Submission to the UN Special Rapporteur on freedom of expression – Freedom of expression and the private sector in the digital age, January 2016

Introduction

Privacy International makes this submission in support of the UN Special Rapporteur's initial mapping report on the responsibilities of Information Communication Technologies (ICT) Sector to protect and promote freedom of expression in the digital age.

As the UN Special Rapporteur has previously noted privacy and freedom of expression are interlinked and mutually dependent rights.[1] So, in many aspects, the roles and responsibilities of ICT companies in respecting and promoting the right to freedom of expression on-line affect also the right to privacy.

In this submission Privacy International focuses on four areas where the links between freedom of expression and privacy are particularly strong and where the ICT sector can play a significant role in respecting these rights: the surveillance industry; the responsibility of companies vis-à-vis unlawful surveillance; the role of companies to promote encryption and oppose its weakening; the challenges to companies posed by government equipment interference (hacking).

1. Explore the role of the surveillance industry

As the Special Rapporteur carries out this mapping exercise on the ICT sector, Privacy International suggests that consideration be given to the surveillance industry and the relationship between telecommunications and internet service providers and surveillance technology companies. In relation to surveillance technologies, the link between freedom of expression and the unlawful invasion of someone's privacy can be particularly strong. For example, technologies such as 'packet inspection' that some governments use for censorship of on-line content are also used for surveillance.[2]

---

1 Report of the Special Rapporteur on freedom of expression and opinion, Frank La Rue, 17 April 2013, A/HRC/23/40, at para. 79, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

2 Packet inspection technologies examine the constituent pieces of data that make up internet and communications traffic as they pass inspection points in the internet architecture, searching for signatures that the technologies recognize as abnormal, such as viruses and spam. Packet inspection technologies can also be programmed to search for particular terms, such as key words in emails. For an example, see Privacy International's report, Tipping the scale: surveillance and security in Pakistan, here: https://privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf

However, the responsibilities of the surveillance industry have so far escaped scrutiny in international human rights settings, such as the UN Business Forum on Human Rights, and their responsibilities to respect and promote human rights remain unexplored.

1.1 Surveillance industry

The surveillance industry is comprised of companies that market, sell or otherwise supply to governments technology specially designed for intercepting, storing, and analysing communications and metadata for the purpose of intelligence gathering or law enforcement (they may well have other customers). These technologies include spyware, internet and phone monitoring tools, a range of systems designed for "lawful interception", location monitoring systems, and passive collection systems designed to monitor on a mass scale, sometimes entire populations. It is a fast growing industry. Until quite recently, the private sector played a limited role in providing the surveillance capabilities used by state law enforcement and intelligence agencies. This picture has shifted significantly with the advent of technologies that put the collection and retention of vast amounts of personal data within the budgetary reach of a growing number of governments. Concurrently, a commercial industry has grown up to service governments' desire for ever-increasing surveillance capabilities. The industry has strengthened demand through aggressive marketing to law enforcement and security services across the globe.

Surveillance technologies are used by governments to target political opponents, journalists and lawyers, crack down on dissent, harass human rights defenders, intimidate populations, discourage whistle-blowers, chill expression and destroy the possibility of private life. Privacy International has published reports showing intelligence and law enforcement agencies complicit in human rights violations using surveillance systems in Colombia[3], Morocco[4], Pakistan[5], Uganda[6], and central Asia.[7]

Privacy International has consistently advocated for a range of measures that should be taken by companies within the surveillance industry, including:

- Develop a policy commitment to respect human rights, approved at the most senior level, and made publicly available.
- Carry out due diligence on any potential customers to identify, prevent and mitigate adverse human rights impact prior to agreeing to a potential transaction.
- Stipulate clear end-use assurances in contractual agreements with strong human rights safeguards that prevent against arbitrary or unlawful use of the technology.
- Carry out a periodic review of states' use of the technology, and refuse to carry out maintenance, training, or updates if the end-use does not conform to these contractual obligations.

So far, these and other recommendations have, by and large, been ignored by the companies

3 See https://www.privacyinternational.org/node/640
4 See https://www.privacyinternational.org/node/622
5 See https://www.privacyinternational.org/node/627
6 See https://www.privacyinternational.org/node/656
7 See https://www.privacyinternational.org/node/293

concerned. Most often the companies selling surveillance technologies point the finger at the end users, i.e. governments, for “misuse” of the technologies. However, there are few or no attempts to limit the availability of this intrusive technology or to assess the human rights' implication of its use prior to entering into a commercial relationship with a buyer. Companies merely hoping that an end user will not violate human rights using a product that is designed for surveillance falls short of of the necessary assessments and measures companies should undertaking to ensure they respect human rights.

1.2 Links between surveillance companies and other ICT companies

Surveillance companies do not operate in a vacuum. They sell electronic surveillance solutions directly to governments, and/or to other ICT companies. This is particularly the case for those communications service providers that need to meet their statutory obligations to facilitate access by law enforcement and security agencies to their networks and to their subscribers’ data.

The legal regimes regulating such access vary from country to country, together with the extent of obligations imposed on companies. As the Special Rapporteur has already noted, these regimes have a significant impact on the right to freedom of expression and to privacy.[8]

ICT companies may be required, by law,to physically install on their network components that comply with interception protocols or, alternatively, install external ‘probes’ somewhere along the transmission cables to allow signals carried on their network to be transmitted to monitoring facilities of requesting government agencies.

Certain countries require direct access by law enforcement and intelligence agencies to the communications network. As part of these requirements, the relevant companies may also need to ensure that their networks are directly connected to monitoring centres.

Privacy International has documented the close relationship between some of the service providers and surveillance companies that develops in order to enable these systems to operate in ways that infringe upon the right to privacy.[9]

In some countries service providers have little meaningful opportunity to monitor,control or refuse state agencies' interception activities and/or mediate the access the state agencies have to the data of individuals using their networks. Hence the risk of their networks being used for unlawful surveillance is particularly high.

While there is no easy policy solution, Privacy International argues that telecommunication and internet service providers should, at least:

- Evaluate the human rights risks of allowing the installation of surveillance technologies directly on telecommunications equipment, infrastructure and networks and the effect that these technologies have on the providers' capacity to control and monitor access to their communications networks by state agencies.

8 UN Doc. A/HRC/29/32.
9 See, for example, Privacy International's report on Pakistan, https://www.privacyinternational.org/node/627

- Develop policies on the minimum legal framework, regulatory and technological safeguards, and standards of oversight that must be in place before they agree to provide access to their services or infrastructure.
- Include in their agreements with governments a stipulation that surveillance agencies provide copies of judicial warrants prior to any interception , and that companies retain the ability to challenge the interception activities of authorities and the power to notify customers of surveillance activities taking place.
- On a country-specific basis, collect and publicly publish data and analysis on surveillance legal frameworks, practices, and numbers of interception requests.

Further, Privacy International encourages the UN Special Rapporteur to consider the role industry bodies, such as the Global Network Initiative (GNI), can play in developing policies and guidelines to companies, including in relation to preventing the selling of products or services to markets where companies cannot adequately ensure that their subscriber's data and communications are safe from unlawful state surveillance.

2. Explore the role of ICT companies in supporting unlawful surveillance and their responsibility

2.1 Complicity in supporting mass surveillance

The Five Eyes and other states have conduct much of their mass surveillance by tapping the main fibre optic cables that carry communications around the world. 95% of the world's communications passes through these cables.[10]

In the UK, for example, GCHQ have been tapping undersea cables operated by a small number of ICT companies since 2004-5. The undersea cables are accessed when they hit the country at the beach. GCHQ asks companies for access, then the communications are split and a mirror copy of the communications data and content is taken. The UK's "Tempora" system buffers most internet communications extracted from fibre optic cables so these can be searched at a later date[11].

In Pakistan, Privacy International revealed that in 2013 the Inter-Services Intelligence, Pakistan's main intelligence agency, sought to commission a mass surveillance system to tap international undersea cables at three cable landing sites in southern Pakistan.[12] Privacy International also documented the Ethiopian governments' plan to deploy surveillance technology capable of tapping its upgraded telecommunication cables.[13]

In 2014 Privacy International filed a complaint with the Organisation for Economic Cooperation and Development (OECD) in the UK against BT, Verizon Enterprise, Vodafone Cable, Viatel, Level 3 and Interoute to challenge the practice of telecommunications companies providing assistance to the UK Intelligence agencies in the mass interception of internet and telephone traffic passing

---

10 See UNEP-WCMC and ICPC report, Submarine cables and the oceans, connecting the world, 2009, available at: https://www.iscpc.org/documents/?id=132
11 See https://en.wikipedia.org/wiki/Tempora
12 See https://www.privacyinternational.org/node/627
13 See https://www.privacyinternational.org/node/546

through undersea fibre optic cables.[14] The complaint argued that that none of the fibre optic cable companies pursued any available legal avenues to protect the rights of their customers.

Despite recognising the merits of the complaint, the OECD National Contact Point in October 2014 refused to further scrutinise the telecommunications companies, claiming that the reports based on documents provided by Edward Snowden and published by the Guardian and Suddeutsche Zeitung did not substantiate a sufficient link between the companies and mass surveillance. Since then, the UK government is seeking to make its mass interception powers, and the ability to force companies to comply, explicit in the Investigatory Powers Bill currently being considered in Parliament.

In our submission we identified the main responsibilities of the companies based on international human rights standards and specific OECD guidelines, such as the 2011 OECD Guidelines for Multinational Enterprises.

These responsibilities can be summarised as:

- Investigate the legality of government requests to facilitate mass interception activities.
- Challenge, to the greatest extent possible, government requests to facilitate mass interception activities.
- Use all measures available to minimise involvement in mass interception activities.
- Seek to mitigate the adverse impacts of mass interception activities by, for example, informing customers of the relevant laws and types of government requests to which their information and communications might be subject.
- Have publicly available policies detailing company processes for addressing government requests for facilitation of mass interception activities and the processes in place to minimise adverse effects on customers' human rights.

Privacy International suggests that the UN Special Rapporteur includes the above among the measures against which the ICT sector can be assessed for its respect of human rights.

2.2 Other complicity in unlawful surveillance

In 2015, Privacy International documented the role of Microsoft in providing information used to convict an individual under the Thai Computer Crime Act, which isa proxy for the notorious 'lèse-majesté' as a way to repress freedom of expression. According to Microsoft's response to Privacy International's research, the company handed over user information to the Thai authorities on the belief that it was helping the investigation of 'erroneous information' that affected the stock market, but in fact it was aiding a prosecution that affected free expression.[15]

The case raise questions about the level of scrutiny that ICT companies ought to exercise when responding to governments' requests for users data. Privacy International encourages the Special Rapporteur to review existing company policies and principles for responding to government requests for user data, as well as how they are applied in practice.

We also suggest that the Special Rapporteur identifies ways ICT companies take steps to ensure that

14See https://www.privacyinternational.org/node/79
15 See https://www.privacyinternational.org/node/674 (including the reply from Microsoft.)

they are able to fulfill their obligations to respect human rights.

For example, some companies in the USA have challenged the government's demand for secrecy over its requests for users' information.[16] These challenges have significant relevance for freedom of expression, as the lack of transparency about governments' requests of users' data has a chilling effect on individuals' freedom of expression.

3. Explore the role of the ICT sector in defending and promoting encryption

The Special Rapporteur has already noted in his 2015 report how encryption and anonymity tools and services can protect and promote human rights online, particularly the right to freedom of expression and the right to privacy.[17]

There are a range of technical measures that the ICT sector can adopt to promote encryption. The Electronic Frontier Foundation has published a comparative table of some of the key 'messaging services' by a range of companies, comparing some of the fundamental technical elements of encryption.[18] Apple, for example, have been providing encryption in some of their services, including end-to-end encryption with FaceTime and iMessage.

Privacy International encourages the UN Special Rapporteur to identify the key policy and security measures that companies should take to promote encryption among the users of their products. In particular, the UN Special Rapporteur could assess the standards of encryption and security applied by relevant ICTs, including policies on updating them, whether encryption is offered and if so, whether it is offered by default.[19]

Regulation of encryption remains a key policy issue among governments as they review their surveillance practices and capacity to address emerging threats to national security. Governments have adopted different responses. Recently, officials in Finland[20], France[21], the Netherlands[22], and the USA[23] have all signaled that they will not seek ways to undermine encryption. Other governments have instead sought powers to limit or weaken encryption.

In this debate, companies' opposition to governments' efforts to weaken encryption is fundamental. The UK Investigatory Powers Bill offers a good example. Faced with the Home Office attempts to

---

16 See Tech Titans Poised for Showdown With Justice Department Over NSA, Time Magazine, 7 October 2013, available at http://business.time.com/2013/10/07/tech-titans-poised-for-showdown-with-justice-department-over-nsa/
17 UN doc. A/HRC/29/32, 22 May 2015.
18 See https://www.eff.org/secure-messaging-scorecard
19 Some useful examples of assessing encryption policies are included in the Ranking Digital Rights 2015 report (https://rankingdigitalrights.org/index2015/download/).
20 See http://yle.fi/uutiset/report_puts_foreign_intelligence_gathering_online_surveillance_on_the_agenda/7736822
21 See http://www.numerama.com/politique/138689-chiffrement-le-gouvernement-rejette-les-backdoors.html
22 See http://www.bbc.co.uk/news/technology-35251429
23 See http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html?_r=0

introduce a clause that would allow the government to impose obligations on telecommunications service providers to remove electronic protection, thereby *inter alia* weakening encryption, several companies provided written and oral evidence to the IP Bill Parliamentary Joint Committee to argue against such power.[24]

4. Address ICT sector role in government equipment interference/hacking

ICT companies have a responsibility to protect individuals' communications and data against non-state actors attempts to unlawfully gain and exploit such data, including through organised cybercrime.

Security measures to protect personal data, such as those required under relevant data protection standards, need to be constantly reviewed and updated with a view toward implementing the most protective standards and preventing criminal hacking.

In this context, Privacy International is particularly concerned by an increasing threat to the privacy of communications and personal data (with the directly correlated risk to freedom of expression) posed by state sponsored hacking.

Unlike more traditional forms of surveillance, such as targeted requests for users' data or interception, the deployment of state hacking significantly raises the risks of undermining the privacy and the security of a potentially unlimited number of individuals who use modern forms of communication such as the internet.

As law enforcement and intelligence agencies are increasingly relying on equipment interference (hacking) for purposes of surveillance, the responsibility of ICT companies, which may, in some circumstances, be complicit in the deployment of such interference need to be explored.

This is particularly necessary given that some states are seeking to require ICT companies to assist in their hacking. For example, under the UK draft Investigatory Powers Bill any person (which could include ICT companies) may be required to "provide assistance in giving effect to the [equipment interference] warrant." Communications service providers could be compelled to take any steps, unless "not reasonably practicable", to assist the police and the intelligence services to hack our computers and other devices. While we do not know what this assistance might look like in practice, it could include compelling communication service providers to send false security updates to a consumer in order to install malware that the police or intelligence services could then use to control the consumer's computer; or the service provider might be requested to host a "watering hole" attack, by installing custom code on a website they operate that will infect with

---

24 See in particular, written evidence by Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc., Yahoo Inc. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26367.html ; Mozilla, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26349.html; Apple, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26341.html.

malware any device that visits that website.[25]

Some companies have already begun addressing this issue, for example by notifying users when their accounts seem to be under attack from state-sponsored actors.[26] However, it remains to be seen whether such notification also contains sufficient details to identify which state actors may be behind the attack.

Exploring the human rights responsibilities of ICT companies in detecting state sponsored hacking, responding to hacking requests, and in taking remedial action upon discovering state hacking in their network would represent a significant added value to the research of the UN Special Rapporteur in this area.

Further it may help address the difficulties companies face, particularly in view of the secrecy still surrounding the practices of of government hacking. Very few states have acknowledged that they are engaged in hacking. Even when governments, after significant pressure, avow this capability (as the UK did in 2015), the details and circumstances under which they resort to hacking are not publicly disclosed. Further, as in the draft IP Bill in the UK, companies would be placed are under an obligation not to disclose information regarding state hacking.[27] This secrecy risks undermining the trust of individuals who use the internet and other modern form of telecommunications, thereby, inter alia, resulting in a chilling effect on freedom of expression.

———

Privacy International stands available to answer any questions or requests for additional information arising from the issues covered in this submission. The organisation would also be interested in continuing to contribute to this study by the UN Special Rapporteur on freedom of expression.

Contact: Tomaso Falchetta, Legal officer, Privacy International, tomasof@privacyinternational.org

25 The US Federal Bureau of Investigation (FBI) has admitted to deploying such an attack on the servers of the service Freedom Hosting. Each server was turned into a watering hole, and subsequently infected with malware any device that visited the server whether or not that device was of interest to the FBI. Poulsen, K. (13 September 2013) FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, Wired, http://www.wired.com/2013/09/freedom-hosting-fbi/

26 See, for example, Google: https://googleonlinesecurity.blogspot.co.uk/2012/06/security-warnings-for-suspected-state.html; Facebook: https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766; Microsoft: http://blogs.microsoft.com/on-the-issues/2015/12/30/additional-steps-to-help-keep-your-personal-information-secure/ ; Yahoo: https://yahoo-security.tumblr.com/post/135674131435/notifying-our-users-of-attacks-by-suspected ; Twitter: http://www.aljazeera.com/news/2015/12/twitter-warns-state-sponsored-attacks-time-151214032016261.html

27 Under the current Investigatory Powers Bill in the UK, for example, the general public is likely never to be made aware of what kind of “hacking” assistance has been required by communication service providers due to the very strict non-disclosure provision in the Bill (Clause 102.)