METAMORPHOSIS
Foundation for Internet and Society

PRIVACY INTERNATIONAL

Committee for Supervising the Work of the Security and Counter Intelligence Directorate and the Intelligence Agency
Assembly of Republic of Macedonia
11 Oktomvri St., No. 10, 1000 Skopje, Republic of Macedonia
k-nadzor@sobranie.mk

11 August 2017

To whom it may concern

We are writing to provide information and seek assurances regarding the legal and technical regime governing telecommunications interception in Macedonia.

Privacy International is a United Kingdom-based charity founded in 1990. We are the first organization to campaign on privacy issues at an international level. We undertake research and investigations into government and corporate surveillance with a focus on the technologies that enable these practices. We litigate or intervene in cases implicating the right to privacy in courts around the world. To ensure universal respect for the right to privacy, we advocate for strong national, regional and international laws that protect this right. We make regular representations to governments, regional bodies like the European Union, and the United Nations.

Metamorphosis is an independent, nonpartisan and non-profit foundation founded in Skopje, Macedonia in 2004. Its mission is to contribute to the development of democracy and increase the quality of life through innovative use and sharing of knowledge. Based on its guiding values of openness, equality and freedom, Metamorphosis had been advocating protection of human rights in the digital sphere, privacy in particular, through policy making, support for strengthening the state institutions, capacity building, public education, and litigation (including 2010 initiative with other CSOs to the Constitutional Court which overturned the amendments stipulating unconstitutional blanket surveillance through direct access without court order).

Privacy International and Metamorphosis are both member organisation of European Digital Rights, an association of civil and human rights organisations from across Europe.

This letter is being sent to the President of the Government of Republic of Macedonia, the Ombudsman of the Republic of Macedonia, and the Committee for Supervising the Work of the Security and Counter Intelligence Directorate and the Intelligence Agency. A copy of the

letter has also been sent to the Delegation of the EU and to DG Neighbourhood and Enlargement Negotiations of the European Commission.

Following reports of unlawful surveillance in Macedonia, the UN Human Rights Committee expressed concerns "that thousands of State party nationals, including opposition politicians and journalists, have been allegedly subjected to wiretapping by the security services, potentially affecting their rights to freedom of expression and privacy."[1] We understand that the Special Public Prosecutor's Office has opened an investigation concerning unauthorised interception of communications.[2]

As a result, we note and welcome commitments in the 2017-2020 Work Programme of the Government[3] to:

- Introduce new mechanisms to improve internal and external control of the work of the police and security services
- Reform the UBK intelligence agency and subject it to parliamentary control
- Strengthen parliamentary control and establish the institution of police ombudsman, with competences to conduct independent investigations on alleged overstepping of police competencies and infringement on human rights and freedoms
- Build a system of public consultations for legislative changes, which includes all stakeholders, including civil society organizations
- Implement legislative changes to limit authority to conduct surveillance
- Introduce guarantees which would limit arbitrary surveillance

We believe that such reforms are a matter of urgency, and recommend that further changes are implemented to ensure that police and security agencies do not have "direct access" to telecommunications networks and interception systems.

"Direct Access"

In June 2015, an assessment[4] by senior rule of law experts appointed by the European Commission to carry out an analysis and provide recommendations found that the UBK intelligence agency had a direct connection to telecommunications networks to conduct interception, regardless of whether prior notice or judicial authorisation was received and without the involvement and knowledge of the telecommunications operators which run the network:

[1] Concluding observations on the third periodic report of the former Yugoslav Republic of Macedonia, 17 August 2015
[2] See Macedonia's reply to the Human Rights Committee: http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/MKD/INT_CCPR_FCO_MKD_25047_E.pdf]
[3] http://vlada.mk/sites/default/files/programa/2017-2020/ProgramaVlada2017-2020_08062017.pdf
[4] See, http://ec.europa.eu/enlargement/news_corner/news/news-files/20150619_recommendations_of_the_senior_experts_group.pdf

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….

From the point of view of technical capability, the UBK holds the monopoly over the use of surveillance in both intelligence and criminal investigations. Surveillance is executed and monitored exclusively by the UBK on its own behalf, and also on behalf of the Police, Customs Administration and Financial Police. Therefore the UBK has the means to interfere in criminal investigations and, indirectly, to undermine the independence of the leader of the investigation (ie. the prosecutor).

Such "direct access" to telecommunications networks by law enforcement and intelligence agencies has a defined link to arbitrary and abusive practices that impact privacy and freedom of expression. Commenting on the legislation underpinning telecommunications interception in the Russian Federation, the 2015 European Court of Human Rights judgement in the case of Roman Zakharov v. Russia stated that:

"...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."[5]

For further information, please find attached a copy of Privacy International's report on wiretapping in Macedonia, and an overview of "direct access" developed by Privacy International and submitted to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression in November 2016.

Given the judgement of the European Court of Human Rights and the link between direct access and abuses, we are writing to seek clarification and assurances on the following points:

- Do you agree with the European Commission-appointed rule of law experts that the intelligence agency in Macedonia could "*intercept communications directly, autonomously and unimpeded, regardless of whether a court order has or has not been issued*"?
- Do you agree that such a system "*is particularly prone to abuse*" as stated by the European Court of Human Rights?

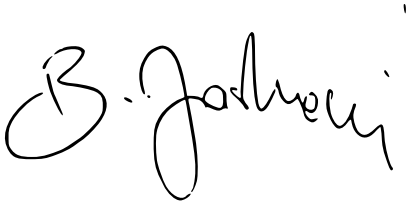
[5] European Court of Human Rights, Roman Zakharov v. Russia judgement (4 December 2015) para 270. http://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22zakharov%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-159324%22]}

- Do you agree that Articles 175 and 176 of the Law on Electronic Communication allowed “direct access” to telecommunications networks in Macedonia?
    - If so, will you provide assurances that the Law will be amended to ensure “direct access” is not practiced in Macedonia?
    - If not, can you provide other assurances that “direct access” is not and will not be practiced in Macedonia?

We thank you for your attention in this matter and stand ready to assist further in any way we can. Please send any response to either email address below.

Yours sincerely





Edin Omanovic
Privacy International
edin@privacyinternational.org

Bardhyl Jashari
Metamorphosis
info@metamorphosis.org.mk

PRIVACY INTERNATIONAL

Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

Study on Telecommunications and Internet Access Sector

Submitted by Privacy International

November 2016

Submission to the UN Special Rapporteur on the Promotion and 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,

---

[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

ISPs and Network Equipment Providers (or vendors), a number of which 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).

Macedonia: Society on Tap



“This is my personal opinion,” concedes Branko, a taxi driver in Skopje, the Republic of Macedonia's capital. “It was done by America to stop Putin building his gas pipe line through Macedonia.”

> “This is just politics,” he advises, skeptically.

It's a common reaction to the wiretapping scandal in Macedonia. Beginning in February last year when opposition leader Zoran Zaev posted a series of wiretaps online that he called 'bombs' – they seemingly showed that for years the phone calls of some 20,000 activists, lawyers, opposition members, journalists, civil servants, business people, and even members of the government had been unlawfully monitored. In June 2015, an assessment by senior rule of law experts appointed by the European Commission substantiated many of the claims.

Branko the taxi driver's opinion is understandable yet arguably manipulated. For several years the media landscape in Macedonia has been subject to a campaign of consolidation, media freedoms have been restricted and editorial policy controlled through ownership, financing, and personal relationships with senior staff. Macedonia was ranked 117th in Reporters Without Borders' 2015 Press Freedom Index, just behind Tajikistan and Qatar. In 2007, it was ranked 36th.

The opposition leader claims that the wiretapping was conducted by the Prime Minister at the time, Nikola Gruevski, and his cousin, Saso Mijalkov, who was at the time head of Macedonia's intelligence agency, the Administration for Security and Counter Espionage (UBK). Gruevski claims the wiretapping was conducted by foreign intelligence agencies in order to destabilise the country.

In such a controlled media space, it is difficult to know who to trust. Rumours thrive.

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, and to new elections scheduled for June 2016. The long term effects of such wide scale wiretapping however will be felt by individuals and Macedonian society for years to come.



Opposition leader Zoran Zaev announcing the wiretaps and holding copies of the recordings. February 2015. Youtube

The *"Sorosoids"*

The climate of close control is familiar for those that experienced living in the former Yugoslavia. Macedonia was a constituent Republic of the socialist federation in which the communist party exerted tight control over the media and regularly spied on its people until its bloody break-up in the early 1990s.

In 1976, theatre director Vladimir Milchin was selected for surveillance by the party as an 'anarcho-liberal,' an opponent of the State. In 2000, he was able to read his file – for five years, the ruling party had been recording his conversations. There were transcripts of his conversations with family, with friends, with everyone.

This year, he received another transcript. This time however, it was in the form of CD, and the surveillance was not being conducted by a communist state, but by the intelligence agency of a modern European democratic republic.

In February 2015 the opposition party, Social Democratic Union of Macedonia (SDSM) began

providing victims with transcripts and CDs of their own intercepted phone calls.

“I wasn't shocked,” explains Vladimir, who went on to become the Executive Director of the Open Society Institute in Macedonia for 20 years, an international foundation supporting liberal civil society and individuals financed by multi-billionaire George Soros.

> “What was disappointing was that it is now the same as in a one party communist state, where I'm judged to be an internal enemy.”

“On 21st April this year [2015], I was attacked in the street by a man wearing a hood... I've received death threats. One time I was told that my dead body wouldn't be buried in Macedonia. This is how opponents are treated in this country.”

Violeta Gligoroska, a life long activist and journalist who also worked at the Open Society Institute, received a similar batch of her own private conversations in May.

“It felt like I had been raped, like I had been raped by the State."

> “My father was a communist dissident expelled from the party. For sure he was under surveillance. I never asked for the files. As my father was already dead, I didn't have the courage, the emotions, to go and to ask for it. I wanted the Ministry of Interior as far away from me as possible.”

> “Unfortunately, that didn't happen.”

One of their colleagues who still remains at the Foundation, Slavica Indjevska, explains that it is regularly demonised by the pro-government press, characterized as foreign agents. They are derogatorily referred to as *Sorosoids*.

But surveillance of the foundation's employees does not just concern them. Even the most targeted surveillance also affects everyone who is in contact with the target; it is one of the main objectives and problems of modern surveillance. The job of the foundation's staff is to monitor social and political developments and to speak to journalists and Non Governmental Organisations (NGOs) about their projects, plans, and opinions. Because the Foundation was being surveilled, it gave the Government direct access to everyone they spoke to.

Slavica has yet to bring herself to listen to the CD in her office containing her recordings. On a Sunday evening she was preparing aid packages for refugees that are transiting through Macedonia when she received the phone call telling her that a file of her intercepted communications was available to collect.

“'You must be wrong,' I said... I was speaking to OSF colleagues all over the world where we have projects... It's such a bitter feeling, really an awful feeling when someone is in your private space without your consent. It's like having someone in your house, in your ear. It's just so personal.”

> “This is the worst period in the country's history,” remarks Violeta, the experienced activist. “Even in the communist times, at least we knew we were being spied on.”

“We have taken Stasiland and translated it,” insists Vladimir, the theatre director. “It's just like East Germany; control by poisoning people with fear and propaganda.”

Slavica recalls voting in the independence referendum which saw Macedonia leave Yugoslavia in the early nineties. “I took my son and remember feeling like it could be a bright future for him. But something has gone wrong... during the nineties we witnessed hope and change, and people were

motivated to look past their own individual position. But now we're going backwards."

She's not optimistic about the future. "Simply when I see how much control, effort and money the state has, and the fear in people, with assumptions on their power by the economically weak, you're prone to manipulation, especially when you have no way out."



Vladimir Milchin, 2015. Privacy International

The Journalist

Meri Jordanovska also received a phone call telling her to collect a CD containing her recorded conversations. She's currently a journalist at the Balkan Investigative Reporting Network (BIRN), a network of non-governmental organisations across the former Yugoslav republics promoting freedom of speech, human rights and democratic values.

She studied journalism at university. "When I was a first grader, I wrote my first article because I wanted to travel a lot, to write about different cultures. I thought that I would write about good stuff. When I was seven I knew that I would be a journalist because I wrote a lot, but in Macedonia it's hard to be a journalist at the moment at this time. So if you're with the government, you write pro-government text. If you do anything else, for example cover the refugees, you are seen as a traitor of the country, as a *Sorosoid*... Society is very divided, you are either with them or against. There is no in-

between."

"But the opportunity to make a change is what makes me want to be a journalist, still. There is still something inside that makes you want to dig deeper and deeper to find the truth."

BIRN Macedonia recently published a report showing that the cost of a controversial 2010 government project to build a series of neoclassical monuments and buildings in central Skopje has jumped from the initial € 80 million estimated to € 560 million. In order to promote transparency around the projects, BIRN developed a publicly-accessible database documenting individual costs.

Some believe the new projects show how the government is looking to move Macedonia forward. Others, however, regard it as a nationalistic vanity project that is inexcusable in a country with one of the worst unemployment rates in Europe.



Government building, Skopje, 2015. Privacy International

Meri previously worked at Fokus, a critical independent investigative magazine founded by widely respected free speech pioneer Nikola Mladenov, who died in a car crash in 2013. The opposition leader Zaev is calling for the inquest into his death to be reopened, based on the wiretaps. "Today, audio conversations open the question whether the case can be closed as a tragic accident or there are indications that someone may have initiated the accident".

Journalists at Fokus have been the subjects of civil defamation lawsuits by government officials, while its Editor-in-Chief Jadranka Kostova was recently named in a Lustration process as a former informant passing details on to the Yugoslav secret police during the 1990s, something she shares in common with Vladimir. The Organization for Security and Cooperation in Europe (OSCE) Special Representative for Freedom of the Media, Dunja Mijatovic, subsequently stated that the "decision could be seen as pressuring the magazine, endangering the media outlet and, consequently, having a chilling effect on media freedom".

Prior to Fokus, Meri was at A1, then Macedonia's main independent pro-opposition TV station, which was forced to shut down in 2011 after an unpaid tax dispute with its owner. Reporters Without Borders later concluded that “The government clearly seized the chance to silence some of the few media that criticize it”.

Meri believes she was targeted for surveillance because of her association with A1 and Fokus. “This government doesn't want to be criticized. Instead of denying the stories, they attack the journalist personally.”

According to Meri, her recordings contained 5-6 conversations that she had had with opposition party members about the elections and the secret police. But no one has any idea how many of their conversations were actually recorded in total.

Particularly worrying for her was that she had been having deeply personal conversations with

friends, as well as with Nikola Mladenov, her former and late colleague. “One of my colleagues received a recording of Mladenov congratulating them on the day their son was born.”

“Even that was being spied on.”

It also affects her professionally. She worries that potential sources will be reluctant to speak with her if they believe that their conversations may be being reported, while the fact that the opposition party has access to all the recordings also means that they now presumably have leverage over her and everyone that was being recorded.

The most shocking thing from the wiretaps for Meri was the extent of government influence in Macedonia, with evidence of senior government figures directly interfering in judicial appointments, editorial decisions across media, State appointments, and even interfering in the 2011 election through vote rigging and voter intimidation. The independent EU study concluded that the recordings appear to show “discussion of manipulation of the voter list; voter buying; voter intimidation, including threats against civil servants, and prevention of voters from casting their votes”.

“Every segment of society is under control. I have no faith anymore in the institutions. Everyone has connections to the party.”





Meri Jordanovska, 2015. Privacy International

The Academic

Jasna Koteska sees parallels and differences between surveillance practices back in Yugoslavia and modern techniques.

She is a Professor of Literature, Theoretical Psychoanalysis and Gender Studies. Her father Jovan Koteski was a famous Macedonian poet in Yugoslavia and subject to intense State surveillance for 42 years. “The present right-wing Macedonian government is, ironically, the closest approximation to the communist nomenclature in the post-communist era ... both being highly centralised organisations in which small cadres decide who is adequate and who is not, meaning that anyone disagreeing with the party is treated by the pro-Government media as anti-Macedonian, traitors, and Western protagonists.”

> “It is a procedure essentially equal to what happened in the communist era, where people were routinely labeled interior enemies and dissidents. Ideologically, while the current party may be opposed to communism in favour of a nationalistic strategy, it is merely a change of perspective.”

Jasna is author of Communist Intimacy, a look at the nature of surveillance in Central and Eastern Europe during the socialist era. “Generally, as we all know, in most cases, it is [now] unimportant to have a huge number of actual informers on the field, since technology is already much better developed,” notes Jasna. “In all 46 years (1945-1991) of communist Macedonia the total official number of personal communist files is 14,572 (unofficial sources claim more than 50,000 files). The number of direct snitches in communist Macedonia was estimated at 12,000 to 40,000.”

Now, in a country of 2 million people, 20,000, or one in a hundred, were allegedly having their conversations recorded.

Jasna shared her in-depth analysis on the subject for Privacy International's blog.





Graffiti in Central Skopje, 2015. Privacy International

How did this happen?

Macedonia is an eager candidate for membership of the European Union. As with other candidate countries, EU candidacy weighs heavily on the internal politics and management of the State. The surveillance scandal and related protests led to an investigation by a group of senior rule of law experts appointed by the European Commission and an EU-brokered settlement among the two main parties, known as the Przino agreement. The agreement led to a Special Prosecutor being appointed to establish the factual evidence behind the surveillance, and to Prime Minister Gruevski agreeing to step down and call elections this year, in which he is eligible to run. Originally planned for April, the elections are now scheduled to take place on 5 June 2016.

Katica Janeva, endorsed by all the parliamentary political parties and appointed in September as the Special Prosecutor, is charged with investigating the wiretapping. Already however, pro-government media have been critical of the appointment, while the ruling party has said that it "no longer believes in her independence" and has "serious reservations" on the "legality of her actions."

One of the main tasks of the Special Prosecutor is to ascertain how such widespread unlawful wiretapping could occur and for so long.

Privacy of communications is expressly guaranteed in Article 17 of the 1991 Macedonian Constitution, which states that "the freedom and confidentiality of correspondence and other forms of communication is guaranteed. Only a court decision may authorize non-application of the principle of the inviolability of the confidentiality of correspondence and other forms of communication, in cases where it is indispensable to a criminal investigation or required in the interests of the defence of the Republic."

In 2005, a Law on Electronic Communications was first introduced to govern the relationship between the telecom operators and Government agencies entitled to access intercepted communications, undergoing several changes until a new law was introduced in 2014. Article 175 obliges operators to install the technology necessary for real-time interception of communications.

In 2010, the Ministry of Transport and Communications proposed an amendment to the law forcing telecommunications operators to provide direct and uninhibited access to traffic and other kinds of data to the Ministry of the Interior without prior notice or a court order. After its adoption, the constitutional court in Macedonia repealed the amendment following a petition by NGOs. However, Filip Stojanovski, a Program Director at the NGO Metamorphosis, which had challenged the amendment at the time, believes that the scandal shows that the court's decision was simply not followed.

The European Commission experts' report cites the Law on Electronic Communications as directly responsible for enabling the UBK to have direct access to the telecommunications networks:

Acting on the basis of Articles 175 and 176 of the Law on Electronic Communication, each of the three

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.***

From the point of view of technical capability, the UBK holds the ***monopoly over the use of surveillance*** *in both intelligence and criminal investigations. Surveillance is executed and monitored exclusively by the UBK on its own behalf, and also on behalf of the Police, Customs Administration and Financial Police.* ***Therefore the UBK has the means to interfere in criminal investigations and, indirectly, to undermine the independence of the leader of the investigation*** *(ie. the prosecutor).*

Direct Access

Providing government agencies with uninhibited, direct access to telecommunications networks is a major but murky issue within the telecommunications sector, and one which they must confront.

In Macedonia, the telecommunications sector is dominated by companies operating under the global T-Mobile brand.

The formerly State owned Makedonski Telekom leads the provision of Fixed-line services. Their shares are 51% owned by Hungarian operator Magyar Telecom, which itself is a subsidiary of Deutsche Telekom, one of the world's leading telecommunications companies and the entity behind the T-Mobile brand.

After a process taking several years, on 1 July 2015 Makedonski Telekom merged into one legal entity with its subsidiary T-Mobile Macedonia, which had been the leading mobile operator in Macedonia.



Skopje city centre, 2015. Privacy International

Deutsche and Magyar Telekom declined to answer Privacy International's specific questions relating to the scandal, saying that Magyar had launched its own internal investigation.

Little is publicly known about how prevalent the provision of direct access by operators to State agencies is.

While there are technical standards across Europe for “Lawful Interception” codified by the European Telecommunications Standards Institute (ETSI), handover standards from the network to the agencies are premised on cooperation between telecommunications operators, Law Enforcement Agencies, and the provision of warrants or orders by authorised bodies.

Other standards, such as the Russian “SORM”, work to different specifications. In Russia and many formerly socialist countries that base their telecommunications and interception architecture on SORM, the system is more intrusive in that telecommunications companies have little meaningful opportunity to monitor and control state agencies' interception activities and/or mediate the access the state agencies have to the data of individuals using their networks.

Last year, one of the world's largest operators, Vodafone, revealed that some governments also had direct access to its networks, with no oversight by Vodafone.

In most countries, Vodafone maintains full operational control over the technical infrastructure used to enable lawful interception upon receipt of an agency or authority demand. However, ***in a small number of countries the law dictates that specific agencies and authorities will 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.*

Typically, the operators run their network on infrastructure consisting of switches, routers, and other nodes provided by large equipment vendors such as Ericsson, Cisco, Huawei, or Nokia. This equipment is generally designed to be compliant with lawful interception standards. For example, switches integral for ensuring that telecommunications networks function are themselves commonly used to forward intercepted data or content to a monitoring facility.

Some companies provide services and systems that are specially designed for lawful interception, such as monitoring centres in which law enforcement agencies receive intercepted material, and retention and mediation suites specially designed for lawful interception.

Other companies design and sell probes which passively collect and forward intercepts to agencies without the need to use network nodes, while other companies provide systems for passive collection of data on an indiscriminate, mass scale.

For more information on how different interception architecture functions, Privacy International has an analysis available here.

Although it has been established by the EU investigation that the UBK in Macedonia had themselves direct access, it has not been established how this was carried out technically and which companies provided the necessary equipment.



Skopje city centre, 2015. Privacy International

Who Provided the Surveillance Technology?

It is the job of the Special Prosecutor to ascertain how the interceptions were conducted technically, using which technology, and who it was provided by.

One of the first investigations undertaken is into claims that the surveillance equipment required to carry out the wiretappings was provide by an Israeli company.

In April last year, the opposition released an intercept which they allege shows that the head of the UBK demanded a payment of € 500,000 from a representative of the Israeli Ministry of Defence to proceed with the purchase, totalling some €14 million.

The Macedonian Interior ministry publicly claimed that the money was simply “a donation from our partner services in the Israeli government.”

The recording with what is alleged to be the Israeli middleman, some of which is in English, is still available online.



Recording alleged to show discussion between representitives of Gruevski and Israeli Ministry of Defence. YouTube

A little-known Slovenian manufacturer of telecommunications and surveillance equipment has been engaged in a variety of lawful interception projects in Macedonia.

Iskratel in Macedonia has implemented projects allowing for the lawful interception of the fixed-line network of Makedonski Telekom, and has carried out projects ensuring the lawful interception of various of their network nodes, including a node which allowed for IP Lawful Interception and the development of software used to visualise intercepted data on SORM3 protocols, according to records seen by Privacy International.

Based in Kranj, Slovenia, Iskratel develops and sells IP and fixed-line Lawful Interception (LI) systems to customers across the world. It has been represented at the world's most notorious closed conference on electronic communications surveillance, ISS World, in 2014 and 2015 where it presented on its Lawful Intercept solutions. In June this year, it invited delegates at ISS World to visit their stand saying that it was “strengthening solutions portfolio in the field of Legal Interception for Telecom Operators and Agencies. This year at ISS we will present scalability extensions to Iskratel’s lawful interception solution and a new SI3000 based IP LI in Data Retention All-in-one solution.”

Their brochures, below, advertise both their retention suites for fixed-line Lawful Interception, and their internet interception system.

For lawful interception, Iskratel built a universal, highly flexible traffic-monitoring solution. The solution supports ETSI LI, SORM2 and SORM3 recommendations, and can be used in various IP-based networks – either fixed or mobile, either wired or wireless. The solution is based on the big-data concept – a concept that includes tools, processes and methods that a LEA needs to handle the new traffic types, large amounts of data and storage facilities.

SORM2 is the Russian-based interception standard which applies to all IP traffic, while SORM3 "takes care of collecting all communications, their long-term storage and access to all subscribers' data," according to Andrei Soldatov, a leading authority on the SORM standards.

Iskratel describes itself on its Macedonian website as "the major provider of Telecommunication equipment in Republic of Macedonia in the last 60 years and leading system integrator for design, implementation and maintenance of ICT solutions."

When asked to respond to our analysis, Iskratel replied to say that their "systems must, correspondingly with laws of each country, also ensure the so-called "lawful interception" functions. While confirming this, we can assure you, that Iskratel was never conducting or was a part of any interceptions, legal or not. Iskratel is firmly against any and all means of unauthorized interception."



Iskratel offices, Skopje, 2015. Privacy International



Seminar on the mandate of the Special Prosecutor, Skopje, 2015. Privacy International

---

How to fix this

“There is no legal mechanism that can fix this,” says an audience member to Zarko Trajanovski, a human rights law expert, activist, and blogger, at a public seminar on the scandal in the Holiday Inn in Skopje. “We have surpassed the doings of Fidel Castro.”

There is of course no single solution to ensure that the type of wiretapping seen in Macedonia doesn't reoccur in Macedonia or elsewhere. Zarko, however, points out that any solution must be holistic in nature, requiring reform of all of the Macedonian authorities and institutions, and organised action by all groups in society. As the EU Commissions' Group of Senior Experts' review makes clear, the problem is not that the legal framework governing surveillance in Macedonia is inadequate, but that there is a “considerable gap between legislation and practice,” and specifically a “lack of proper, objective and unbiased implementation.”

Zarko also agrees that foreign companies such as Deutsche Telekom played a role in the scandal and have a role to play in the solution.

Network operators providing direct access to state agencies should not be allowed under any circumstances. The large multinational network operators, far from being innocent providers of services which governments take advantage of, must take strong, concerted action in order to ensure that they are not complicit in wide-scale abuses. Transparency reports are a good start, but proactive action such as legal challenges and industry-wide initiatives must be prioritized.

In addition, it is essential that the trade in lawful interception-related and other surveillance technology, which often sits on top of the network infrastructure itself, be better regulated. If the legal framework in a country is inadequate, or the record of a customer shows that they are complicit in human rights abuses, surveillance systems should not be provided to them given the risk of their abuse or use in violation of international human rights law.

As the ongoing wiretapping affair in Macedonia shows, the implications of surveillance on such a mass scale can be devastating. The ruling party has been able to exert an enormous amount of political control over every sector and institution in Macedonia, including the media, civil society, judiciary, and civil services, empowered by the intelligence it has gained from using modern telecommunications surveillance techniques. As the EU experts' report concludes:

The scale of the unlawful recording of conversations, the concentration of power within the [Administration for Security and Counterintelligence] UBK, the over-wide remit of the UBK's mandate (which, despite its considerable breadth, was nevertheless exceeded) and the dysfunctional external oversight mechanism have resulted in a number of serious violations:

> - *Violation of the fundamental rights of the individuals concerned;*
> - *Serious infringements of the personal data protection legislation;*
> - *Violation of the 1961 Convention on Diplomatic Relations (Vienna Convention), given that diplomats have also been illegally intercepted;*
> - *Apparent direct involvement of senior government and party officials in illegal activities including electoral fraud, corruption, abuse of power and authority, conflict of interest,*
>
>   *blackmail, extortion (pressure on public employees to vote for a certain party with the threat to be fired), criminal damage, severe procurement procedure infringements aimed at gaining an illicit profit, nepotism and cronyism;*
> - *Indications of unacceptable political interference in the nomination/appointment of judges as well as interference with other supposedly independent institutions for either personal or political party advantages.*

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

Ensuring that this does not happen again in Macedonia or elsewhere requires a holistic, comprehensive approach, reliant on ensuring that appropriate legal frameworks in line with international human rights standards exist, that States have good levels of governance with transparent institutions and an accountable security sector, that industry takes a pro-active role, and that individuals have access to secure networks and devices and know how to secure themselves. Safeguards to stop the export of surveillance systems and make the industry more transparent can and must also form part of this solution. Externally, it is up to the EU and its Member States to take the first steps to ensure that European companies do not only undermine individuals' human rights, but also that the very policies that they themselves are pursuing in Macedonia through the enlargement process are not also undermined.

Privacy International will be working with industry and regulators to try to ensure thatprohibit systems where intelligence agencies are provided with direct access to telecommunictions networks, such as in Macedonia, do not exist, and that to develop international standards for surveillance that protect individuals' right to privacy from such abusive practices.

It is in Macedonia however, where redress and progress needs to be achieved. This is now the job of the Special Prosecutor, journalists, civil society, politicians, and its citizens.

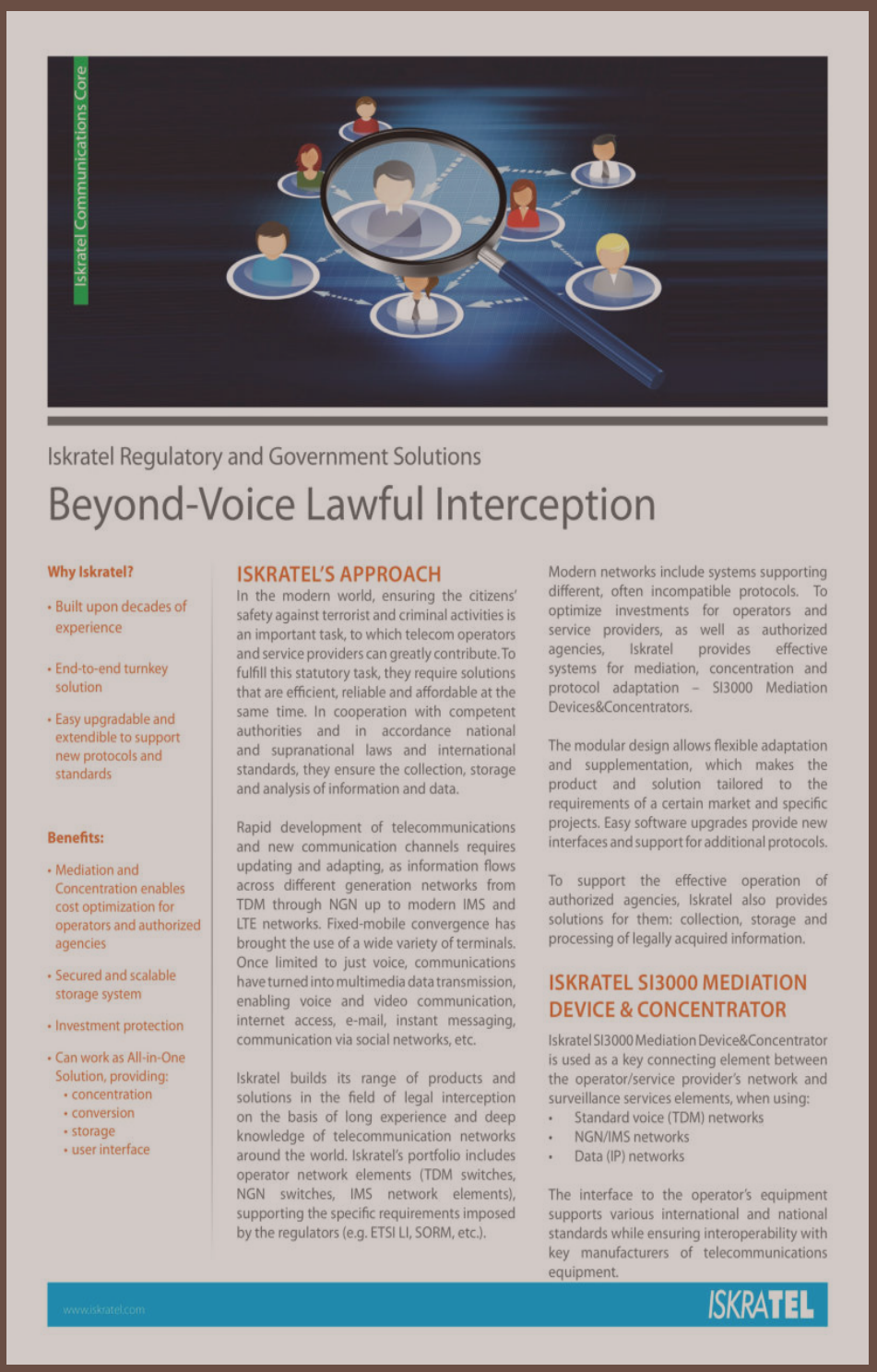


Skopje, 2015. Privacy International



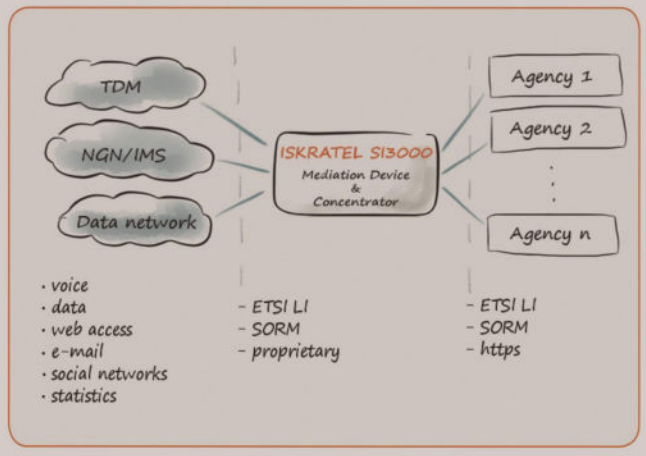


Skopje, 2015. Privacy International



Key features:

- Suitable for all types of operators/service providers
- Independent of underlying technology
- Flexibility and fast project adaptation
- Variety of supported standards and interfaces (ETSI LI, SORM, SORM-2, SORM-3...)
- Scalability
- Redundancy and Georedundancy



EVOLUTION AND MODULARITY

The system allows for flexible placement in the network and can be upgraded according to the operator's needs and regulatory requirements. Collection, storage and transmission of voice communication data is further supplemented by gathering information on different types of data traffic. At the same time the system ensures collection and storage of statistical data (data retention).

RELIABILITY

The solution is based on carefully selected components. Its modular design allows for efficient start-up packages for small operators. The basic variant of the system is unduplicated, and a duplicated one is used for larger configurations. A georedundant version is also available. The software design allows upgrading without any downtime or impact on the users' work.

CONNECTION TO AUTHORIZED AGENCIES

The interface towards agencies supports many international and national standards as well. Modular design allows for quick and efficient adaptation to specific requirements. Thus, in addition to the standard (such as ETSI LI and SORM) interfaces, the https interface can be used, ensuring adaptation to specific customer wishes. The information collected can be simultaneously sent to multiple agencies, with mutual independence provided.

Flexible design makes the system fit for use in networks of different types and generations. Software upgrade allows supplementing functionality in compliance with new regulatory requirements and network development. The user interface is easily customizable to meet the subscriber's needs. Security mechanisms prevent unauthorized use.

ISKRATEL Group

Iskracom, Naurizbay batyra 17, office 213, 050004 Almaty, Kazakhstan, phone: +7 727 244 82 22, fax: +7 727 244 82 19, e-mail: info@iskracom.kz, www.iskracom.kz
Iskratel, Ljubljanska cesta 24a, SI 4000 Kranj, Slovenia, phone: +386 4 207 20 00, fax: +386 4 202 26 06, e-mail: info@iskratel.si, www.iskratel.com
Iskratel Baku, Fazail Bayramov str. 2, kvartira 2, AZ1025 Baku, Azerbaijan, phone: +994 12 496 73 71, e-mail: info@iskratel.az, www.iskratel.az
Iskratel Bosnia and Herzegovina, Kulovića 3/IV, 71000 Sarajevo, BiH, phone/fax: +387 33 225 602, e-mail: emir.cengic@iskratel.si, www.iskratel.com
Iskratel Moldova, Teatralniy pereulok 15, Kishinev, Moldova, phone: +373 22 20 03 03, fax: +373 22 21 00 02, e-mail: iskratel@mtc.md, www.iskratel.com
Iskratel Poland, Legnicka str. 55/4, 54-203 Wrocław, Poland, phone: +48 71 349 29 05, fax: +48 71 349 29 02, e-mail: m.trzcinski@iskratel.pl, www.iskratel.com
Iskratel Tashkent, pr. Amira Temura, 99A, 100084 Tashkent, Uzbekistan, phone: +998 71 234 38 89, e-mail: sharifov@iskratel.si, www.iskratel.com
Iskratel Turkey, Bestekar Sevki Bey Sokak No 34, Balmumcu Besiktas Istanbul 34349, Turkey, phone: +90 212 211 1020, e-mail: samo.ivancic@iskratel.si, www.iskratel.com
Iskratel Ukraine, Artema str. 72a, 04050 Kiev, Ukraine, phone: +380 44 394 50 00, fax: +380 44 394 50 12, e-mail: itu@iskratel.si, www.iskratel.com
Iskrauraltel, Komvuzovskaya str. 9a, 620137 Ekaterinburg, Russian Federation, phone: +7 343 210 69 51, fax: +7 343 341 52 40, e-mail: iut@iskrauraltel.ru, www.iskrauraltel.ru
ITS Iskratel Skopje, Kej 13 Noemvri, Kula 4/2, 1000 Skopje, Macedonia, phone: +389 2 323 53 00, fax: +389 2 312 05 58, e-mail: info@its-sk.com.mk, www.its-sk.com.mk

© Iskratel, March 2015



Iskratel Regulatory and Government Solutions

Data-Network Lawful Interception

Why Iskratel?

- Built upon decades of experience
- End-to-end turnkey solution
- Easy upgradable for investment protection
- Extendible to support new protocols and standards

In a modern world, we exploit high-tech communications to stay connected to the internet at all times from any imaginable place, using services like email or social networks.

Just as we exploit the broad availability and ease of communication, so do the terrorist groups and organised criminal networks: they exchange information over the same data and voice communications channels.

A NEED FOR ACTION

Growing concern over global terrorism, criminal activities or electronic fraud, makes the ability to catch related network traffic and isolate it for in-depth analysis of great importance. The law-enforcement agencies (LEAs) now require the ability to focus on individual subscribers and to monitor the source of data traffic, its destination, and its contents.

The carriers have no choice but to implement the technology that allows deep inspection, without impacting the performance or integrity of customer traffic.

ISKRATEL'S LI SOLUTION

For lawful interception, Iskratel built a universal, highly flexible traffic-monitoring solution. The solution supports ETSI LI, SORM2 and SORM3 recommendations, and can be used in various IP-based networks – either fixed or mobile, either wired or wireless.

The solution is based on the big-data concept – a concept that includes tools, processes and methods that a LEA needs to handle the new traffic types, large amounts of data and storage facilities.

THE MAIN INGREDIENT: MD

The primary building block of the solution is the mediation device (MD). Deep packet inspection (DPI) supports complex traffic classification and decoding of contents. The MD is compliant with network equipment of different vendors and functions with various network probes.

An easy-to-use graphical user interface provides users with tools for monitoring the system actions and collection of monitoring results.

The MD allows interconnection to multiple LEAs over its northbound LI handover interfaces (like HI interfaces, SORM interface, or secure HTTP interface).

Key Features

- Pattern matching and behavioural analysis
- Integrated DPI
- Local storage for lossless high-speed interception
- Passive and active solution options
- Applicable in different network models
- Interconnection to multiple agencies
- Supports multiple users with different authorizations
- Supports ETSI LI, SORM2, SORM3
- Adaptable to support other standards

FUNCTIONALITIES OF MD

The MD provides three functional layers necessary for efficient legal interception.

- **Administration function** enables users to control the system, set up interception rules and manage LI requests;
- **Mediation function** executes the LI requests and communicates with network interception probes;
- **Presentation function** analyses the intercepted traffic and presents the results of analysis to the LEA(s).

Passive LI approach

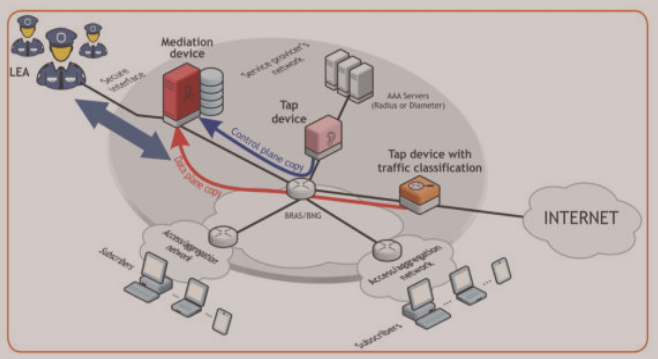
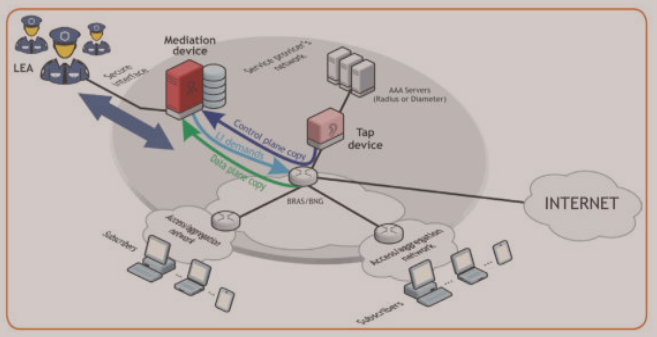


Figure shows the passive approach to LI process, with an overlay infrastructure (using taps) for control and data plane traffic replication. Intercepted traffic is forwarded for content processing to the mediation device.

Active LI approach



Active LI approach involves target traffic filtering and replicating for analysis in core or edge routers, which are participating in production network. This approach enables filtering and replication on any router interface, and for any encapsulation.

ISKRATEL Group

Iskracom, Naurizbay batyra 17, office 213, 050004 Almaty, Kazakhstan, phone: +7 727 244 82 22, fax: +7 727 244 82 19, e-mail: info@iskracom.kz, www.iskracom.kz
Iskratel, Ljubljanska cesta 24a, SI 4000 Kranj, Slovenia, phone: +386 4 207 20 00, fax: +386 4 202 26 06, e-mail: info@iskratel.si, www.iskratel.com
Iskratel Baku, Fazail Bayramov str. 2, kvartira 2, AZ1025 Baku, Azerbaijan, phone: +994 12 496 73 71, e-mail: info@iskratel.az, www.iskratel.az
Iskratel Bosnia and Herzegovina, Kulovića 3/IV, 71000 Sarajevo, BiH, phone/fax: +387 33 225 602, e-mail: emir.cengic@iskratel.si, www.iskratel.com
Iskratel Moldova, Teatralniy pereulok 15, Kishinev, Moldova, phone: +373 22 20 03 03, fax: +373 22 21 00 02, e-mail: iskratel@mtc.md, www.iskratel.com
Iskratel Poland, Legnicka str. 55/4, 54-203 Wroclaw, Poland, phone: +48 71 349 29 05, fax: +48 71 349 29 02, e-mail: m.trzcinski@iskratel.pl, www.iskratel.com
Iskratel Tashkent, pr. Amira Temura, 99A, 100084 Tashkent, Uzbekistan, phone: +998 71 234 38 89, e-mail: sharifov@iskratel.si, www.iskratel.com
Iskratel Turkey, Bestekar Sevki Bey Sokak No 34, Balmumcu Besiktas Istanbul 34349, Turkey, phone: +90 212 211 1020, e-mail: samo.ivancic@iskratel.si, www.iskratel.com
Iskratel Ukraine, Artema str. 72a, 04050 Kiev, Ukraine, phone: +380 44 394 50 00, fax: +380 44 394 50 12, e-mail: itu@iskratel.si, www.iskratel.com
Iskraraltel, Komvuzovskaya str. 9a, 620137 Ekaterinburg, Russian Federation, phone: +7 343 210 69 51, fax: +7 343 341 52 40, e-mail: iut@iskrauraltel.ru, www.iskrauraltel.ru
ITS Iskratel Skopje, Kej 13 Noemvri, Kula 4/2, 1000 Skopje, Macedonia, phone: +389 2 323 53 00, fax: +389 2 312 05 58, e-mail: info@its-sk.com.mk, www.its-sk.com.mk

© Iskratel, March 2015

Click for larger image

Disclosure: Privacy International is also partly funded by the Open Society Foundation

Authors:

Edin Omanovic

Date:

23 March 2016

Iskratel1.jpg

Iskratel2.jpg

Iskratel_4.jpg

Iskratel_3.jpg

Privacy International | Registered Charity Number: 1147471
62 Britton Street, London, EC1M 5UY | +44 (0) 20 3422 4321

Get email updates

your@email.com

Join!