Global Network Initiative

Evidence for Investigatory Powers Review

Date: October 2014

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

Summary

The Global Network Initiative (GNI) welcomes the opportunity to provide written evidence for the UK Government Review of Communications and Interception Powers. GNI has previously provided evidence to the Joint Committee on the Draft Communications Data Bill and written to the UK Prime Minister concerning the Data Retention and Investigatory Powers Act (DRIPA 2014).[1]

Specifically, we recommend that the UK government:

- Develop reform proposals for lawful interception and communications data that would serve as a worthy model for other countries to adopt, mindful that policy and legislation in the UK is often emulated by governments in the Commonwealth and around the world.
- Halt the bulk collection of content and communications data from providers, and bring all data collection programmes, for law enforcement and national security purposes, under the auspices of an independent oversight regime.
- Prioritize Mutual Legal Assistance Treaty (MLAT) reforms to manage challenges around cross-border data requests, rather than asserting extraterritorial jurisdiction over data controlled outside the UK.
- Adopt a robust set of transparency provisions that enable public understanding of the scope of interception and communications data powers, policies, and practices.
- Broadly consult with industry, civil society organizations, and other key stakeholders to aid in the development of policy options for public debate, informed by human rights impact assessments.

About GNI

GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics, working to protect and advance freedom of expression and privacy in the Information Communications and Technology (ICT) sector.[2] GNI has developed a set of Principles and Implementation Guidelines, based on international human

[1] GNI Comments on UK Draft Communications Data Bill, September 2012, available at https://globalnetworkinitiative.org/news/gni-comments-uk-draft-communications-data-bill;

[2] The current list of GNI participants is available at https://globalnetworkinitiative.org/participants/index.php.

rights standards, to guide responsible company action when facing requests from governments around the world that could adversely affect the freedom of expression and privacy rights of users.[3]

The UK's leadership role

The UK plays an important leadership role in the promotion of Internet freedom. Through the Freedom Online Coalition (FOC) and other initiatives, the UK has secured resolutions at the UN Human Rights Council recognizing that the same rights that apply offline also apply online. The UK co-chairs the Coalition working group on privacy and transparency, and GNI is engaging as part of this group to work to improve government transparency practices, consistent with the FOC's commitment to: "Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance … while committing ourselves to do the same."[4]

We are concerned about the overly broad scope of UK lawful interception and communications data powers, as well as the marked absence of public consultation around significant policy and legal changes. Paired with the UK's standing and influence on the world stage, this approach is likely to be copied and it gives unintended justification in particular to governments who seek to limit human rights and this could undermine the effectiveness of the UK's efforts to advance freedom online. Other countries planning similar laws are already using the UK's position to validate their own legislative programmes in this area.[5] It is worth stressing the potential human rights abuses that such laws could create in those countries, including to UK citizens.

This review presents a rare opportunity to guide future governments on how to better balance the legitimate needs of law enforcement with international human rights standards, both in the formulation of policy and its execution.

We urge you to develop reform proposals for lawful interception and communications data that would serve as a worthy model for other countries to adopt, mindful that policy and legislation in the UK is often emulated by governments in the Commonwealth and around the world.

The changing global context

It is the duty of a government to protect its citizens and also to respect, protect, promote, and fulfil human rights. This includes ensuring that national laws,

---

[3] GNI Principles and Implementation Guidelines available at https://globalnetworkinitiative.org/corecommitments/index.php.
[4] Available at http://www.freedomonline.ee/foc-recommendations.
[5] ZDNet " Data retention is the way western nations are going: Brandis" July 16, 2014 available at http://www.zdnet.com/au/data-retention-is-the-way-western-nations-are-going-brandis-7000031658.

regulations, and policies are consistent with international human rights laws.[6] Finding the right approach is not easy, particularly in the global, complex, and constantly evolving ICT sector. At the same time, we note that threats, capabilities, and technologies are not the only factors that are evolving with respect to the interception of communications. Huge amounts of data are flowing across borders and being stored in multiple jurisdictions. For example, 100 hours of video are uploaded to YouTube every minute, double the rate from 2011.[7] Technological advancements mean that it is easier than ever to collect, analyse, and store communications data at scale, but also increasing the human rights risks in the event of the misuse of such practices.[8]

A 2014 BBC poll of 17 countries around the world found that 52% of citizens do not believe that "the internet is a safe place to express my opinions." In the UK, more than one in three respondents (38%) did not believe they were free from government surveillance.[9]

Meanwhile, public perceptions of the relationship between the government and private sector companies who often host their personal data have evolved considerably in recent years, particularly in the wake of the Edward Snowden disclosures. Beyond undermining user confidence in their freedom to express their views and maintain privacy, the extensive surveillance practices revealed in the last few years have done serious economic damage to the Internet and broader economy.[10]

Compounding these problems, governments around the world have sought to use the Snowden revelations to exert greater control over online communications in their territory and beyond. In some cases this includes mandating communications providers to store data locally, most recently in Russia.[11] In others, governments are asserting extraterritorial jurisdiction over data controlled abroad. At the international level, there are heated debates about

---

[6] 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, 2014, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[7] See YouTube statistics available at https://www.youtube.com/yt/press/statistics.html and http://youtube-global.blogspot.jp/2011/05/thanks-youtube-community-for-two-big.html.

[8] Kevin Bankston and Ashkan Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones," Yale Law Journal, January 2014, available at http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

[9] BBC World Service Poll, 31 March 2014, available at http://downloads.bbc.co.uk/mediacentre/bbc-freedom-poll-2014.pdf.

[10] Danielle Kehl with Kevin Bankston and Robert Morgus, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cybersecurity," New America Foundation Open Technology Initiative, July 2014, available at http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf.

[11] See Moscow Times, "Russia Asks Facebook, Google, Twitter to Comply with Law on Data Storage," 26 September 2014, available at http://www.themoscowtimes.com/news/article/russia-demands-facebook-google-and-twitter-comply-with-law-on-data-storage/507852.html.

the future of Internet governance, a topic that will next be on the agenda at the 2014 ITU Plenipotentiary Conference. In these debates, authoritarian regimes are seeking to exert a greater degree of control over the Internet.

A wide array of stakeholders have responded to government surveillance revelations by calling for reforms that would bring law enforcement powers and surveillance programs into alignment with international human rights standards. More than 400 civil society organizations, as well as academics and prominent individuals, and elected officials and political parties have endorsed the International Principles on the Application of Human Rights to Communications Surveillance.[12] Major Internet companies formed the Reform Government Surveillance Coalition and have issued their own principles to guide reform efforts.[13] Working together through GNI and in concert with other stakeholders, companies and civil society groups have advanced legislative reform proposals in the United States and succeeded in gaining greater ability to be transparent with the public about the national security requests they receive from the US government.[14]

UK legal framework

In September 2013, GNI wrote to the UK and other members of the Freedom Online Coalition (FOC), expressing concern that "the UK's communications surveillance practices, including both access to communications data as well as the interception of communications content, seriously threaten its reputation as a champion of Internet freedom and undermine your ability to advocate for other governments to support human rights online."[15]

The absence of constitutional constraints makes it particularly important that the UK reflect on how to define appropriate boundaries within law enforcement and surveillance powers should be defined and exercised. The current trend towards broadly worded, all-encompassing powers is particularly concerning.

Most problematic are practices that entail mass surveillance or bulk collection of user data. Mass interception or bulk collection of communications data threatens privacy and freedom of expression rights and undermines trust in the security of electronic communications services. This harm is caused both by direct bulk collection by governments, and by mandates that companies or other third

[12] International Principles on the Application of Human Rights to Communications Surveillance, available at https://en.necessaryandproportionate.org/text.
[13] See https://www.reformgovernmentsurveillance.com/.
[14] See Washington Post "US to allow companies to disclose more details on government requests for data" 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.
[15] GNI Letter to UK government, September 2013.

parties store data they would otherwise not retain in in order to facilitate government access.[16]

The UK government has consistently asserted, "All of GCHQ's work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorized, necessary and proportionate."[17] However, it is difficult to square this statement with the disclosures of programs such as the unauthorised mass collection of webcam images from providers and other programs that are clearly disproportionate, of suspect necessity and for which the legal basis is, at best, unclear.[18]

The use of lawful interception and communications data in the UK is principally but not solely regulated by the Regulation of Investigatory Powers Act 2000 (RIPA). But as the Interception of Communications Commissioner has himself stated, RIPA is "a difficult statute to understand."[19] Serious effort should be given to revising the complex and fragmented oversight regime, so concerned citizens can more easily understand these activities. This is particularly the case with regard to warrants issued under Section 8(4) of RIPA, where the Interception of Communications Commissioner's Office (IOCCO) has raised questions regarding the need for "the possibility of some structural or other consideration."[20]

The UK should halt the bulk collection of content and communications data from providers, and bring all data collection programmes under the auspices of an independent oversight regime.

Extraterritorial assertion of jurisdiction

GNI has observed a troubling legislative trend around the world in which requirements are placed on communications providers to respond to government requests for user data controlled outside that government's jurisdiction. Section 4 of DRIPA 2014 could provide unintended justification for such actions by other governments, including those that actively seek to limit freedom of expression and other human rights online. These provisions may encourage other governments to expand claims of jurisdiction without regard to

[16] As proposed in the 2012 Draft Communications Data Bill, although that bill was not formally introduced in Parliament.
[17] Marc Scott, "British Spy Agencies Assert Power to Intercept Web Traffic," New York Times, 16 June 2014, available at http://www.nytimes.com/2014/06/17/business/international/british-spy-agencies-said-to-assert-broad-power-to-intercept-web-traffic.html.
[18] It is not clear whether this and other GCHQ activities disclosed by Snowden are authorized under RIPA or other statutes. See the Vodafone Law Enforcement Disclosure Report: Legal Annexe for the UK legal powers governing real-time interception, disclosure of communications data, and national security and emergency powers, available at http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf.
[19] The Rt Hon. Sir Anthony May, "2013 Annual Report of the Interception of Communications Commissioner," available at http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf, para 1.6.
[20] Ibid., para 6.6.8.

the physical location of data centres, undermining the rights of UK citizens and the broader international framework for legal assistance.

Rather than asserting extraterritorial jurisdiction directly, the UK government should rely on other means of lawfully obtaining data from other jurisdictions, namely through mutual legal assistance treaties (MLATs). These treaties have not kept pace with the demand for communications and surveillance data, and are in most cases under resourced. The UK National Crime Agency has been a leading proponent of reforms to the MLAT process that would better address individual rights and law enforcement needs. GNI has commissioned a study on MLAT reforms that will be released later this year.

We recommend that the UK prioritize MLAT reforms as a more suitable approach to managing challenges around jurisdiction and cross-border data requests.

Transparency

GNI has urged greater transparency from the UK government regarding communications surveillance. Section 6 of DRIPA 2014 requires half-yearly reports from the Interception of Communications Commissioner's Office (IOCCO). However, an increase in the frequency of reporting alone will not improve the quality and effectiveness of these reports. The Home Office has assured GNI that "the government is wholly committed to ensuring that the use of communications data remains as transparent as possible."[21] Although the IOCCO 2014 report does represent a significant improvement from prior reports, with more information that is more clearly presented, there is much more that should urgently be considered to improve UK transparency.

There are both qualitative and quantitative aspects to transparency that need improvement. Qualitative disclosures include making publicly available the laws and legal interpretations authorizing electronic surveillance or content removal, among other measures listed below. Quantitative disclosures include the reporting of aggregate numbers of requests for user data or content removal, and the number of users impacted by these requests.

As well as making these disclosures themselves, the UK government should permit companies to issue analogous reports. The combination of government and company reporting can help the public understand the scope of surveillance. Under Section 19 of RIPA 2000, data relating to lawful interception warrants cannot be published, which significantly hampers public debate about the scope and scale of communications surveillance.[22]

The consequences of excessive secrecy surrounding data requests are now front-page news, with recent revelations that police have used RIPA to target

[21] Letter from Security Minister James Brokenshire to GNI, 11 November 2013.
[22] Vodafone Law Enforcement Disclosure Report.

journalists and reveal protected sources.[23] GNI welcomes the IOCCO inquiry into this matter, which attests to the importance of robust enforcement and transparency as well as the need for protections to ensure press freedom are incorporated into future reforms.[24]

We recommend that the UK government adopt the following transparency provisions regarding lawful interception and access to communications data:

- Publicly post information on the specific laws that authorize surveillance as well as official legal interpretations of the law, including executive orders, legal opinions that are relied on by executive officials, and court orders.

- Public disclosure of information about:
    - Which intelligence agencies/bodies are legally permitted to conduct surveillance;
    - The scope of the surveillance authorities of each of those entities;
    - The judicial, ministerial, other oversight mechanisms required for the authorization of each instance of surveillance;
    - The judicial, ministerial or independent oversight mechanisms that oversee the implementation of surveillance;
    - The mechanisms for redress that victims of unlawful surveillance may pursue; and
    - The scope of unlawful surveillance and remedial and disciplinary actions taken.n

- Disclose to the victim of unlawful surveillance that unlawful surveillance has taken place as soon as practical, considering the needs of the specific pending investigation.

- Disclose aggregated information about the surveillance demands they make on companies including:
    - The number 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 or both, and how the authorities define these terms.

[23] Nick Kraven, "How police hacked Mail on Sunday phone," Mail on Sunday, 6 October 2014, available at http://www.dailymail.co.uk/news/article-2780809/How-police-hacked-Mail-Sunday-Officers-used-anti-terror-laws-seize-phone-records-identify-source-exposed-Chris-Huhne-s-speeding-points-fraud.html.

[24] "IOCCO Launches Inquiry into the use of RIPA powers to acquire communications data relating to confidential sources of journalists, 6 October 2014," available at http://www.iocco-uk.info/docs/IOCCO%20inquiry%20into%20use%20of%20comms%20data%20to%20identify%20journalistic%20sources.pdf.

- Permit companies to disclose, with the level of detail set out above, aggregated information on number of surveillance demands that they receive and how they respond to them 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 such as requirements to design lawful intercept capability into communications technology and to decrypt encrypted communications.

Consistent with the above recommendations, GNI believes that the declassification of an array of documents by the US government in the wake of the Snowden disclosures and in response to legal challenges by civil liberties organizations offers an instructive model for the UK to consider.[25]

Conclusion

The independent review of the legal framework for communications data and interception provides an opportunity for the UK government to rethink how it approaches policymaking at the intersection of national security and human rights concerns. **Building upon this call for evidence, we recommend a broad process of consultation including industry, civil society organizations, and other key stakeholders to aid in the development of policy options for public debate, informed by human rights impact assessments.** Both the process and the substance of UK policy and legislative review should ensure a rights-based approach worthy of adoption globally.

[25] See http://icontherecord.tumblr.com/tagged/declassified for documents released by the US intelligence community following declassification review and in response to Freedom of Information Act requests.