April 1, 2014

Office of the High Commissioner for Human Rights
United Nations Office at Geneva, CH-11
1211 Geneva, 10
Switzerland

Global Network Initiative

Protecting and Advancing
Freedom of Expresssion and
Privacy in Information and
Communications Technologies

Global Network Initiative
Submission on "The right to privacy in the digital age"

The Global Network Initiative welcomes the opportunity to provide input for the report of the United Nations High Commissioner for Human Rights being prepared as requested in General Assembly Resolution 68/167 entitled "The right to privacy in the digital age." This submission expands on GNI's February 24 letter to the High Commissioner on this topic.[1]

GNI brings together ICT companies with civil society organizations, investors, and academics to forge a common approach to protecting and advancing free expression and privacy online. GNI has developed a set of principles and implementation guidelines to guide responsible company, government and civil society action when facing requests from governments around the world that could impact the freedom of expression and privacy rights of users.

This submission offers specific recommendations to inform the High Commissioner's report based on the experience and perspectives of GNI's multi-stakeholder membership. We recommend the report include the following specific points:

- Bulk collection of communications data—both content and metadata—threatens privacy and freedom of expression rights.
- Rather than bulk collection, government surveillance should be particularized, with independent judicial oversight.
- Governments that exercise "virtual control" over the digital communications of foreigners have an obligation to respect their privacy rights under the International Covenant on Civil and political Rights (ICCPR).
- The GNI principles and guidelines provide specific measures that can be taken by companies to respect privacy and free expression rights when facing requests by governments for access to data.
- Increased transparency by governments and companies is a key building block to ensure that communications surveillance regimes are consistent with human rights standards.
- Governments and companies should be as specific as possible with their users and the general public about the legal limitations on disclosing surveillance practices.
- Governments should commit to more specific areas of increased transparency based on consultation with other stakeholders.

[1] "GNI Writes to UN High Commissioner for Human Rights on Privacy in the Digital Age," February 24, 2014, available at http://globalnetworkinitiative.org/news/gni-writes-un-high-commissioner-human-rights-privacy-digital-age.

Human rights and the rule of law

GNI's Principles on Freedom of Expression and Privacy are rooted in international human rights laws and standards, while also recognizing that companies are compelled to obey domestic law in countries where they operate.

GNI does not underestimate the challenge governments face in finding the appropriate balance between security and privacy and free expression. But international human rights standards set out narrowly defined circumstances under which governments may restrict the rights to free expression and privacy.[2]

Digital communications provide new opportunities, and demand new levels of responsibility from governments

The Internet is a network-of-networks, much of which is built and operated by the private sector, while other parts are partially or entirely state-owned. Via the Internet, vast and ever increasing quantities of digital communications flow across borders and around the world in microseconds.

The U.S. government and private industry have played a critical role in the development of the Internet. Due to these historic factors, a significant proportion of global Internet traffic continues to flow through the United States, as well as through submarine telecommunications cables connecting to the United Kingdom. Services provided by a number of US-based companies, including members of GNI, are used by billions of users located all around the world.

All governments engage in communications surveillance for foreign intelligence purposes to some degree, but the degree of control that the U.S. is able to exert over global communications providers and the access it has to global communications traffic means that the U.S. is now the focus of global attention on this issue. Revelations regarding digital communications surveillance have focused on both the upstream bulk collection of communications content and metadata from fiber optic cables, as well as downstream requests made of Internet and communications providers, including under the Foreign Intelligence Surveillance Act (FISA). Technological advancements mean that is easier than ever to collect, analyze, and store communications data at scale, increasing concerns about the potential misuse of such practices.

The High Commissioner's report should state that bulk collection of communications data —both content and metadata—threatens privacy and freedom of expression rights and undermines trust in the security of electronic communications services provided by companies. This includes bulk collection by governments, and mandates to companies or other third parties to store data that they would otherwise not retain in order to facilitate government access.

---

[2] Guidance on these circumstances can be found in Articles 17 and 19 of the ICCPR. See also General Comment 16 of the Human Rights Committee; and UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression, Frank La Rue, U.N. Doc A/HRC/23/40, April 17, 2013, available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement. See also the 2012 report commissioned by GNI on this issue: Ian Brown and Douwe Korff, "Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online," June 2012, available at http://globalnetworkinitiative.org/content/digital-freedoms-international-law-0.

Such practices are incompatible with the principles of necessity and proportionality that the legal frameworks for communications surveillance must meet to ensure they are consistent with human rights standards. Reports that the UK intelligence agency, GCHQ, has intercepted millions of Yahoo! webcam images provide a particularly compelling example of the urgent need to end bulk collection practices.[3]

Rather than engaging in bulk collection, government surveillance programs should be particularized and based on individual suspicion, with independent judicial oversight that is adequately informed.[4]

Furthermore, communications surveillance programs that involve bulk collection and are premised on distinguishing nationals from foreigners for increased privacy protections are unlikely to be effective. Invariably, bulk collection will sweep up the communications of nationals using foreign services (e.g. a national traveling abroad using an international network or service). These practical considerations buttress our view that international human rights laws set standards that must protect the freedom of expression and privacy rights of users from all countries.

GNI has urged the United States to recognize the right to privacy of non-U.S. persons and to strengthen reforms to effectively protect this right. When governments exercise "virtual control" over the digital communications of foreigners, such control should entail an obligation to respect their privacy rights under the ICCPR, and we recommend that the High Commissioner's report endorse this view.[5] This is consistent with the recent concluding remarks of the Human Rights Committee on the Universal Periodic Review of the United States, which noted that under Article 17 of the ICCPR "measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance."[6]

The role of the private sector

The UN Guiding Principles on Business and Human Rights define the respective roles of the public and private sector as the state duty to protect and the corporate responsibility to respect human rights. Companies should engage in human rights due diligence to "know and show" that they are addressing potential human rights impacts. The GNI Principles provide focused guidance on how ICT companies can respond to government

---

[3] Spencer Ackerman and James Ball, "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ," *The Guardian*, February 27, 2014, available at http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

[4] This recommendation reflects the consensus of company and civil society recommendations for surveilance reform. See CDT, "Common Ground Between Company and Civil Society Surveillance Reform Principles," January 15, 2014, available at https://www.cdt.org/files/pdfs/common-ground-surveillance-principles.pdf.

[5] For example, see Peter Marguiles, "The NSA in Global Perspective: Surveillance, Human Rights, and Counterterrorism," Fordham Law Review (forthcoming), available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2383976.

[6] Human Rights Committee, "Concluding observations on the fourth report of the United States of America," Advance Unedited Version, para. 22, available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en.

requests implicating privacy in ways that respect the rights of users. And a process of independent assessment of company implementation of their GNI commitments provides accountability.

We recommend that the High Commissioner's use the GNI principles and guidelines as examples of specific measures that can be taken by companies to respect privacy and free expression rights when facing requests by governments for access to data.

GNI's principles and guidelines specify a set of steps that companies can take to respect and protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards.[7] In particular, companies should:

- Narrowly interpret and implement government demands that compromise privacy.
- Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy.
- Request clear communications, preferably in writing, that explains the legal basis for government demands for personal information including the name of the requesting government entity and the name, title and signature of the authorized official.
- Require that governments follow established domestic legal processes when they are seeking access to personal information.
- Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that Country.
- Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.

The first assessments of our founding companies Google, Microsoft, and Yahoo have pointed to the difficulties that can arise when governments impose secrecy requirements on companies who receive national security surveillance requests, limiting their ability to be transparent about the steps they take to minimize risks to the privacy of their users.[8] When companies are legally barred from disclosing whether or not they have been subject to national security surveillance demands, it is not possible to independently assess how a company responds, and to show how it is respecting users' rights.

---

[7] See the GNI Implementation Guidelines, including application guidance, available at http://globalnetworkinitiative.org/implementationguidelines/index.php.

[8] See GNI's Public Report on the Independent Assessments of Google, Microsoft, and Yahoo, available at http://globalnetworkinitiative.org/content/public-report-independent-assessment-process-google-microsoft-and-yahoo.

Even when they are legally barred from disclosing government demands, companies can take action, consistent with the GNI Principles, to press for reform.

In 2013, Yahoo filed a motion requesting the declassification and release of opinions related to its formerly classified 2008 challenge and subsequent appeal of a FISA directive in the FISA Court (FISC) and the FISA Court of Review. The 2008 challenge and appeal was the one instance in which a non-governmental party substantively contested a directive from the government under FISA in the FISC. In addition GNI members and other companies have filed legal challenges with the U.S. Government seeking the right to share data with the public on the number of FISA requests they receive, which have contributed to the significant, although insufficient, reforms described below.

GNI's Principles state: "Individually and collectively, participants will engage governments and international institutions to promote the rule of law and the adoption of laws, policies and practices that protect, respect and fulfill freedom of expression and privacy." Consistent with this principle, companies have also publicly supported legislative reform efforts in the United States. In December 2013, the GNI members joined with other Internet companies to issue principles on Global Government Surveillance Reform, urging changes to practices and laws regulating government surveillance of individuals and access to their information.[9]

Transparency and the responsibilities of governments and companies

Transparency reforms are a necessary first steps in examining whether domestic laws adequately protect rights to privacy and freedom of expression. The High Commissioner's report should identify increased transparency by governments and companies as a key building block to ensure that communications surveillance regimes are consistent with human rights standards.[10]

In September 2013, GNI wrote to the 21 governments in the Freedom Online Coalition, asking them to report on the requests they make for electronic communications surveillance and to make it legally possible for companies to report regularly to the public on the government requests that they receive from law enforcement as well as national security authorities. GNI has held productive dialogue with leading members of the Coalition, has received multiple responses from individual governments, and is encouraged that the Coalition is considering adopting important recommendations before its next meeting in Estonia on April 28-29, 2014, regarding commitments to a principled approach to electronic surveillance, including increased transparency.

In the United States, the government announced it would allow companies to publicly report more information about national security requests for user data.[11] These reforms, which allow companies to report details about national security requests in bands of

[9] See http://reformgovernmentsurveillance.com/.
[10] La Rue, para. 91.
[11] See Craig Timberg and Adam Goldman, "U.S. to allow companies to disclose more details on government requests for data," *Washington Post*, January 27, 2014, available at http://www.washingtonpost.com/business/technology/us-to-allow-companies-to-disclose-more-details-on-government-requests-for-data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html.

either 250 or 1,000, are an important step forward but fall short of what is needed to allow companies to be transparent with their users. GNI continues to urge legal and policy reforms that would enable more granular reporting.

GNI is particularly concerned that even governments committed to human rights online can be overly broad in their assertions of nondisclosure requirements for national security purposes. For example, the Government of Canada told GNI: "concerning public reporting by telecommunications service providers, the *Criminal Code* prohibits them from publicly reporting on interceptions in order to ensure that our investigative capabilities are not exploited by criminals. For example, publishing figures about services with any indication of volume could cause criminals and terrorists to switch their means of communication to avoid detection."[12]

The obligation of governments to provide security and law enforcement is one that GNI acknowledges and takes seriously. However, many companies already report without harm in this manner on requests they receive related to criminal investigations, and the progress toward reporting on national security requests in the United States makes clear that there is more that both governments and companies can say about interception requests without endangering national security. The release of transparency reports by Internet companies, telecommunications companies, and cable ISPs in recent months is a welcome development that should be encouraged internationally (see appendix for a list of companies reporting on government requests for user data).

Where governments assert that the law prohibits companies from making disclosures about communications surveillance, it is important that both governments and companies be as specific as possible with their users and the general public about the legal limitations. The stand taken recently by Vodafone is instructive in this regard: "Where it is not lawful for us to disclose we will say so and we will say what provisions of law apply."[13]

The Global Principles on National Security and the Right to Information (Tshwane Principles) offer useful guidance relating to government authority to withold information on national security grounds, that should inform this debate at the national and international level.[14]

Given the trend toward broad commitments by governments to increase transparency regarding surveillance practices, we recommend that governments commit to more specific areas of increased transparency based on consultation with other stakeholders.[15]

---

[12] Letter to GNI from Steven Blaney, P.C., M.P., Minister of Public Safety and Emergency Preparedness, Canada dated February 20, 2014.
[13] Quoted in Juliette Garside, "Vodafone takes a stand on privacy with plan to disclose wiretapping demands," *The Guardian*, January 15, 2014, available at http://www.theguardian.com/business/2014/jan/15/vodafone-aims-to-disclose-wiretap-demands.
[14] Available at http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.
[15] For more information, see Chris Tuppen, "Opening the Lines: A Call for Transparency from Governments and Telecommunications Companies" available at http://globalnetworkinitiative.org/content/opening-lines-call-transparency-governments-and-telecommunications-companies.

In particular:

- Ensure that laws authorizing surveillance are public, clear, specific, that their application is foreseeable, and that official legal interpretations of the law are published, with deletions as necessary.
- Establish adequate independent oversight mechanisms to ensure that government reports on surveillance activities are accurate and complete.
- Compel the competent authorities to disclose the information about:
    - Which intelligence agencies/bodies are legally permitted to conduct surveillance;
    - The scope of the powers of each of those entities;
    - The process by which an intelligence agency/body is assigned these powers;
    - The judicial, ministerial, independent, or other oversight mechanisms through which redress for unlawful surveillance may be pursued.
- Compel the competent authorities to disclose information about the surveillance demands they make, collectively, on companies, including:
    - The number and nature of surveillance demands;
    - The number of user accounts affected by those demands;
    - The specific legal authority for each of those demands; and
    - Whether the demand sought communications content or non-content.
- Permit companies to disclose, with the level of detail set out above, information on surveillance demands that they receive on at least an annual basis.
- Permit companies to disclose technical requirements for surveillance that they are legally bound to install, implement, and comply with.

Next steps at the international level

GNI appreciates the inclusive process of consultation and engagement to inform the development of the High Commissioner's report. There have been a plethora of high-level commissions, panels, and gatherings seeking to address Internet governance following the national security surveillance revelations of 2013, but none possess the global legitimacy of the UN General Assembly and Human Rights Council.

We urge the High Commissioner to continue to consult both with governments—particularly the intelligence and security agencies that conduct surveillance—as well as a wide array of non-governmental voices, including civil society and the private sector, and to maintain a sustained focus on these issues.

In order to do so most effectively, and given the urgency and complexity of this topic, we recommend that a Special Rapporteur on the right to privacy in the digital age be established with a mandate to address this issue holistically. Although Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, and on the promotion and protection of human rights while countering terrorism, Ben Emmerson, have addressed these issues in reports and briefings, the gravity and pervasiveness of concerns regarding this issue demand sustained attention at the global level. Reporting by a special rapporteur on privacy could highlight specific areas of concern and best practices at the national level and help lay the groundwork for future international action on this topic.

Appendix – Company Transparency Reports

Apple
https://ssl.apple.com/pr/pdf/131105reportongovinforequests3.pdf
https://ssl.apple.com/pr/pdf/140127upd_nat_sec_and_law_enf_orders.pdf

AT&T
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html

Comcast
http://corporate.comcast.com/comcast-voices/comcast-issues-first-transparency-report

Credo
http://www.credomobile.com/misc/transparency.aspx

Dropbox
https://www.dropbox.com/transparency

Facebook
https://www.facebook.com/about/government_requests

Google
https://www.google.com/transparencyreport/

LinkedIn
http://help.linkedin.com/app/answers/detail/a_id/41878/ft/eng
http://help.linkedin.com/app/answers/detail/a_id/21733/related/1

Microsoft
http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

Time Warner Cable
http://help.twcable.com/privacy-safety.html

Tumblr
http://transparency.tumblr.com/

Twitter
https://transparency.twitter.com/

Verizon
http://transparency.verizon.com/

Yahoo
https://transparency.yahoo.com/