Submission to the UN Special Rapporteur on the Protection of the Right to Freedom of Opinion and Expression: Study on Telecommunications and Internet Access Sector

November 2016

Intro

Privacy International welcomes the opportunity to contribute to the Special Rapporteur's next report to the Human Rights Council in June 2017, and to engage with the ongoing project on freedom of expression in the telecommunications and internet access sector.[1] This submission focuses on "direct access" by State actors into networks and services provided by Telecommunications and Internet Service Providers ("Telcos and ISPs) and associated companies, and in turn their relevant policies and practices.

Direct access broadly describes situations where law enforcement and intelligence agencies have a direct connection to telecommunications networks in order to obtain digital communications content and data (both mobile and internet), often without prior notice or judicial authorisation and without the involvement and knowledge of the Telco or ISP that owns or runs the network. Direct access poses both legal and technical challenges and is a practice that has a defined link to arbitrary and abusive practices that impact freedom of expression and privacy.

Direct access is not a new issue. Privacy International have highlighted concerns since the 1990s about the increasing trend of law enforcement agencies and intelligence agencies having direct access to personal information- not just communications but also data such as Passenger Name Records (PNRs) and financial transactions.[2]

As direct access of communications can technically happen at various points throughout a telecommunications network, we welcome the Special Rapporteur's focus on companies throughout the Information and Communication Technology (ICT) sector beyond Telcos, ISPs and Network Equipment Providers (or vendors), a number of which

---

[1] See Privacy International's submission to the Special Rapporteur's 2016 report, *"Freedom of expression and the private sector in the digital age"* A/HRC/32/38
http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx

[2] See, *Privacy International extends legal action against banking giant SWIFT* (2006)
https://www.privacyinternational.org/node/534
An assessment of the EU-US travel surveillance agreement (2012)
https://www.privacyinternational.org/node/927
Private Interests: Monitoring Central Asia (2014)
https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf
Macedonia: Society on Tap (2016) https://www.privacyinternational.org/node/816

are already engaged in the business and human rights debate. As the Special Rapporteur has identified, it is necessary to broaden the focus to other parts of the sector that potentially have an impact on human rights such as Internet exchange points (IEPs) and submarine cable providers, which at present do not engage in the business and human rights debate.

In the age of big data and the "internet of things", more devices are connected to the internet and generate data, including personal data, which needs protecting. Therefore, it is important to continue to tackle the issue of direct access as it is in danger of broadening unchecked beyond traditional communication devices.

State Regulation of Direct Access

There is currently no accepted definition of "direct access" in the telecommunications and technology sector. Rather, it can be considered a technical or legal practice which allows State actors access to subscriber data or call/message content contained within a network or service without the knowledge or intervention of the concerned Telco, ISP, or "over the top" (OTT) provider.

Direct access of communications and other personal data is clearly an interference with the right to privacy. Its effects also limit the right to freedom of expression and other human rights. As noted by the European Court of Human Rights, direct access is "particularly prone to abuse."[3]

As part of delivering telecommunications networks, Telcos and ISPs are usually required under local law of many jurisdictions to provide the technical means for individual communications to be intercepted for the purposes of legal investigations of criminal activity.

The European Telecommunications Standards Institute (ETSI) is an independent standard setting body and has taken the lead in standardising lawful intercept technical requirements. Although defined as a regional standardisation body, ETSI standards do not just cover Europe, but are also widely applied worldwide. They define lawful interception as,

" A security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organisations."[4]

Therefore, in the ETSI standard the Telco, ISP, or Network Equipment Provider has a role to play to enable interception to happen, in accordance with the law of a country.

---

[3] European Court of Human Rights, Roman Zakharov v. Russia judgement (4 December 2015) para 270. http://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22zakharov%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-159324%22]}

[4] See, http://www.etsi.org/index.php/technologies-clusters/technologies/security/lawful-interception

Other standards, such as the Russian "SORM", work to different specifications. SORM was put into practice across Russia in the early 1990s and provides an architecture by which law enforcement and intelligence agencies can obtain direct access to data on commercial networks, bypassing involvement of the Telco.[5] It has been adopted in a range of countries, such as in the Central Asian Republics.

Commenting on the legislation underpinning SORM in the Russian Federation, the 2015 European Court of Human Rights judgement in the case of Roman Zakharov v. Russia stated,

"…the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great."[6]

Direct access therefore bypasses both legal and technical protections and safeguards against arbitrary surveillance which impacts freedom of expression, privacy and other rights. The result of direct access is that surveillance practices are more prone to abuse and fall short of international human rights standards.

The impact of direct access on freedom of opinion and expression – the case of the Former Yugoslav Republic of Macedonia

The Special Rapporteur's previous report mapping the ICT sector outlines the impact of surveillance on freedom of expression,

"Unnecessary and disproportionate surveillance may undermine security online and access to information and ideas (see A/HRC/23/40). Surveillance may create a chilling effect on the online expression of ordinary citizens, who may self-censor for fear of being constantly tracked. Surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children (see A/HRC/29/32)."[7]

[5] *Private Interests: Monitoring Central Asia* (2014) https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf , pp28-30

[6] European Court of Human Rights, Roman Zakharov v. Russia judgement (4 December 2015) para 270. http://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22zakharov%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-159324%22]}

[7] See A/HRC/32/38, para 57

Privacy International's 2016 report into surveillance in Macedonia[8] focused on allegations made by an opposition party that a State intelligence agency, the Administration for Security and Counter Espionage (UBK), had allegedly intercepted the communications of activists, government officials, senior public officials, Mayors, Members of Parliament, the Speaker of the Parliament, opposition leaders, judges, the State Prosecutor, civil servants, journalists, editors and media owners. In total, they claimed that 20,000 people had their telephone communications intercepted over a number of years, including during the 2014 General Election.

Many victims of surveillance were sent transcripts or recordings of their phone calls by the opposition party as evidence. Journalists and activists described to Privacy International the detrimental impact this had on conducting their professional work, and on their privacy and security. Such practice goes beyond a "chilling effect" on freedom of expression: it amounts to intimidation and an attempt to silence government criticism and independent press during elections. The added shock many felt was that surveillance was not being conducted by a communist state, but by the intelligence agency of a modern democratic republic.

Following the reports of large scale interception of communications in Macedonia, the European Commission (DG Neighbourhood Policy and Enlargement Negotiations) appointed a group of independent senior rule of law experts to carry out an analysis and provide recommendations in response. The analysis found that direct access was mandated under law,

"Acting on the basis of Articles 175 and 176 of the Law on Electronic Communication, each of the three national telecommunications providers equips the UBK with the necessary technical apparatus, enabling it to mirror directly their entire operational centres. As a consequence, from a practical point of view, the UBK can intercept communications directly, autonomously and unimpeded, regardless of whether a court order has or has not been issued in accordance with the Law on Interception of Communications."[9]

The largest Telco Magyar Telekom (a subsidiary of Deutsche Telekom) declined to answer Privacy International's specific questions relating to direct access carried out by the State intelligence agency, saying that Magyar had launched its own internal investigation.

Part of the reason for the investigation was due to the fact that the European Union (EU) had financed projects in Macedonia to ensure free and fair elections. The discovery of direct access to communications jeopordised this goal. The investigation concluded:

"As the EU was heavily investing in democratization and liberalisation projects, the fact that the ruling party had access to the personal communications of some 20,000 people,

[8] *Macedonia: Society on Tap* (2016) https://www.privacyinternational.org/node/816
[9] See, http://ec.europa.eu/enlargement/news_corner/news/news-files/20150619_recommendations_of_the_senior_experts_group.pdf

including during a general election, effectively means that many of these efforts have been wholly undermined."[10]

These concerns were summarised by the UN Human Rights Committee's concluding observations, which recommended:

'*The State party should take all measures necessary to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17. In particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity. It should also ensure that persons who are unlawfully monitored are systematically informed thereof and have access to adequate remedies."*[11]

The immediate effects of the scandal have been far-reaching: mass protests led to the EU brokering an agreement leading to the resignation of both the Prime Minister and his cousin (the head of the UBK) and to new elections, now scheduled for December 2016 after several delays. It is not known what, if any, reforms have been taken to stop direct access in Macedonia, or whether any reforms are forthcoming.

Policies and Practices of Telcos, ISPs and Associated Business Regarding Direct Access

Telcos and ISPs

When networks are configured technically to bypass the involvement of the Telco and ISP, the company is reportedly unaware when customer's communications are being intercepted. Therefore, in States that practice direct access, Telcos and ISPs cannot exercise control over government access to their customer's data. This leaves them open to both being linked with negative human rights impacts arising from arbitrary surveillance, and even complicit in abuses committed by third parties if they are seen to benefit (either financially or otherwise).

Further, Telcos are often legally prevented from disclosing that law enforcement or intelligence agencies have direct access to their networks. According to the report by the former UN High Commissioner for Human Rights Navi Pillay,

"Governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic."[12]

---

[10] ibid

[11] Human Rights Committee, concluding observations on the third report of the former Yugoslav Republic of Macedonia, UN doc. CCPR/C/MKD/CO/3, 17 August 2015, para 23.

[12] 2014 UN report: Right to Privacy in the Digital Age (A/HRC/25/117) para 3

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

However, this does not mean Telcos, or other companies enabling or allowing direct access are exempt from their responsibilities to protect human rights, including privacy and freedom of expression.

The UN Guiding Principles on Business and Human Rights states that the responsibility to respect human rights requires that all business enterprises must,

"13 (a) Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur;

(b) Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."

Exposing direct access

In order to effectively highlight and challenge the process companies must make efforts to bring transparency to this highly secretive process. The issue is too big for one company to tackle alone. A group of Telcos have begun to provide increasing amounts of information over the years, despite legal restrictions, which helps increase our understanding of the situation and ability to effectively challenge the process. The Telecommunications Industry Dialogue published a statement in 2014 expressing the view that,

"…government surveillance programs should be subject to ongoing review by an independent authority and that governments should not conduct any type of registry, search, or surveillance by means of direct access to companies' infrastructure without any technical control by the company or without the company controlling the scope of the data collection."[13]

A number of companies have recently begun to publish reports on the governments' requests of access to their communications networks, often referred to as "transparency reports." On the issue of direct access, Telcos have either disclosed in which jurisdiction they are required to provide for direct access or, where this is not legally possible, presented the limitations they are under to disclose direct access taking place in jurisdictions where they operate.

The UK based telecommunications operator Vodafone published its first transparency report in 2014, called the Law Enforcement Disclosure Report[14], which focuses on the company's operations in 29 countries. This report confirms that in some countries, the laws on interception have little or no legal oversight and allow law enforcement to bypass the operator and have direct access to the network. The report states,

---

[13] Telecommunications Industry Dialogue 2015 Annual Report https://www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Dialogue-Annual-Report-2015.pdf

[14] Vodafone Law Enforcement Disclosure Report, featured in Vodafone's 2014 Sustainability report http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf pp 61-81

> *"…In a small number of countries the law dictates that specific agencies and authorities must have direct access to an operator's network, bypassing any form of operational control over lawful interception on the part of the operator. In those countries, Vodafone will not receive any form of demand for lawful interception access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link*."[15]

Vodafone did not detail the countries in question due to concerns regarding possible retaliation against staff, but media reports state there are "about six" countries where the law obliges operators to install "direct access pipes" or allow governments to do so.[16]

In 2015, Telenor published its first Government Access report which stated,

"In others [countries], the CSP [communication service providers] must allow permanent direct access to its network with no control or visibility over the interception activities that the government in question carries out."[17]

Telia Company (formerly TeliaSonera) published a Law Enforcement Disclosure Report in 2015 which published information on laws in countries in which they operate that mandate direct access.

Millicom's 2015 Law Enforcement Disclosure report[18] stated that they operate in five markets where law enforcement authorities have direct access to their network, and they do this without Millicom's knowledge or involvement.

Information from these companies fed into a data base of laws of 44 countries published by the Industry Dialogue.[19]

Tele2 published a statement[20] outlining the challenges of operating in countries where the SORM system is utilised. It said that in Kazakhstan, *"intercept activities are carried out in a highly confidential manner and therefore are unbeknownst to Tele2 Kazakhstan".* Their role is limited to *"the installation of technical equipment for SORM, provision of access to the equipment for designated state authorities and collection and retention of personal information of subscribers, as well as submission of the information to them at their lawful request."*

---

[15] Ibid p69
[16] The Guardian, 6th June 2014 *Vodafone reveals the existence of secret wires that allow state surveillance,* http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance?CMP=EMCNEWEML6619I2
[17] https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf p3
[18] http://www.millicom.com/media/4562097/millicom_tr_law_2016_final_300316.pdf p6
[19] http://www.telecomindustrydialogue.org/resources/country-legal-frameworks/
[20] http://www.tele2.com/our-responsibility/esg/topics-relevant-matters/social/user-safety/privacy-and-sorm/

Tele2 is not allowed to see any warrants. *"That surveillance systems, as SORM, is getting such a wide spread is not the main reason for concern (even though it is a challenge). The foremost concern is that operators are not allowed to see the warrant. This means that the operator cannot know if the ruling is lawful and that there is a warrant behind each and every case (e.g. the system is not overused or misused)."*

Earlier this year, Privacy International wrote to over 20 telecoms providers around the world asking for more information about the issue of direct access to increase our understanding. Of the companies that responded, there is a will to try and move the dialogue on the issue. We appreciate the companies' mentioned efforts to provide information in order to help civil society highlight and campaign around the issue.

Engaging with a broad spectrum of actors in the ICT sector

While some Telcos have begun to address this issue, as they have close relationships with governments and are customer facing, there are other companies in the ICT ecosystem where the role in providing direct access are less clear, which needs to be explored.

Network Equipment Providers:

Network Equipment Providers (NEPs), are companies that build and service the infrastructure of a telecommunications network. They are not consumer facing. Their customers typically comprise enterprise customers, operators, and government departments. They provide the underlying infrastructure and network nodes such as switches, and configure networks to the technical standards mandated by a particular country. Much of the equipment produced by NEPs technically facilitates surveillance requirements, whether or not legal safeguards are in place to prevent abuse. Some also actively assist in ensuring that the infrastructure is adaptable to surveillance. For example, in Kazakhstan, Ericsson confirmed in writing to Privacy International that, since its Lawful Interception Management System does not conform to the SORM requirement, it works a local third party to ensure their systems are accessible to law enforcement through the use of "SORM-converters".[21]

Other NEPs also provide explicit surveillance products specially designed for and sold to government agencies or operators for government end-use. Nokia, for example, markets a "Unified Lawful Interception Suite" which:

"[E]nables Network Operators (NWO)/Communication Services Providers (CSP) to comply with government regulations for lawful interception of telecommunications and data retention. It offers a complete system for extracting communications of targeted subscribers

[21] *Private Interests: Monitoring Central Asia* (2014) https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf , p76

in real time. It also provides retention capabilities for a specific set of data related to the activity of all subscribers."[22]

It is often unclear which country is using which technical standards, and how the technical infrastructure operates, making it difficult to determine if a country practices direct access. Transparency reporting, while increasingly common among Telcos and ISPs is not a standard practice among NEPs, mostly due to the fact they do not receive government requests like Telcos do. However, they can play a significant role in enabling the technical surveillance capabilities of governments, and providing more information about the standards employed by countries, thereby supporting to build a global picture of which States practice direct access.

Internet Exchange Points (IEPs) and Submarine cable providers:

Very little information exists on the role and responsibility of IEPs and submarine cable providers (also called undersea cable providers) regarding proving direct access, which could be happening on the infrastructure they provide, and more research is needed. Both IEPs and submarine cables are often owned by consortiums, so it can be difficult to ascertain ownership and therefore apportion responsibility.

In 2014, Privacy International filed formal complaints with the Organisation for Economic Development (OECD) National Contact Point (NCP) in the UK against the telecommunication companies BT, Verizon Enterprise, Vodafone Cable, Viatel, Level 3 and Interoute regarding claims that they granted access to their fibre optic networks for the UK's Government Communications Headquarters (GCHQ) surveillance program, Tempora, as revealed by Edward Snowden.[23] Privacy International argued this action went well beyond what was legally required in facilitating GCHQ's mass surveillance and the companies received payment for their cooperation. By collaborating with GCHQ and providing access to networks, Privacy International argued that these companies have knowingly contributed to the violation of human rights by enabling the mass and indiscriminate collection of data and interception of communications.

The claim was rejected; the NCP claimed that reports based on documents provided by Edward Snowden and published by the Guardian and Suddeutsche Zeitung do not substantiate a sufficient link between the companies and mass surveillance.[24] This example demonstrates the lack of a forum available to bring transparency to and scrutinise the practices of these companies.

In addition, ISPs such as Google and Facebook have reportedly invested in building their own undersea cables[25], one of which between the US and Japan is already live.[26] As these

[22] Nokia, "Unified Lawful Interception Suite" https://networks.nokia.com/products/1357-unified-lawful-interception-suite
[23] See, https://www.privacyinternational.org/node/79
[24] See, http://www.oecdwatch.org/cases/Case_308
[25] Matt Burgess, *Google and Facebook's new submarine cable will connect LA to Hong Kong*, Wired, 14 October 2016 http://www.wired.co.uk/article/google-facebook-plcn-internet-cable

companies are already engaged in the business and human rights debate, providing further information as part of their existing transparency efforts would help identify points at which direct access might happen at the cable level.

The UN Working Group on Business and Human Rights strongly encourages all States to develop, enact and update a national action plan (NAP) on business and human rights as part of the State responsibility to disseminate and implement the UN Guiding Principles on Business and Human Rights. Currently ten countries have produced at least one NAP since 2013, with another 19 countries that are in the process of developing a NAP or have committed to doing one, including Azerbaijan, Mexico, and the USA. In another 8 States, National Human Rights Institutions (NHRI's) or civil society have begun to develop NAPs, including Kazakhstan, South Africa, and the Philippines.[27] The NAP can (and should) include concrete actions the State will take to ensure companies respect human rights. Privacy International encourages States to include in their NAPs action for companies throughout the ICT ecosystem to engage with the issue of direct access.[28]

Recommendations:

Based on the above, Privacy International encourages the Special Rapporteur to consider the following recommendations.

For States:

- Direct access of communications and personal data is particularly prone to abuse of human rights, including privacy and freedom of expression. States should review their legislation governing requests of personal data and interception of communications to ensure that it complies with the principles of legality, necessity and proportionality.

- In the short term, States should remove restrictions that prevent Telcos and other ICT companies from including information about direct access in their transparency efforts.

- Companies that currently engage in the business and human rights debate are mainly consumer facing. States should encourage companies in the ICT sector not currently engaged to become so. One way would be to include in State National

---

[26] Matt Burgess, *Google's 'Faster' undersea internet cable goes live*, Wired, 30 June 2016 http://www.wired.co.uk/article/google-faster-cable-japan-us

[27] http://www.ohchr.org/EN/Issues/Business/Pages/NationalActionPlans.aspx

[28] For example, the UK's 2013 NAP included an action for the government to produce guidance for UK based cybersecurity companies exporting cybersecurity products and services that are not subject to export control but could still pose a risk to human rights. The consultation for this guidance included cybersecurity companies that had not engaged previously in the business and human rights debate. See, https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf

Action Plans on Business and Human Rights concrete avenues and actions for companies throughout the ICT ecosystem to engage with the issue of direct access.

- Where States provide finance and project assistance to other States to aid democracy, governance and rule of law, a condition of this assistance should be that there are no direct access practices, as this risks interfering directly in the democratic process, as demonstrated in the earlier example of Macedonia.

For Companies:

Identify direct access legislation: No one company can tackle this issue alone, a collective position is needed in order to bring transparency to a sensitive, secretive process and begin to raise standards within a country and set best practice. We appreciate the efforts of some Telcos in publicly identifying direct access legislation in their operating markets. For those companies that haven't yet made a statement on this issue, this is the first step. We recommend to companies that have conducted internal investigations on this issue to publish a summary of findings, as in the case of Macedonia mentioned above.

Policy Development: While there is no easy policy solution, companies 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.
- 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.

Identify technical standards: it can be difficult to ascertain the technical standards by which a State requires to configure their networks, whether ETSI, SORM or another standard. We recommend companies such as Telcos and Network Equipment Providers assist in identifying technical standards in particular countries and their technical characteristics, in order to identify direct access practices and the points at which direct access might take place in the network.

Advocate transparency among companies that provide access to Telecommunications and Internet Services: Part of the ICT sector involved in providing telecommunications and internet access and services, such as IEPs and submarine cable providers, are not engaged in the business and human rights debate or with civil society efforts to improve human rights. It would be helpful if consumer facing companies such as Telcos and ISPs, which do engage in the debate and advocate transparency, raise the

issue of direct access with other companies in their value chain and with relevant standard bodies and governance bodies where companies have membership eg. European Technical Standards Institute (ETSI) Telecommunication Industry Dialogue, Internet Engineering Task Force (IETF), Telecommunications Industry Association and the International Telecommunications Union (ITU).