

**The Internet Openness Metric Project:**  
**Susan Ariel Aaronson, GWU**  
**Rod Abouharb, University College London**  
**And other organizations**  
**Contact: [saaronso@gwu.edu](mailto:saaronso@gwu.edu)**

**Overview:**

When you go online in Beijing, Brooklyn or Beirut, the web looks and feels different. Most of us think that's fine: the Internet should reflect a country's economic, social, and political culture. However, to some extent, the web looks different because it *is* different. Some countries restrict their citizens' Internet access more than others. The Internet Openness Measurement Project attempts to measure Internet freedom (*how you experience the web*) and Internet openness (*how governments, business and netizens shape the web*) around the world.

**Internet freedom** is a component of Internet openness; it can be defined as the promotion, protection and enjoyment of human rights on the Internet. In contrast, **Internet openness** can be defined as a broader swath of policies and procedures (including those ensuring human rights and those promoting economic activity) that allow netizens to make their own choices about applications and services to use and decide which lawful content they want to access, create, or share with others.

*This proposal attempts to define the components of Internet openness and to develop a multidimensional metric that accurately describes Internet freedom and openness focusing both on human rights and on the regulatory context in which the Internet functions.<sup>1</sup> The metric would be built on new and existing data. Such a metric would include the components of Internet freedom as delineated by the UN Special Rapporteur, Frank LaRue, on the promotion and protection of the right to freedom of opinion and expression.<sup>2</sup> This metric would emphasize a broader vision of relevant human rights commitments and include information related to the larger regulatory context that makes provision and access to the Internet workable. It would also accommodate different ideas about the appropriate role of the state online.<sup>3</sup>*

**Utility of the Metric:**

We believe such a metric would be extremely useful to policymakers, consumers, and activists. It would:

- Give gravitas and rigor to the concept of Internet openness.
- Allow policymakers and activists a tool to measure and compare state policies and status in achieving Internet openness.
- Provide policymakers with a quantitative tool to assess whether their policies to achieve Internet openness in other countries (through policies such as capacity building or sanctions etc.) are effective and lead to change over time in both governance performance (supply side) and citizen realization of rights (demand side).
- Complement existing efforts funded by governments, businesses, and other entities to measure Internet filtering or advance Internet freedom online.
- Encourage governments and international organizations to develop further data.

It may also be helpful to activists, policymakers and scholars who seek greater understanding of:

- The indivisibility of human rights.
- The relationship of international law both online and offline.<sup>4</sup>



#### **Strategy for the Metric:**

**We are seeking comments on our development of the metric from the broad public. Please comment on the proposed metric components.**

Some of the components of this metric are widely available through existing human rights and development statistics prepared by widely respected entities such as the World Bank, UNCTAD, the Web Index, Freedom House, the CIRI Human Rights Data Project, and Global Integrity. However, some of these sources do not cover all countries for all years. Those starred\* have existing datasets. It is important to note that there are no widely accepted data sets for the non-starred components, and thus, we would need to generate or work with others to generate data for these components. In general, available metrics cover conditions in the country as a whole for freedom of expression or ability to organize, and do not focus on online conditions specifically. However, this strategy accords with the July 12 UN Human Rights Council resolution, which affirmed that “people have the same rights online as they do offline and those rights are applicable regardless of frontiers.”<sup>5</sup>

#### **Components of the Metric:**

The Internet freedom component of the metric will be comprised of the applicable human rights covenants under the UDHR (Universal Declaration of Human Rights)

1. Access to information is part of Art.19<sup>6</sup>
2. Freedom of expression (speech) Art. 19
3. Ability to organize\* Art. 20
4. Protecting IPR online without unduly restricting access to information\* Art 27.2
5. Protecting privacy online. Art 12<sup>7</sup>

6. Protecting personal integrity rights off and online (governments do not monitor and then arbitrarily arrest citizens using the Internet).\* Art.3
7. Due process rights online (citizens will be duly informed of Internet policies and have the right to challenge these policies) \*Art 8, 10, 11
8. Digital literacy (as a component of literacy) Art 26
9. Free access to Internet through public venues such as libraries or schools Art.21.2
10. Recognizing and realizing the rights of everyone to enjoy the benefits of scientific progress and its applications Art. 15 IESCR<sup>8</sup>

Economic and business conditions:

1. Role of foreign and domestic firms in maintaining Internet openness<sup>9</sup>
2. Commitments to maintain free flow of information in bilateral FTAs and international economic principles such as those put forward by the OECD.
3. Does the government encourage firms to act in accordance with international laws and guidelines regarding transparency and respect for human rights?<sup>10</sup>
4. Respect for other countries' cyber companies, territory, and products.<sup>11</sup>
5. The state has taken activities to regulate the behavior of nonstate actors that may violate another nation's cyber assets.
6. Role of Internet in increasing access to markets<sup>12</sup>
7. Does the State have copyright laws that enhance or restrict Internet freedom including exceptions for fair use, educational purposes, parody etc...?
8. Does the state require firms to be transparent about cyber incidents so consumers can protect their identities and products online?<sup>13</sup>
9. Does the state use online tools to spy on its citizens and if so under what legal provisions?
10. Does the state have the right to disconnect citizens from the Internet and for what reasons?

Government commitment:

1. Has the government signed the Declaration for Free expression on Internet?
2. Is the government a member of the Open Government Partnership?
3. Does the government have cyber security legislation that respects property and privacy rights?<sup>14</sup>
4. Does the government have procedures for due process when it asks companies or individuals to take down sites for copyright violations or for national security reasons?<sup>15</sup>
5. Under national law does the government have the authority to filter or regulate the Internet? Does the law strictly limit when and how governments can censor?
6. Is the state transparent about when it asks or acts to block or filter online?

**HELP AND ADVICE WANTED!!!!**

**What are we missing?**

## Endnotes:

<sup>1</sup>Scott Wallsten, "Regulation and Internet Use in Developing countries," World Bank Policy Research Working Paper No. 2979, 12/2002, [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=366100](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=366100), p. 7; Ministry of Foreign Affairs of the Netherlands, "Background Paper: The Role of Governments in Protecting and Furthering Internet Freedom," 2011, [http://www.minbuza.nl/binaries/content/assets/minbuza/en/the\\_ministry/the\\_role\\_of\\_governments\\_in\\_protecting\\_internet\\_freedom---freedom-online.pdf](http://www.minbuza.nl/binaries/content/assets/minbuza/en/the_ministry/the_role_of_governments_in_protecting_internet_freedom---freedom-online.pdf); and UN General Assembly Conference Secretariat, "The Digital Economy: Integrating the LDCs Into the Digital Economy," A/Conf.19/L.15, 19 May 2001; and Internet Governance Forum, TS Workshop 182: Global Internet Related Public Policies: Is there an Institutional Gap? 9/2011, <http://www.intgovforum.org/cms/component/content/article/71-transcripts-/919-ts-workshop-182-global-Internet-related-public-policies-is-there-an-institutional-gap>

<sup>2</sup> 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. La Rue stresses that governments should not block access to the Internet. "States should consult with all segments of society to make the Internet widely available, accessible and affordable to all."

<sup>3</sup> Here we refer to the governments that actively provide public goods such as education and public health services online rather than governments that want to safeguard and control their Internet such as China and Russia.

<sup>4</sup> Harold Koh, "International Law in Cyberspace," 9/18/2012, <http://www.state.gov/s/l/releases/remarks/197924.htm>

<sup>5</sup> UN Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet," 6/29/2012, A/HRC/20/L.13

<sup>6</sup> There is no right to information per se in the UDHR. However, information is a global public good; access to information is a basic human right under international human rights law, and hence governments have responsibility to ensure their citizens have access to information through transparency mechanisms. In fact, in the first session of the UN General Assembly member states agreed, "Freedom of information is a fundamental human right and ... the touchstone of all the freedoms to which the United Nations is consecrated. Inge Kaul, Isabelle Grunberg, and Marc A. Stern, Eds.. Global Public Goods: International Cooperation in the 21<sup>st</sup> century (NY, Oxford University Press, 1999) [http://web.undp.org/globalpublicgoods/Executive\\_Summary/executive\\_summary.html#introduction](http://web.undp.org/globalpublicgoods/Executive_Summary/executive_summary.html#introduction); Keith E. Maskus and Jerome H. Reichman, eds. INTERNATIONAL PUBLIC GOODS AND TRANSFER OF TECHNOLOGY: UNDER A GLOBALIZED INTELLECTUAL PROPERTY REGIME, Cambridge, UK: Cambridge University Press, 2005; and Toby Mendel, Freedom of Information as an Internationally Protected Human Right, <http://www.article19.org/data/files/pdfs/publications/foi-as-an-international-right.pdf>.

<sup>7</sup> EDRI, "An introduction to Data Protection," [http://www.edri.org/files/paper06\\_datap.pdf](http://www.edri.org/files/paper06_datap.pdf); and <https://www.accessnow.org/blog/2013/01/28/happy-data-privacy-day>.

<sup>8</sup> States are required to recognize the right of everyone to enjoy the benefits of scientific progress and its applications, to conserve, develop and diffuse science, respect the freedom indispensable for scientific research. AAAS, Scientific Responsibility, Human Rights and Law Program, Science as a Human Rights: "Article 15," [shr.aas.org/programs/program\\_article15.htm](http://shr.aas.org/programs/program_article15.htm). Individuals need the free flow of information to enjoy the benefits of scientific progress, as in Google's global science fair.

[https://www.google-sciencefair.com/en/2013/?utm\\_medium=hpp&utm\\_source=en-hpp&utm\\_campaign=gsf2013](https://www.google-sciencefair.com/en/2013/?utm_medium=hpp&utm_source=en-hpp&utm_campaign=gsf2013)

<sup>9</sup> For example, it could be hard to measure but what happens when Twitter or Facebook shut an account? Jeffrey Gettleman, "Somalia: Twitter Shuts Rebels Account," New York Times, 1/26/2012.

<sup>10</sup> As example, the role of telecom companies in providing access to the web.

<https://www.accessnow.org/blog/2013/01/30/telco-hall-of-shame-france-telecom-orange>; and

<https://www.accessnow.org/blog/2013/01/29/hall-of-shame-vodafone>

<sup>11</sup> As an example of the lack of respect, see Adam Segal, "The People's Republic of Hacking," 1/31/2013.

[http://www.foreignpolicy.com/articles/2013/01/31/the\\_people\\_s\\_republic\\_of\\_hacking\\_china\\_new\\_york\\_times?wp\\_login\\_redirect=0&utm\\_source=Sinocism+Newsletter&utm\\_campaign=9f534ce581-Sinocism02\\_01\\_13&utm\\_medium=email](http://www.foreignpolicy.com/articles/2013/01/31/the_people_s_republic_of_hacking_china_new_york_times?wp_login_redirect=0&utm_source=Sinocism+Newsletter&utm_campaign=9f534ce581-Sinocism02_01_13&utm_medium=email).

Also see Akamai, "The State of the Internet," Vo.. 5, No. 3, 3<sup>rd</sup> quarter 2012 Executive summary,

[http://www.akamai.com/dl/akamai/akamai\\_soti\\_q312\\_exec\\_summary.pdf](http://www.akamai.com/dl/akamai/akamai_soti_q312_exec_summary.pdf). "During the third quarter of 2012, Akamai observed attack traffic originating from 180 unique countries/regions. China remained far and away the top traffic

source, responsible for nearly a third of observed attack traffic. The United States and Russia held the second and third place spots respectively, accounting for just below 18% of observed attack traffic combined.”

<sup>12</sup> Andreas Lendle et al., “There Goes Gravity, How eBay reduces trade costs,”

[Hhttp://econ.worldbank.org/external/default/main?pagePK=64165259&piPK=64165421&theSitePK=469372&menuPK=64166093&entityID=000158349\\_20121025161729](http://econ.worldbank.org/external/default/main?pagePK=64165259&piPK=64165421&theSitePK=469372&menuPK=64166093&entityID=000158349_20121025161729)

<sup>13</sup> See SEC rules on disclosure of cyber incidents, <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>

<sup>14</sup> As example firms struggle to balance their users’ privacy rights with government need to protect the public. Facebook and the three largest email providers told The Hill this week that they require police to obtain a search warrant before accessing their users’ private online communications. Their policies go beyond the privacy standards of the Electronic Communications Privacy Act (ECPA), a 1986 law that only requires police to obtain a subpoena, issued without a judge’s approval, to read emails, instant messages and other forms of digital communication that have been opened or that are more than 180 days old. See Brendan Sasso, “Facebook, email providers say they require warrants,” 1/27/2012, <http://thehill.com/blogs/hillicon-valley/technology/279441-facebook-email-providers-require-warrant-for-private-data>

<sup>15</sup> Twitter recently announced the number of USG requests for user account data. The USG comprised 81% of the data requested. David Kravetz, “Government Appetite Growing for Twitter User Data,” *Wired*, 1/28/13, <http://www.wired.com/threatlevel/category/surveillance/>