MAJOR CIVIL SOCIETY CONCERNS RELATED TO THE REFORM OF MACEDONIA'S SYSTEM FOR INTERCEPTION OF COMMUNICATIONS.

As civil society organizations working on monitoring and supporting the implementation of the Urgent Reform Priorities in Macedonia, we welcome the resolve of the new Government to initiate reform of the system for interception of communications that would address the relevant issues outlined by the European Commission. However, in this document we would like to point out some of the major civil society concerns with regard to the proposed legal amendments that the Government has sent to Parliament.

Failure to align the new laws with relevant EU acquis. The drafts are not aligned with the General Data Protection Regulation, the Police and Criminal Justice Data Protection Directive 2016/680, other European standards and the relevant case law of the European Court of Justice and the European Court of Human Rights.[1] This is especially troubling as the reform is conducted, among other things, in order to address the EU's concerns related to national laws and practice in this field.

Non-transparent introduction of technology for communication interception that bypasses the telecom providers and the OTA. Articles 17 and 34 of the draft Law on Interception of Communications introduce special technology for interception of communications bypassing the system of the newly proposed Operational-Technical Agency (OTA) and the telecom providers. The draft does not specify the exact technology covered with this article, though it may, among other things, refer to IMSI catchers.[2] This type of equipment was rumored to have been used in the past to illegally intercept communications of, among others, NATO countries' diplomats and embassy staff. However, legalizing the use of such equipment negates the rationale for creation of the OTA,[3] and renders the reform meaningless. As the state will anyhow retain access to the signal from the telecom providers, it is difficult to imagine scenarios in which there would be a legitimate purpose for utilizing IMSI catchers.[4] Furthermore, the draft fails to put forward effective measures for oversight and control of the use of such equipment, including an electronic register that will allow permanent logging of its activation and deactivation, and of its targets. The current text of Articles 17 and 34 was absent from the version of the draft law that was consulted with the public and was added later in the version sent by the Government to Parliament without explaining the rationale for its introduction. We thus fear that these articles may enable authorities to bypass the safeguards against illegitimate surveillance. No privacy impact assessment was conducted in relation to these proposed articles, which is contrary to the requirements set out in Article 27 of the EU's Police and Criminal Justice Data Protection Directive 2016/680 and Article 35 of the General Data Protection Regulation.

Doubts whether the draft laws address the key concerns of the EU. According to the reform, the direct access to the communications of every citizen would be in the hands of the Operational Technical Agency (OTA) – an institution that will have the authorization to redirect the signal to the bodies for interception of communications. Article 2 of the draft Law on the OTA states that the Agency will not activate the interception of communications or record the communications. However, Article 3 of the same draft law stipulates that the Agency will have the power to activate the signal, and a Ministry of Interior employee stated on a meeting with civil society organizations held on December 22 2017 that OTA will nonetheless

[1] The proposed laws are to be implemented by November 2018, which is well after the deadline for transposition of the mentioned Directive/application of the Regulation.
[2] Devices which imitate mobile towers of telecom providers. Used for intercepting mobile phone traffic and tracking location data of mobile phone users.
[3] OTA is supposed to act as a gatekeeper between the citizens' communications transmitted by the telecom providers and the state institutions authorized to perform surveillance.
[4] Or other controversial surveillance technologies, such as FinFisher, which the authorities reportedly possess.

record the intercepted communications. Such arrangement does not address the requirements set out in the Urgent Reform Priorities and the suggestions by the expert group led by Reinhard Priebe that clearly recommend that the telecommunication providers should activate and divert the signal to the authorized bodies, only after receiving a court order.[5] Furthermore, OTA will be partly staffed by UBK[6] personnel – the institution that has massively and illegally intercepted communications in the past – who would now be expected to act as gatekeepers ensuring legal access for their former colleagues from the UBK. Regarding newly hired OTA personnel – i.e. those that will not be transferred from the UBK – UBK will retain the final say on their employment in OTA due to the simple fact that it will perform their security clearance checks. To summarize, we share the doubts expressed in the Priebe report from 2017 on "whether such centre [OTA] could withstand political influence and pressure in a way that the established institutions in the country have been unable to withstand", as we can't identify sufficient safeguards in the draft laws.

Wide range of authorizations for interception of communications related to *"protection of the country's interests in defense and security"*. The existence of these special provisions in the draft Law on Interception of Communications is unwarranted as such crimes are already covered with the articles for interception of communication as a special investigative measure, including in instances of serious crimes against the state order, terrorism, etc. The explanation of the Government that such special provisions are needed for preventive purposes does not hold ground – the special investigative measure of interception of communications can also be authorized for preventive purposes, i.e., for revealing such criminal offences which are under preparation or whose execution is ongoing. Thus, the wide authorizations for interception of communications related to *"protection of the country's interests in defense and security"* may be used to bypass the safeguards associated with the use of special investigative measures and target political opponents, media or civil society activists. This concern arises from Article 28 of the draft Law on Interception of Communications, which stipulates that the intercepted communications for defense/security purposes may be used as an indication for criminal prosecution unrelated to defense and security matters. Additionally, in matters of state defense and security the authorities will also have the possibility to obtain metadata directly from telecom providers, without an order from a judge or prosecutor. This goes against article 17 of Macedonia's Constitution which stipulates that the secrecy of citizens' communications can be breached only with a prior court order. Additionally, the draft Law on Interception of Communications expands the scope for interception related to "defense/security" matters by adding crimes against the armed forces in this category – a broad spectrum of criminal offences, some of which carry a prison sentence of as little as 3 months. This goes against relevant international law that specifies that communications interception – as a highly intrusive measure affecting the private lives of individuals – may be allowed in instances of serious crime. The United Nations define serious crimes as ones that carry imprisonment of four or more years. Furthermore, in the version of the Draft Law on Interception of Communications sent to Parliament, the Government has reduced the time that judges have to decide on requests for interception related to "defense/security" issues from 24 to mere 12 hours. The public was not consulted on this change, as it was absent from the original version of the draft law that the Government published for consultation.

Expanding massive geo-tracking of all citizens. The existing Law on Electronic Communications already obliges telecom providers to retain metadata for all of their users for 12 months[7] – including location data. Article 4 of the draft law on amending the Law on Electronic Communications expands this massive surveillance even further. It obliges providers to retain additional location data for all users for up to 72 hours, regardless of whether the users are engaging in any communication activities. The amendment to this article was not published for public consultation and without explanation was added later in the version of the draft law that the Government sent to Parliament.

Removing the right of the Parliamentary oversight committee to summon the officials of the competent authorities for interception of communications. Article 40 of the draft Law on Interception of Communications published for public consultation empowered the Parliamentary oversight committee to

[5] Pribe 2015 report.
[6] National security service.
[7] Which runs against the verdict of the European Court of Justice to abolish the Data Retention Directive due to massive and disproportionate infringement on citizens' privacy (Case C-293/12 and 594/12).

summon the officials of the competent authorities, as well as the telecom providers' executives and employees. This was meant to prevent the repeat of past incidents when officials refused to appear in front of the Committee. Without any explanation this article was later removed in the version of the draft law that the Government sent to Parliament.

Broad expansion of the scope for intercepting communications of third persons. Article 7 of the draft law on amending the Criminal Procedure Law seeks to expand the interception to also cover the families and "close persons" of people under reasonable suspicion. Such broad wording creates the risk for massive surveillance of citizens and illegitimate invasion of their privacy. The new wording of this article was not published for public consultation and without explanation was introduced later in the version of the draft law that the Government sent to Parliament.

Unreasonable time-limits for storage of intercepted communications. According to Article 16 of the draft Law on Communication Interception, the intercepted communications shall be stored until the criminal prosecution deadlines have expired – even in instances where the court reaches a verdict to release the accused from charges or to reject the charges. In instances of interception related to *"protection of the country's interests in defense and security"*, the draft proposes that the communications shall be stored for up to 3 years, but this period may be restarted in *"instances where new important information is obtained"*.[8] This actually removes any meaningful safeguards against unreasonably lengthy or even perpetual storage of intercepted communications – which from a privacy viewpoint is unacceptable – and expands the risks for improper usage of such personal data.

Bypassing the Parliamentary oversight committee in the procedure for adoption of the new laws. By law, Parliament's communication interception oversight committee is presided by the opposition, and this committee has traditionally discussed amendments to the relevant laws. However, during the ongoing reform, the parliamentary majority designated the Parliamentary committee on defense and security as the competent committee for the draft laws.[9] The Defense and security committee is traditionally presided by the political parties in power. We are concerned that the bypassing of the key committee on these matters during the Parliamentary debate on the laws may undermine the credibility and the success of the reform.

Association for Development Initiatives – Zenith
Institute of Social Sciences and Humanities, Skopje (ISSHS)
European Policy Institute – Skopje (EPI)
Analytica think tank

[8] Article 29, draft Law on Interception of Communications.
[9] The draft Law on Interception of Communications and the draft Law on the OTA.