



MOBILIZING
FOR
GLOBAL
DIGITAL
FREEDOM

Navigating Troubled Online Waters After Egypt *How States Can Respect, Protect, and Fulfill Digital Rights Through Domestic and Foreign Policy,* Discussion Paper, March 2011

We have entered a moment in time where we have a global public commons of information through which citizens of the world can share, receive, and impart information; but this free exchange of communication is under siege on multiple fronts. **National governments, supranational bodies, corporations, criminals, and other non-state actors are all chipping away at the freedom of the internet, and, in doing so, our rights.**

This brief will focus on how States can fulfill their duty to protect against human rights abuses in the digital era, a topic that has taken on profound relevance with the recent wave of protests sweeping the Middle East and North Africa. As repressive governments continue to leverage their control over national infrastructure and corporations operating within their jurisdictions to quash peaceful protest, locate dissidents, and shut down the internet, a plethora of human rights risks and ethical dilemmas for States and corporations -- especially around how to protect freedom of expression and privacy online -- is rapidly emerging.

The debate about the use of ICT infrastructure for surveillance during recent protests in the Middle East has raised questions about the role of corporations vis-à-vis governments.¹ There are examples of a deeply disturbing trend of corporations, in the interest of profits, choosing to work with States and give away control over their networks and the rights of their users, rather than face the loss of a potentially huge market. For example, BlackBerry maker RIM -- which has been praised for its encryption standards in the past² -- has already reached an agreement with the Indonesian government to start filtering content on its handsets, demonstrating that obtaining this kind of control over private telecommunications infrastructure and thereby also surveillance of citizens, are not just pipedream "demands" of governments, but rather an increasingly very real and dangerous reality.³

While other actors have an important role to play in the realization of human rights, responsibility for defending human rights, protecting against violations (by States and other actors), and taking appropriate steps to investigate and redress abuses lies primarily with national governments. These international obligations apply online as they do offline, but governments, individual politicians, corporations, judiciaries, and civil society are increasingly uncertain about what their roles are in this arena, what steps they should take next, and how to ensure their legitimacy in the face of an explosion of digital activism and online information exchange. **This brief is designed to give some guidance to States in how to navigate these troubled online waters.**

¹ http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf: "...the Iranian elections raised questions for the providers of telecommunications network equipment. The closure of entire mobile telecommunications networks in Egypt exposed the vulnerability of telecommunications services providers to government demands. The "Green Dam Youth Escort" proposals in China were of great concern to computer makers. And demands from the governments of UAE, Saudi Arabia, and India (among others) to access messages sent over BlackBerry devices piqued the interest of handset makers everywhere

² <http://crackberry.com/blackberry-6-earns-fips-security-certification-u-s-government-agencies>

³ <http://www.guardian.co.uk/technology/2011/jan/10/blackberry-indonesia-pornography-filter>

The application of human rights in the digital age – what will be referred to here as digital rights – occurs in three ways. Firstly, it is the application of existing international human rights frameworks applied to the Internet. For example, freedom of speech must be protected online as fervently as it is offline and the same rights that have traditionally existed for mail sent through the postal system must be extended to e-mail. Secondly, there are rights that are enabled via access to the Internet, such as the right to health care through remote medicine, or the availability of education through online learning. And finally, there may well be the evolution of new rights that are unique to the digital sphere, such as unrestricted Internet access as a right unto itself. This third area must be approached with caution, as new rights must never be a substitute for existing rights or an opportunity to water down others.

Yet, the Internet's decentralized infrastructure does not lend itself well to clear rules of governance or regulation. Technological change outpaces the speed at which policy and regulations can be made and the consequences of technological policy decisions are often difficult to predict. Moreover, the interests of governments, the private sector, and civil society are frequently not aligned in such a way to make the preservation of digital rights a high priority. Nevertheless, as we speak, legal precedents are being set in courtrooms, contracts, and legislation that will directly impact the digital rights landscape for the foreseeable future. It is at these decisions points, where States are reassessing their relationship with the internet and the information society more generally. **An open internet is an unprecedented tool for the realization of digital rights, a forum for innovation, the gateway to prosperity, and the wellspring of social and economic growth, but in order to ensure a bright digital future, States must act now.**

With that in mind, Access offers the following recommendations to States focusing on: steps States can take within their own jurisdiction, steps States can take in their interactions with other States, steps States can take with respect to corporations within their jurisdiction, steps States can take on the international level, and steps States can take to bridge the digital divide.

These recommendations come from different constituencies and “schools of thought” and are intending to give a holistic view of ways in which States can take action to protect internet freedom and promote digital rights. Finally, this brief builds off of and inculcates elements from many other groups and people working on these issues including the Internet Rights and Principles Coalition⁴, The Council of Europe⁵, and the UN Special Rapporteur on Freedom of Expression Frank La Rue.⁶

Steps States can take within their own jurisdiction

Incorporate principles of digital rights

- Take measures to ensure that everyone has the legal right to access, and make use of, the internet (as is already the case to varying degrees in countries such as Estonia, Finland, Spain, and France).^{7 8} This should include making internet access available at libraries, community centers, clinics, schools, and other public institutions. Unfettered access to the internet via mobile devices must also be supported and promoted.
- States must not filter, block, throttle⁹, or censor the internet, and it is incumbent upon all States to implement policies to ensure that people can freely share, receive, and impart

⁴ <http://internetrightsandprinciples.org/>

⁵ e.g., <https://wcd.coe.int/wcd/ViewDoc.jsp?id=1678251&Site=CM>

⁶ e.g., <http://www.youtube.com/watch?v=q-TvU423ars>

⁷ http://news.cnet.com/8301-17939_109-10374831-2.html

⁸ Estonia, France, and Spain have also previously made access to the internet a universal right. See for reference:

<http://www.csmonitor.com/2003/0701/p07s01-woeu.html>

http://technology.timesonline.co.uk/tol/news/tech_and_web/article6478542.ece

<http://www.reuters.com/article/2009/11/17/spain-telecoms-idUSLH61554320091117>

⁹ Slowing down internet traffic and speed – a process sometimes called “throttling” or retarding – is a much more subtle form of internet traffic shaping and is often a highly effective way for governments to suppress free speech. For a recent example, see:

<http://www.renesys.com/blog/2011/03/what-libya-learned-from-egypt.shtml>

information online. Any restriction to this principle must strictly adhere to the rule of law and comply with international human rights law.

- States must refrain from online surveillance, interception, or monitoring of the internet, including any measures which have the result of intimidating internet users or encouraging self-censorship of expression online, including by direct or indirect pressure on internet intermediaries to carry out law enforcement activities under guise of “self-regulation.” Any restriction to this principle must strictly adhere to the rule of law and comply with international human rights law.
- Establish policies to ensure that people can communicate anonymously and securely including through the use of encryption technology and the free expression of an online identity.
- Put in place a comprehensive and transparent legal framework and corresponding security mechanisms to protect the privacy and personal data of citizens from state and company intrusion; and to ensure that citizens can exercise informed control over how their personal data is collected, used, disclosed, retained, and disposed of.
- Designate the internet a public utility with similar universal service provision requirements as existing telecommunications utilities (e.g., telephone service) and facilitate the right to participate in the global digital economy, in particular through e-commerce, to all citizens.

Establish principles of internet governance

- Ensure that such internet governance policies (including investment in infrastructure, policies on service provisions and carriage requirements, and laws regarding online conduct and property) adhere to principles of openness, inclusiveness, and accountability and are consistent with international human rights standards.
- Uphold principles of net neutrality (i.e., treating all data equally, no matter its origin or content), to ensure the free, equal and non-discriminating exchange of information.
- Adopt open spectrum policies, which will help reduce the digital divide by allowing communities to more easily build their own communications networks, lower costs, and diversify ownership of this public utility.¹⁰
- Facilitate and maintain interconnectivity and innovation by ensuring that communication infrastructures and protocols are interoperable and open.

Normalizing digital due process

- Ensure that everyone has the right to legal remedy and fair trial for any actions involving the Internet including procedural fairness and the right to due process.
- Curtail use of sealed subpoenas -- which do not allow online service providers to inform their users that a law enforcement authority has requested their information -- to only cases where they are absolutely necessary, adhere to the rule of law, and are appealable.
- States must ensure that they or other parties do not pressure online intermediaries to remove, hide, block content, or disclose information about Internet users.
- States should adopt policies exempting online intermediaries from liability so that any actions taken against illegal activity on the internet be aimed at those directly responsible for such activities, and not at the means of access, broadcast, or transport.
- Copyright laws should be designed in a way that does not limit the capacity of the internet to support public access to knowledge, resources, and culture or restrict innovation or creativity.
- Mandate that any and all requests for the take down of online information or seizure of digital property (e.g., domains) require a ruling by a judge or magistrate, so as to avoid a chilling effect on free speech.¹¹
- Interpret data retention mandates narrowly; limit data retention to the shortest period necessary for the purposes of network management and the defense of human rights;

¹⁰ <http://www.apc.org/en/node/11923/>

¹¹ <http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/>

publicly disclose what kinds of data are stored; allow individuals to request a copy of the data that a public or private entity has of theirs; and properly protect all data.

Steps States can take with respect to corporations within their jurisdiction

- Make operating licensure agreements transparent and open to public audit; currently this information, in most jurisdictions, can only be disclosed by the issuing authority (e.g. a national government).¹²
- Ensure greater due diligence in licensing for export technology that might be or by definition do infringe digital rights. For example, Deep Packet Inspection is an advanced surveillance technology that allows the user, typically ISPs or government entities overseeing them, to monitor and log all data that passes through a particular network.¹³¹⁴¹⁵
- Require sustainability reporting of companies, as outlined in the Ruggie Framework,¹⁶ that include criteria on the company's products' or services' capacity to infringe or diminish digital rights and internet freedom, or otherwise be used as tool of repression.¹⁷¹⁸
- Engage in frequent dialogue with corporations to clarify, educate, design, and keep regulation at the same pace as technology advances.¹⁹
- Require that search engines are transparent and fair in their indexing and presentation of results so that only minimal personal information about searches is collected and kept, and that filtering is not imposed on searches.²⁰
- Develop as a multi-stakeholder process best practice guidelines for the development of effective, competitive, decentralized network infrastructure.

Steps States can take on the international level

- Supporting non-political, multi-stakeholder internet regulatory bodies to oversee internet governance on the national level.²¹ While not without its flaws, this model has been effective on the supranational level in the form of the Internet Corporation for Assigned Names and Numbers (ICANN).²² Bolstering and more seriously engaging with existing international bodies that promote digital rights, such as the Internet Governance Forum.²³
- Resist efforts to transfer regulatory authority for the internet away from ICANN to a highly politicized new UN body that would have less latitude to act and with far fewer stakeholders represented, as India, Brazil, and South Africa (IBSA) are currently proposing to do.²⁴
- Utilize the General Assembly, the Human Rights Council, and other organs of the international human rights system to promote digital rights. For example, as part of its Universal Periodic Reviews of all UN member states, the UN Human Rights Council should include clear analysis and recommendations on Internet freedom and utilize more broadly the Special Procedures mechanism.

Steps States can take in their interactions with other States

¹² The publication of this information would, for example, allow the world to gain a better understanding of which countries have the right to compel corporations operating in their jurisdiction to shut down the internet.

¹³ <http://www.washingtontimes.com/news/2009/apr/13/europe39s-telecoms-aid-with-spy-tech/?page=1>

¹⁴ <http://www.zdnet.com/blog/sustainability/nokia-siemens-networks-respond-to-iran-human-rights-abuses-claims/1351>

¹⁵ <http://www.freepress.net/press-release/2011/1/28/questions-raised-about-us-firms-role-egypt-internet-crackdown>

¹⁶ <http://www.business-humanrights.org/Documents/RuggieHRC2008>

¹⁷ Among other examples, the Johannesburg Securities Exchange mandates sustainability reporting, as does France's law on new economic regulations.

¹⁸ "Guidelines for external reporting by Swedish State-owned companies", adopted 29 November 2007, available at <http://www.sweden.gov.se/sb/d/8194/a/93506>; and "Instructing opinions about central State-owned enterprises fulfilling social responsibility", issued by China's State-owned Asset Supervision and Administration Commission of the State Council, 4 January 2008.

¹⁹ For more info see: http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf

²⁰ Adapted from: <http://www.article19.org/pdfs/press/council-of-europe-ensure-free-expression-in-search-engines-and-social-network.pdf>

²¹ <http://www.wgig.org/docs/book/Waudo-Siganga.html>

²² <http://icann.org/>

²³ <http://www.intgovforum.org/cms/>

²⁴ For more information, see www.un.int/india/2010/IBSA%20STATEMENT.pdf

- Respond to other countries attempts to cut off internet access with swift condemnation and clearly enunciated consequences, including, but not limited to, economic and trade sanctions, the conditionality of foreign investment, and active intervention to restore internet connectivity (e.g. via satellite²⁵).
- Query international relationships with other countries according to their adherence to digital rights, and develop a process for considering non-humanitarian aid when internet access to an overwhelming majority of a country is deliberately cut off or throttled.
- Promote, advance, and respect digital rights in trade agreements and demand that trade partners do so as well.
 - A major decision point where countries in the Asia-Pacific Economic Cooperation can and should take a stand on this issue is fast approaching in the form of the upcoming round of negotiations on the Trans-Pacific Partnership Agreement²⁶ in November 2011. During these proceedings, the U.S. government should not seek to further hold online intermediaries based outside of its jurisdiction liable for copyright infringement, as it has done in previous trade agreements.
 - Access further strenuously urges the EU to strike down the Anti-Counterfeiting and Trade Agreement (ACTA) negotiated last year, which would force negotiations on this far-reaching and dangerous treaty to be reopened.²⁷

Steps States can take to promote ICT development and bridge the digital divide

- Give appropriate priority to information communication technologies in national development strategies, in keeping with the Tunis Agenda.²⁸
- Design, develop, and implement information and communication technologies that contribute to sustainable human development and empowerment, including through support and encouragement of the use of free and open source software.
- Bridge the digital divide by providing uniform and affordable access to the internet and education about online tools and information. Special attention should be paid to addressing the needs of persons with disabilities, of poor means, women, children, indigenous peoples, those living in remote or rural areas, and other traditionally socially excluded individuals, as part of a greater goal of protecting a nation's cultural and linguistic diversity online.
- Introduce policies to empower users to fully exploit the economic, social and cultural opportunities and benefits offered by the Internet and ICTs (e.g., remote medicine and online learning) by expanding access to the internet, education about the availability and how to use online information and tools, transfer of technology, and investments in infrastructure.
- Make available government information, which should be released in a timely and accessible, machine-readable manner (e.g., the U.S.'s data.gov initiative²⁹).
- Renew efforts to fulfill commitments made in the Geneva and Tunis phases of the WSIS.³⁰
- Reducing international Internet costs charged by backbone providers, supporting, among other things, the creation and development of regional ICT backbones and Internet Exchange Points to reduce interconnection cost and broaden network access.³¹
- Making, as appropriate, effective use of debt relief mechanisms as outlined in the Geneva Plan of Action, including inter alia debt cancellation and debt swapping, that may be used for financing ICT for development projects, including those within the framework of Poverty Reduction Strategies.³²

²⁵ <http://ahumanright.org/blog/about/>

²⁶ <https://secure.eff.org/site/Advocacy?cmd=display&page=UserAction&id=471>

²⁷ <http://www.edri.org/edriagram/number9.4/us-pushes-acta-european-parliament>

²⁸ <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>

²⁹ <http://www.data.gov/>

³⁰ Paragraph 29 of the 2005 Tunis Agenda, available at: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>

³¹ Paragraph 27 of the Tunis Agenda, available at: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>

³² Paragraph 27 of the Tunis Agenda, available at: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>

- Build centers of expertise and other institutions to facilitate know-how transfer and exchange of best practices, in order to enhance the participation of developing countries and all stakeholders in Internet governance mechanisms.³³

While this list of principles of digital rights and internet governance intentionally sought to be comprehensive, undoubtedly there are ways in which States can protect, respect, and fulfill human rights online which have been overlooked. Moreover, as the internet and the information society along with it develops, new principles will almost certainly be needed as well. That said, the recommendations contained in this brief are a good basis upon which States can begin to build national and international frameworks and legislation for the protection of digital rights. Other actors, namely civil society organizations and corporations, should work with States to implement these policies and assess individual nations on their progress in doing so.

Furthermore, States should adopt these recommendations not just because they are critical to their obligation to protect, respect, and fulfill human rights, but also because doing so will leave States and their citizens behind in the global information economy. Failure to uphold these rights will result in a poorly developed information nation that is likely to miss out on the social and economic benefits of a global information economy.

Decisions being made in the next five years are fundamentally going to shape the trajectory of our collective future; if our digital rights are to be protected, States must act decisively now.

Access is a global movement premised on the belief that political participation and the realization of human rights in the 21st century is increasingly dependent on access to the internet and other forms of technology. For more information, please visit www.accessnow.org or e-mail info@accessnow.org



Navigating Troubled Online Waters After Egypt by [AccessNow](http://www.accessnow.org) is licensed under a [Creative Commons Attribution 3.0 Unported License](http://creativecommons.org/licenses/by/3.0/).

³³ Excerpted from Paragraph 51 of the 2005 Tunis Agenda, available at: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>