Rights Watch news release, July 22, 2015, https://www.hrw.org/news/2015/07/22/kuwait-cybercrime-law-blow-free-speech.

[27] Ragab Saad, "Egypt's Draft Cybercrime Law Undermines Freedom of Expression," Atlantic Council, April 24, 2015, http://www.atlanticcouncil.org/blogs/egyptsource/egypt-s-draft-cybercrime-law-undermines-freedom-of-expression (accessed August 21, 2015).

[28] Human Rights Watch, "Joint Statement from Article 19, Human Rights Watch, Privacy International, Digital Rights Foundation, and others on the Prevention of Electronic Crimes Bill 2015 Pakistan," April 19, 2015, https://www.hrw.org/news/2015/04/19/joint-statement-article-19-human-rights-watch-privacy-international-digital-rights.

[29] This issue emerged early in the Internet's commercial history, where France sought to restrict access to pro-Nazi hate speech that is protected under US constitutional law, but was easily accessible in France where such speech is proscribed.

These restrictions are often disproportionate: for example, blocking an entire user-generated content site (like Blogger, Facebook, or YouTube) merely because one single post was found to be illegal. Internet blocking and filtering is often non-transparent and occurs without independent court oversight or safeguards to prevent mistakes or abuse. As an extreme measure, some governments have shut down networks in response to unrest, which also has broad, negative economic consequences.[30]

Governments have also applied pressure on Internet intermediaries—private companies that provide the networks and online services that make up the Internet—to censor expression online on their behalf.[31] Some governments impose direct liability on user-generated content sites (for example, Facebook, YouTube, Blogger) for the content posted by users, which drives companies to proactively monitor and restrict what users can say on their websites.

Finally, freedom of expression also entails the ability to speak anonymously online.[32] Yet some governments impose "real name registration" requirements for individuals who want to comment on websites, login at a cybercafé, or purchase a mobile SIM card.[33] Such requirements are often used to help the government to identify online activists who rely on anonymity as a shield against reprisals.

- ***Internet filtering and censorship***: As measured by the OpenNet Initiative, more than 40 countries filter and block Internet websites to some degree.[34] In the last few years, several countries, including ***Pakistan***, ***Turkey***, ***Vietnam***, and ***Tajikistan***, have blocked social media sites wholesale—and in a disproportionate manner—despite the fact that the vast majority of content hosted on such sites are legal.[35] In many jurisdictions, website blocking occurs without a court order and without adequate transparency or independent oversight, leaving far too much discretion for abuse. For example, in ***India***, the rules for blocking provide little in way of rights

[30] See Organisation for Economic Co-operation and Development, "The economic impact of shutting down Internet and mobile phone services in Egypt," February 4, 2011, https://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm (accessed August 21, 2015).

[31] See Center for Democracy & Technology, "Shielding the Messengers: Protecting Platforms for Expression and Innovation," December 2012, https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf; Manila Principles on Intermediary Liability, https://www.manilaprinciples.org.

[32] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, May 22, 2015, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (accessed August 21, 2015); UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, May 16, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (accessed August 21, 2015).

[33] See Human Rights Watch, "Comments Submitted to the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression On the Use of Encryption and Anonymity in Digital Communications," February 18, 2015, https://www.hrw.org/news/2015/02/18/comments-submitted-un-special-rapporteur-protection-and-promotion-right-freedom.

[34] OpenNet Initiative, "Global Internet Filtering in 2012 at a Glance," April 3, 2012, https://opennet.net/blog/2012/04/global-internet-filtering-2012-glance (accessed August 21, 2015).

[35] See Dana Liebelson, "Here Are the Countries That Block Facebook, Twitter, and YouTube," *Mother Jones*, March 28, 2014, http://www.motherjones.com/politics/2014/03/turkey-facebook-youtube-twitter-blocked (accessed August 21, 2015); Google Transparency Report, "Known Disruptions of Traffic to Google Products and Services," undated, https://www.google.com/transparencyreport/traffic/disruptions (accessed August 21, 2015).

safeguards or accountability for abuse.[36] Leaked blocking orders served on ISPs show that government authorities do not provide grounds for blocking content and also require that these orders be kept confidential. There is no provision to file an appeal in cases of error or abuse and failure to comply can result in fines or imprisonment. Because of the secrecy surrounding the process, it is difficult to assess how much material in India is being blocked and for what reason.

- *Vietnam*: Vietnamese citizens are increasingly well-informed about the country's problems. This has led to a dynamic expansion of critical but overwhelmingly constructive commentary expressed via digital and other media, questioning official policies, exposing official corruption, protesting land-grabbing, practicing religious beliefs in unauthorized ways, or calling for democratic alternatives to one-party rule. The government has responded with repression, including by expanding its legal assault on expression of opinion via the Internet. Enhancing already extensive government powers to punish and otherwise deter digital freedom, the government in September 2013, put into force Decree 72, which contains provisions legalizing content-filtering and censorship, and outlawing vaguely defined "prohibited acts." In November 2013, the government signed Decree 174, imposing fines on people who post "propaganda against the state" or "reactionary ideology" on social media channels like Facebook. In the past few years, Vietnam has become one of the most prolific jailers of dozens of bloggers and activists, under these and other laws.[37]

- *Ethiopia*: Human Rights Watch research has documented how the government has blocked access to independent news sources from outside the country.[38] The government has also previously tried to block encrypted Tor traffic, which is a tool used to communicate privately and anonymously online.[39] In 2014, six bloggers from Zone 9, a blogging collective that provides commentary on current events in Ethiopia, were charged under the abusive anti-terrorism law and the criminal code. The arrest and prosecutions of the Zone 9 bloggers has had a wider chilling effect on freedom of expression in the country, elevating the level of fear among bloggers and online activists who increasingly fear posting critical commentary on Facebook or other social media platforms.[40] Two of the bloggers were later released in July 2015 ahead of a visit from US President Barack Obama to Ethiopia.[41]

---

[36] Jayshree Bajoria, "Online Censorship Laws Needs Reform" *The Hoot*, January 21, 2015, https://www.hrw.org/news/2015/01/21/online-censorship-laws-needs-reform.

[37] Human Rights Watch, "Vietnam Universal Periodic Review Submission 2013," January 7, 2014, https://www.hrw.org/news/2014/01/07/vietnam-universal-periodic-review-submission-2013.

[38] Human Rights Watch, *"They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia*, pp. 53-60, March 25, 2014, https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia.

[39] "Ethiopia Introduces Deep Packet Inspection," post to Tor (Blog), May 31, 2012, https://blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection (accessed February 12, 2015).

[40] Human Rights Watch, *"Journalism Is Not a Crime": Violations of Media Freedoms in Ethiopia*, January 22, 2015, http://www.hrw.org/reports/2015/01/21/journalism-not-crime (accessed February 12, 2015).

[41] "Ethiopia releases journalists and bloggers ahead of Obama visit," *Agence France-Presse*, July 9, 2015, http://www.theguardian.com/world/2015/jul/09/ethiopia-releases-journalists-bloggers-obama-zone-9 (accessed August 21, 2015).

- *Russia*: Since 2012, Russia has steadily expanded Internet content blocking for several categories of prohibited content, including broadly defined "extremist" content. Several different agencies can order website blocking without a court order and these powers have been used to block opposition and independent media websites and blogs.[42] Without adequate transparency, it is hard to evaluate how many websites have been blocked, but some estimate it could be as many as 50,000 sites.[43] New regulations also went into effect in August 2014 that would require bloggers with 3,000 or more daily readers to register with the media regulator and identify themselves publicly, making it easier for the government to identify potential critics.[44] Similarly, separate regulations were published that would require users to provide identification to connect to public Wi-Fi networks.[45] Social networks remain a significant tool for organization and communication for activists and the political opposition. The government is imposing increasing pressure on social networking companies to take down content, especially content used to mobilize collective action.[46]

- *China*: China has constructed one of the world's most sophisticated systems of information control. The government imposes nationwide Internet blocking of a wide range of websites at centralized gateways that constitute the Great Firewall of China. In addition, the government imposes intermediary liability on all online service providers, including social media companies. As a result, Internet companies that operate in China are pressured to proactively censor user content that they may host.[47] A range of issues are systematically censored, including independent reports of China's human rights record, treatment of ethnic minorities, and criticism of certain areas of government policy. Over the years, the government has also sought to enforce real-name registration requirements to more easily identify social media users.[48] In February 2015,

[42] "Russia: Halt Orders to Block Online Media," Human Rights Watch news release, March 23, 2014, https://www.hrw.org/news/2014/03/23/russia-halt-orders-block-online-media; Human Rights Watch, *Laws of Attrition: Crackdown on Rusia's Civil Society after Putin's Return to the Presidency*, April 24, 2013, https://www.hrw.org/node/115058/section/11.

[43] Freedom House, *Freedom on the Net 2014*, "Russia," December 2, 2014, https://freedomhouse.org/report/freedom-net/2014/russia (accessed August 21, 2015); Human Rights Watch, "Russia: Don't Get Tagged on Social Media in Russia," *The Moscow Times*, December 31, 2014, https://www.hrw.org/news/2014/12/31/russia-dont-get-tagged-social-media-russia.

[44] "Russia: Veto Law to Restrict Online Freedom," Human Rights Watch news release, April 24, 2014, http://www.hrw.org/news/2014/04/24/russia-veto-law-restrict-online-freedom.

[45] "Russia demands Internet users show ID to access public Wifi," *Reuters*, August 8, 2014, http://www.reuters.com/article/2014/08/08/us-russia-internet-idUSKBN0G81RV20140808 (accessed February 12, 2015).

[46] Sam Schechner and Gregory White, "U.S. Social-Media Giants Are Resisting Russia Censors," *Wall Street Journal*, December 26, 2014, http://www.wsj.com/articles/u-s-tech-firms-face-showdown-with-russian-censors-1419620113 (accessed August 21, 2015).

[47] China's censorship requirements also pose considerable financial costs and harm innovation. For example, Youku Tudou, China's YouTube equivalent, must employ hundreds of staff to implement censorship requirements. See Kathrin Hille, "China's 'Manhattan' Becomes Censorship Capital," *Financial Times*, November 4, 2012, http://www.ft.com/cms/s/0/77b7cde6-24e1-11e2-8924-00144feabdc0.html (accessed August 21, 2015); Beibei Bao, "How Internet Censorship is Curbing Innovation in China," *The Atlantic*, April 22, 2013, http://www.theatlantic.com/china/archive/2013/04/how-internet-censorship-is-curbing-innovation-in-china/275188 (accessed August 21, 2015).

[48] "China: Renewed Restrictions Send Online Chill," Human Rights Watch news release, January 4, 2013, http://www.hrw.org/news/2013/01/04/china-renewed-restrictions-send-online-chill.

the government renewed calls to enforce these requirements, as well as shut down parody accounts by regulating online pseudonyms.[49] The government has also tried to block or interfere with Tor and encrypted web traffic and has recently stepped up blocks of Virtual Private Networks.[50] These tools use encryption to shield web traffic from surveillance and to circumvent the Great Firewall and are used by anti-corruption activists and business people alike.

- *Pakistan*: In recent years, Pakistani authorities have ordered multiple shutdowns of mobile networks in specific provinces or cities, often in the name of national security and public order or in response to sectarian violence.[51] In addition to the negative economic implications, such broad shutdowns can actually undermine public safety if people who rely primarily on mobile communications cannot reach emergency services.[52] Human rights experts from international and regional bodies have stated that such shutdowns "can never be justified under human rights law."[53] Pakistan has also threatened to ban encryption[54]. Most recently, digital rights group Bytes for All released a document in August 2015 that showed that authorities have instructed telecom companies to shutdown BlackBerry's enterprise communication services because of its use of encryption.[55]

UN human rights experts on freedom of expression have called on states to refrain from blocking Internet content, shutting down networks, imposing responsibility on Internet companies to censor users, and requiring real name registration.[56]

---

[49] Josh Chin, "China Is Requiring People to Register Real Names for Some Internet Services," *Wall Street Journal*, February 4, 2015, http://www.wsj.com/articles/china-to-enforce-real-name-registration-for-internet-users-1423033973 (accessed February 12, 2015).

[50] Craig Timberg and Jia Lynn Yang, "Google is encrypting search globally. That's bad for the NSA and China's censors," *Washington Post*, March 12, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/12/google-is-encrypting-search-worldwide-thats-bad-for-the-nsa-and-china/ (accessed February 12, 2015); Emerging Technology From the arXiv, "How China Blocks the Tor Anonymity Network," *MIT Technology Review*, April 4, 2012, http://www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network/ (accessed February 12, 2015); Andrew Jacobs, "China Further Tightens Grip on the Internet," *New York Times*, January 29, 2015, http://www.nytimes.com/2015/01/30/world/asia/china-clamps-down-still-harder-on-internet-access.html?_r=0 (accessed February 12, 2015).

[51] CGCS Mediawire, "Kill Switch in Pakistan: Q&A with Bytes For All Pakistan," January 8, 2014, http://www.global.asc.upenn.edu/kill-switch-in-pakistan/ (accessed August 21, 2015); Article 19, "Pakistan: Government Must Stop 'Kill Switch' Tactics," August 23, 2012, https://www.article19.org/resources.php/resource/3422/en/pakistan:-government-must-stop-'kill-switch'-tactics (accessed August 21, 2015).

[52] For example, see Media Alliance, "Cell Phone Network Shut Down in Pakistan," *Imran Ali Teepu Newspaper*, September 21, 2012, http://www.media-alliance.org/article.php?id=2169 (accessed August 21, 2015).

[53] Organisation for Economic Co-operation and Development, "The economic impact of shutting down Internet and mobile phone services in Egypt," February 4, 2011; Article 19, "Joint Declaration on Freedom of Expression to Conflict Situation," May 4, 2015, https://www.article19.org/resources.php/resource/37951/en/joint%C2%ADdeclaration%C2%ADon%C2%ADfreedom%C2%ADof%C2%ADexpression%C2%ADand%C2%ADresponses%C2%ADto%C2%ADconflict%C2%ADsituation (accessed August 21, 2015).

[54] See Matthew Rice, *Tipping the Scales: Security & Surveillance in Pakistan*, Privacy International, July 21, 2015, https://www.privacyinternational.org/?q=node/624 (accessed August 21, 2015).

[55] Syed Raza Hassan, "Pakistan Cracks Down on BlackBerry's Encrypted Messaging," *Reuters*, July 24, 2015, http://www.theglobeandmail.com/technology/tech-news/pakistan-cracks-down-on-blackberrys-encrypted-messaging/article25669209/ (accessed August 21, 2015).

[56] Frank La Rue, A/HRC/17/27; David Kaye, A/HRC/29/32.

The Internet cannot enable civil society actors to participate in governance or critique government policy if they cannot freely access information, use social media services, or if entire networks have been shut down. Activists and journalists cannot protect sources or do their work safely if governments restrict anonymity online, including through real-name registration requirements.

The World Bank should urge governments to:

- Protect freedom of expression online and ensure any restrictions are legitimate, necessary, and proportionate. Governments should refrain from blocking and filtering Internet content.

- Refrain from holding ICT companies responsible for content of their users or requiring them to censor content on the government's behalf.

- Protect anonymity online and refrain from requiring users to register with their real name or identity number as a prerequisite for Internet access, use of social media, or acquiring a mobile SIM card.

- Refrain from shutting down Internet or mobile networks wholesale. Such measures are inherently disproportionate.

4. International Human Rights Framework

Human rights law provides guidance for discussing relevant policy implications in Part II of the report. UN human rights experts have increasingly documented human rights violations linked to the Internet and articulated standards for permissible limitations on human rights online. Human Rights Watch urges the World Bank to incorporate the human rights standards articulated in this growing body of jurisprudence.

- In a seminal 2011 report, the then UN Special Rapporteur on freedom of expression Frank La Rue recognized the importance of free and open access to the Internet to the realization and enjoyment of a wide range of rights, from freedoms of expression, association and assembly to the right to take part in cultural life and education. Thus, the special rapporteur stated that "there should be as little restriction as possible to the flow of information via the Internet, except in few, exceptional, and limited circumstances prescribed by international human rights law."[57] Any restriction to rights online must be provided in law, pursuant to a legitimate aim, and limited to only what is necessary and proportionate.

- In two groundbreaking reports in 2013 and 2014, the then UN High Commissioner for Human Rights and the UN Special Rapporteur on freedom of expression documented how laws in most

[57] Frank La Rue, A/HRC/17/27, para. 68.

countries that regulate surveillance have not kept pace with technological change that enables new forms of highly intrusive or mass surveillance.[58] Applying old legal frameworks to new capabilities often leaves privacy and other human rights unprotected. The High Commission has called on all states to review national legal frameworks and bring them in line with human rights law to protect privacy.[59]

- In a May 4, 2015 joint statement, UN and regional human rights experts clarified that even in areas of conflict, "Filtering of content on the Internet, using communications 'kill switches' (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law."[60]

- On June 17, 2015, the UN Special Rapporteur on freedom of expression presented a report to the UN Human Rights Council that found that promoting strong encryption and protecting anonymity are fundamental for the protection of cybersecurity and human rights in the digital age.[61] Encryption and anonymity, separately or together, "create a zone of privacy to protect opinion and belief" and safeguards the work of journalists and their sources, civil society organizations, whistleblowers, and members of persecuted minority groups.[62]

5. The Role of Donors

The World Bank and other donors have an important role to play in supporting expansion of internet access in a rights-respecting manner. In the WDR, the World Bank should emphasize how donors can achieve this.

In particular, donors should:

- Assess the risks to privacy, freedom of expression, association and movement, and access to information of its projects with ICT components prior to project approval and throughout the life of

[58] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, April 17, 2013 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed August 26, 2013); UN Human Rights Council, "The right to privacy in the digital age," A/HRC/27/37.

[59] "Joint Civil Society Statement on Privacy in the Digital Age Submitted to the 27th Session of the UN Human Rights Council," Human Rights Watch, September 11, 2014, https://www.hrw.org/news/2014/09/11/joint-civil-society-statement-privacy-digital-age-submitted-27th-session-un-human-ri.

[60] Article 19, "Joint Declaration on Freedom of Expression and Responses to Conflict Situation," May 4, 2015, http://www.article19.org/resources.php/resource/37951/en/joint-declaration-on-freedom-of-expression-and-responses-to-conflict-situation (accessed August 26, 2015).

[61] "Joint Civil Society Statement on Privacy in the Digital Age Submitted to the 27th Session of the UN Human Rights Council," Human Rights Watch, September 11, 2014, https://www.hrw.org/news/2014/09/11/joint-civil-society-statement-privacy-digital-age-submitted-27th-session-un-human-ri.

[62] David Kaye, A/HRC/29/32.

the project. They should identify measures to avoid or mitigate these risks and comprehensively supervise the projects, including through third parties.

- In the context of telecommunications technical assistance, ensure that all advice provided is consistent with respect for the rights to freedom of expression and to privacy, particularly with respect to the risks of Internet censorship and illegal surveillance.

- Publicly and privately raise with government officials concerns about censorship, illegal surveillance, and network shutdowns and that human rights violations may undermine development priorities. Express such concerns in country strategies and similar documents that govern a donor's partnership with the government.