**Privacy International's submission in advance of the consideration of the periodic report of Uzbekistan, Human Rights Committee, 114th Session, 29 June – 24 July 2015**

1 June 2015

## 1. Introduction

In Uzbekistan, pervasive government surveillance of personal communications and control over the internet infringes on the right to privacy, as well as the right to freedom of expression, association and peaceful assembly.

State surveillance plays a significant part in the government's widespread repression of human rights, leading to the arbitrary arrests and prosecutions of human rights defenders, independent journalists, and political opposition figures in the country. Uzbekistan has failed to adopt laws to effectively regulate the activities of its powerful National Security Service (SNB.) The SNB regularly unlawfully interferes with the right to privacy of individuals. In some cases information gathered through unlawful surveillance has been used as evidence against political opposition activists, journalists and human rights defenders in criminal proceedings motivated by the desire of government authorities to stifle legitimate dissent and intimidate those reporting on the government's human rights violations and other abuses.

The government's tight control of the state-owned telecommunications network, private internet service providers, and mobile phone companies assists the security services in intercepting individuals' communications and accessing users' personal data. The communications and online activities of political activists have been especially targeted by the intelligence services, while strict regulations of the use of internet cafes and other measures have significantly curbed the capacity of individuals to communicate anonymously.

Control over the internet and knowledge of the security services' surveillance activities causes fear and results in self-censorship by activists and journalists, as well as the wider internet community. Sensitive issues relating to human rights and politics are avoided, which significantly limits public discourse on these topics.

## 2. Uzbekistan's failure to effective protect privacy and to limit state communication surveillance in its laws

Article 27 of the 1992 Uzbekistan constitution guarantees the privacy of "written communications and telephone conversations". However, there is no data protection law in Uzbekistan.

The Uzbekistan criminal procedure code provides for search and seizure of post and telegraph communications and wiretapping of telephone or other communications of persons under criminal investigation upon authorisation by the prosecutor or a court (Articles 166-170).[1]

There appears to be no reference in the criminal procedure code to ex-post judicial oversight or scrutiny of the activities conducted on the basis of the warrants. There is no restriction on the duration of warrants. In the absence of any law on data protection, there do not appear to be any provisions regulating the use or destruction of intercepted material or personal data after the surveillance has ceased. No provision is made in the legislation for dealing with confidential or privileged material. Further, there are no regulations governing or restricting the retention and storage of and access to intercepted material.

Outside of the surveillance powers pertaining to criminal investigation proceedings, in December 2012 Uzbekistan adopted a law on surveillance activities, which had previously been largely unregulated. However, the law on "Operational and Investigative Activity" fails to provide necessary protections against arbitrary interference with the right to privacy and the right to freedom of expression. In particular, there is no system of independent oversight, heightening the risk that surveillance powers will be abused and unlawful interception of personal communications will occur, and enabling the intelligence services to operate outside public scrutiny. Significantly, surveillance activities conducted outside criminal investigations are not subject to judicial authorisation and there is no requirement to notify individuals who have been under surveillance.[2]

As a result of this lack of effective regulation, surveillance being carried out by State security or law enforcement authorities outside the context of a targeted criminal investigation lead to unlawful interference with the right to privacy, in violation of Uzbekistan's obligations under Article 17 of the ICCPR.

## 3. Unlawful interference with the right to privacy

1 See Criminal Procedure Code of the Republic of Uzbekistan, http://www.legislationline.org/download/action/download/id/1713/file/d6356a54f81eebad3ba253f23eac.htm/preview

2 See Freedom House, Freedom on the net 2014.

The National Security Service (SNB) operates in this context of weak or non-existent domestic legal and policy framework to limit interference with the privacy of personal communications.

SNB is currently Uzbekistan's lead intelligence agency. Established in 1991 as the successor agency to the Soviet Union KGB, it reports directly to the president with a mandate to concentrate on internal security, counter-espionage and anti-terrorism. Its mandate also includes working on the development of technical measures related to national security, such as standardisation, licensing, and certification in the field of encryption of digital communications. The SNB have been involved in wide-scale human rights violations. The 2005 Andijan Massacre, which took place outside of the SNB headquarters building, saw SNB officers fire indiscriminately, killing hundreds.

State surveillance (together with tightened control on the media and on-line activities) significantly intensified following the Andijan Massacre in 2005. Survivors, including refugees who fled in the aftermath of the massacre, have been subsequently targeted by the SNB and placed under extensive surveillance.[3] The SNB systematically eavesdrops on citizens' communications over e-mail, mobile phone and Skype, in online forums, and social networks. There is no independent oversight to guard against abusive surveillance, leaving the SNB wide discretion in its activities.

Numerous political activists, journalists and human rights defenders living in Uzbekistan and abroad, report that their communications have been monitored. Uzbek authorities appear to be monitoring phones calls and emails of Uzbeks working on what state authorities perceive to be politically sensitive topics. Transcripts of their private communications are used in criminal proceedings against them aimed at suppressing legitimate political dissent or criticism of the government human rights record.

In several cases Uzbek authorities appear to have obtained transcripts of Skype conversations and Uzbek activists claim to have had their Facebook and other social media accounts accessed and have been called in for questioning by SNB agents. In 2014, Privacy International documented a number of cases of unlawful interference with the right to privacy by state security services.[4]

## 4. The technical infrastructure of unlawful state surveillance: SORM and communication surveillance technologies.

Uzbekistan's internet and telecommunication infrastructure is vulnerable to such pervasive state surveillance of personal communications. The Uzbekistan telecommunication systems operate within a surveillance model adopted in Russia and other states formerly within the Soviet Union. The System of Operative Investigation Measures (SORM) provides the architecture by which law enforcement and intelligence

3 See Human Rights Watch, Saving its secrets. Government repression in Andijan, 2008, available at: http://www.hrw.org/sites/default/files/reports/uzbekistan0508webwcover.pdf
4 For more information and additional cases, see Privacy International, Private Interest, cited above.

agencies can obtain direct access to personal data on telecommunications network, including telephone and mobile networks as well as internet traffic. Unlike American and European frameworks, the SORM model requires direct access by law enforcement and intelligence agencies to the communications network.

The companies operating the communications network must install SORM and other surveillance equipment on their networks in order to obtain a license. Once operational, 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. Further, telecommunications providers face possible financial sanctions or license revocation if they fail to design their networks to accommodate state interception's capabilities.

SORM-related development work in Uzbekistan is overseen by a state-owned research centre. State Unitary Enterprise Scientific Engineering and Marketing Research Center (UNICON) is a state-sponsored research and development centre created in 1992 by decree of the Uzbek Ministry of Communication. The facility has a SORM equipment certification, testing, and development centre. The centre also handles certification for telecom companies, ICT standardization, standard protocols development and information security facilities, plus marketing research and consultancy activities.

The capacity of the Uzbekistan intelligence agencies to intercept and analyse the private communications passing through telecommunications and internet networks is provided by the use of monitoring centres.

According to research conducted by Privacy International in 2014, monitoring centres with mass surveillance capabilities have been provided to Uzbekistan (and Kazakhstan) by the Israeli branch of the US-based Verint Systems and by the Israel-based NICE Systems. These monitoring centres are capable of mass interception of telephone, mobile, and IP networks. Such a system means that the communications of every individual are within the reach of the security and law enforcement agencies. While some technical limitations to the ability to analyse intercepted material still exist, future upgrades can be made using the enabling infrastructure.

While the full range of digital surveillance techniques employed by the security services are unknown, there are reports that sophisticated malware marked by the Italian company Hacking Team is currently or has previously been in use in Uzbekistan.[5] Hacking Team's Remote Control System can be used to hijack computer and mobile devices, whilst remaining undetectable to users, as it is designed to bypass common antivirus programmes and encryption. It can covertly collect, modify and/or extract data from the targeted device, including remotely turning on and control the microphone and camera of the device. As such it is a particularly intrusive form of electronic surveillance

5 The Citizen Lab, Mapping Hacking Team's "Untraceable" Spyware, 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

given the personal information that can be obtained from such access. The company manufacturing this malware only markets it to law enforcement and intelligence agencies.[6]

## 5. Systematic on-line surveillance and limitation to on-line anonymity

Uzbek security and intelligence agencies, such as the SNB, operate in a context of pervasive government control of online communications, including blocking of access to internet sites hosting independent news and any content that is critical of the government. This control is made possible by legislation (such as the 1999 Law on Telecommunications and Order No.216 of 2004) that gives authorities wide discretionary powers to withheld, suspend or revoke licences to telecommunication companies if they fail to prevent their network from being used for disseminating information deemed to violate national legislation. Several government entities monitor and control online communications, though lack of transparency and accountability makes it impossible to establish how powers are exercised.[7]

Since July 2004, operators of internet cafes and other public internet access places have been required to monitor their users and cooperate with state bodies. Following regulatory amendments in March 2014, operators of internet cafes and public access places must install surveillance cameras on their premises as a new measure to "ensure safety of visitors." They are also required to maintain a "registry of internet web-resources (logfiles)" used by customers and to retain this information for a period of three months.[8] The OpenNet Initiative reports that SNB officers frequently visit ISPs and internet cafes to monitor compliance.[9]

## 6. Recommendations

Based on these observations, Privacy International suggests that the following recommendations are addressed to government of Uzbekistan:

- Take all necessary measures to ensure that communications surveillance and collection of personal data in Uzbekistan 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.
- Establish effective and independent oversight over the surveillance activities of law enforcement and intelligence agencies, including by requiring that every

6 For a briefing on the activities of Hacking Team, see Privacy International, Briefing for the Italian government on Hacking Team's surveillance exports, April 2015, available at: https://www.privacyinternational.org/?q=node/561

7 For an overview of these measures and their effects on access to information, see Freedom House, Freedom on the Net, 2014, and Reporters Without Borders, Uzbekistan, Enemies of the Internet 2012.

8 See Freedom House, Freedom on the Net, 2014.

9 See "CIS Overview", OpenNet Initiative, 2010, available at https://opennet.net/research/regions/cis

interception of personal communication is authorised by an independent court; and by establishing an independent oversight body with powers to review intercepted material, and recommend for prosecution individual officers or agencies suspected of abuses of authority.

- Stop the use of any technology for which there is no clear legal framework governing its use, especially intrusive technologies used to hijack mobile and computer devices.
- Maintain and regularly publish statistics on interceptions of communications and identified abuses and inform any victim of arbitrary surveillance not in keeping with constitutional protections, national legislation, or international human rights law.
- Ensure that public and private telecommunications and internet service providers can review warrants before any interception of personal data from their network takes place or whenever data related to their subscribers is requested, and that they can challenge such warrants to an independent monitoring authority or before the courts.
- Lift restrictions on anonymity and unlawful restrictions of access to information on line.