Uzbekistan

Key Developments: June 2016 – May 2017

• The government introduced a new online portal allowing citizens to channel public grievances and prompting greater citizen engagement (see Media, Diversity, and Content Manipulation).

• Following a change in Uzbekistan’s leadership, some online journalists serving lengthy sentences were released from prison, though new arrests were also reported (See Prosecutions and Detentions for Online Activities).

• Many services offering free online calls, including Skype, WhatsApp, and Viber, remain restricted (See Restrictions on Connectivity).
Introduction

The internet freedom environment in Uzbekistan remains repressive, though it improved slightly with the introduction of an online government portal allowing citizens to voice their grievances and concerns.

Following the death of authoritarian President Islam Karimov in September 2016, Shavkat Mirziyoyev took over the presidency in December 2016. Mirziyoyev promised to honor Karimov's legacy, and civil liberties remain severely restricted. However, there are some indications that the government may be willing to promote citizen engagement using online tools. The establishment of the government's “virtual office” initiative, an online platform allowing citizens to voice criticism directly to government bodies, launched hundreds of thousands of complaints, and many were successfully resolved.

A number of independent online journalists serving lengthy sentences were released from prison after Mirziyoyev came to power. Others, however, remain imprisoned, and internet users were newly detained, supposedly for causing public disorder through communication apps.

Voice over Internet Protocol (VoIP) calls, including services offered by Skype, WhatsApp, and Viber, remain largely unavailable, though both the government and service providers denied blocking them. The websites of many international news outlets have been blocked for the past decade.

Obstacles to Access

Nearly half of the population had internet access in 2016, with growing mobile penetration playing a critical role in improving access. However, expensive service, low broadband speeds, and limits on data continue to curb internet use. The state controls the country's international internet gateways through the state-owned telecommunications operator Uztelecom. Some VoIP services such as Skype, WhatsApp, and Viber remain inaccessible.

Availability and Ease of Access

<table>
<thead>
<tr>
<th>Key Access Indicators</th>
<th>2016</th>
<th>46.8%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet penetration (ITU)&lt;sup&gt;a&lt;/sup&gt;</td>
<td>2015</td>
<td>42.8%</td>
</tr>
<tr>
<td></td>
<td>2011</td>
<td>18.6%</td>
</tr>
<tr>
<td>Mobile penetration (ITU)&lt;sup&gt;b&lt;/sup&gt;</td>
<td>2016</td>
<td>77%</td>
</tr>
<tr>
<td></td>
<td>2015</td>
<td>73%</td>
</tr>
<tr>
<td></td>
<td>2011</td>
<td>90%</td>
</tr>
<tr>
<td>Average connection speeds (Akamai)&lt;sup&gt;c&lt;/sup&gt;</td>
<td>2017(Q1)</td>
<td>5.9 Mbps</td>
</tr>
<tr>
<td></td>
<td>2016(Q1)</td>
<td>3.3 Mbps</td>
</tr>
</tbody>
</table>

Internet penetration continues to rise in Uzbekistan. Internet access is based primarily on ADSL technology, which the government estimates is available to 68 percent of subscribers.¹ The remaining 32 percent use connections via fiber optic nets. Users increasingly access the internet through their mobile devices, with the number of mobile internet users reaching 14.7 million in April 2017.²

Internet connection speeds remain relatively low. Subscribers experience poor connection quality and frequent disconnections. “Unlimited” fixed-line subscriptions, advertised by all internet service providers (ISPs), actually entail quotas on traffic. If the quota is exceeded, connection speeds decrease to almost zero. Mobile providers continued to invest into 4G LTE broadband connectivity, with speeds of up to 70 Mbps offered by provider UMS.³ In general, access to the internet remains prohibitively expensive in comparison to the average household income in Uzbekistan.⁴

The capital Tashkent has the highest rates of internet penetration and of fiber-to-the-building (FTTB) broadband connectivity compared to the country’s 12 regions (viloyati) and the autonomous Republic of Karakalpakstan.⁵ Uztelecom’s FTTB broadband service reaches 4,500 buildings in Tashkent, compared to just four in Termez city in the remote Surkhandaria region on the border of Afghanistan, with a population of 136,000.⁶ The government plans to further develop broadband infrastructure, aiming to construct over 277,000 km of fiber optic nets across the country by 2021.⁷ ICT facilities also depend on a stable electricity supply to the telecommunications infrastructure, which has been less reliable in rural areas.⁸

Uztelecom and at least two private mobile operators offer public Wi-Fi hotspots in limited locations. In 2016, Uztelecom operated 67 hotspots across Samarkand, Bukhara, and four regions, including 14 in Tashkent.⁹ In February 2016, the government set a goal of extending public Wi-Fi coverage to the remaining eight regions, and the Republic of Karakalpakstan. The private mobile operator Beeline launched its first public Wi-Fi network in August 2015 and currently operates 27 Wi-Fi hotspots in 6 cities.¹⁰

Public access points such as internet cafes remain popular, particularly among young internet users.

---

⁴ As reported by ITU in 2016, internet access prices were prohibitively high in Uzbekistan and exceeded the monthly GNI per capita level at the rate of approximately 188 percent. See ITU, “Measuring the Information Society: 2016.”
¹⁰ Beeline has Wi-Fi hotspots: 16 (Tashkent), 5 (Samarkand), 3 (Samarkand), 1 (Namangan), 1 (Fergana), and 2 (Djizak), https://www.beeline.uz/uz/Catalog/Services/Wi-Fi/ru/wi-fi.
However, minors are officially prohibited from visiting internet cafes unsupervised between 10:00 p.m. and 6:00 a.m.\footnote{11}

Since September 2005, all public institutions such as educational institutions, youth organizations, libraries, and museums, must connect to the wider internet exclusively via ZiyoNET,\footnote{12} a nationwide access and information network that enables the government to monitor all communications traffic. Since July 2013, the state-owned Uztelecom has served as the exclusive provider of access to ZiyoNet.\footnote{13}

The use of mobile technology is formally restricted in schools and universities, but the restriction is enforced only during certain examinations.\footnote{14} In a May 21, 2012 resolution, the government had banned the use of mobile phones in educational institutions except in “justified and urgent” cases, in order to prevent cheating and access to banned ideology.\footnote{15}

\section*{Restrictions on Connectivity}

The government exercises significant control over ICT infrastructure. Some Voice-over-Internet-Protocol (VoIP) services, including Skype, continued to be disrupted in the past year.

Internet access is routed via Uztelecom, a state-owned telecommunications and internet access provider, and a TAS-IX peering center and content delivery network that effectively functions as a government-backed intranet. Uztelecom is an upstream ISP and sells international internet traffic to domestic ISPs at a wholesale price. Uztelecom runs the International Center for Packet Switching to aggregate international internet traffic at a single node within its infrastructure. Private ISPs are prohibited by law from bypassing Uztelecom’s infrastructure to connect to the internet, and from installing and maintaining their own satellite stations in order to establish internet connectivity.

The TAS-IX peering center and content delivery network, established in February 2004, interconnects the networks of private ISPs to enable traffic conveyance and exchange at no mutual charge and without the need to establish international internet connections via Uztelecom.\footnote{16} Private ISPs provide no traffic limitations on websites hosted within the TAS-IX networks but filter and block other websites to the same extent as Uztelecom.\footnote{17}

The authorities have been known to periodically impose temporary shutdowns. Most recently, internet users in Tashkent reported an interruption in connectivity in January 2016, after Uztelecom

\footnote{11} “О порядке предоставления доступа к сети Интернет в общественных точках доступа” [On Adoption of the Terms of Provision of Access to the Internet Network in Public Points of Use], promulgated by Order of the Communications and Information Agency of Uzbekistan No. 216, July 23, 2004, SZRU (2004) No. 30, item 350, art. 17 (e).
\footnote{12} Resolution of the President RU “О создании общественно-образовательной информационной сети Республики Узбекистан” [On the Establishment of the Public, Educational, and Information Network of the Republic of Uzbekistan], No. ПП-191, 28 September 2005, SZRU (No. 40), item. 305, at Art. 4.
\footnote{13} Resolution of the Cabinet of Ministers RU, “О мерах по упорядочению пользования мобильными телефонами в образовательных учреждениях Республики Узбекистан” [On measures to streamline the use of mobile phones in educational institutions of the Republic of Uzbekistan], No. 139, May 21, 2012, SZ RU (2013 No. 21 (521), item. 229.
\footnote{15} Resolution of the Cabinet of Ministers RU, “О мерах по упорядочению пользования мобильными телефонами в образовательных учреждениях Республики Узбекистан” [On measures to streamline the use of mobile phones in educational institutions of the Republic of Uzbekistan], No. 139, May 21, 2012, SZ RU (2013 No. 21 (521), item. 229.
\footnote{17} TAS-IX participating ISP maintain a service to find out whether a website is in the TAS-IX network. See, e.g., ISP TPS, http://www.tps.uz/tasix/
warned of disruptions for maintenance purposes; observers speculated the disturbance was related to the installation of surveillance equipment.\textsuperscript{18} The authorities also periodically order mobile operators to shut down internet and text message services nationwide to avoid cheating during August university entrance exams.\textsuperscript{19}

Some services offering free VoIP calls through the internet, including Skype, WhatsApp, and Viber, have been unavailable to users in Uzbekistan since at least July 2015, with some reports of disruptions from as early as October 2014; some users reported the apparent block was lifted briefly in October 2015. As of May 2017, the Skype website remained inaccessible from within Uzbekistan except by using a virtual private network (VPN). Experts linked the restrictions to the threat these free services pose to Uztelecom’s revenue.\textsuperscript{20} Uztelecom and the Ministry for the Development of Information Technologies and Communications, which regulates ICTs, both denied responsibility for the block. In May 2016, in an official response to a user complaint posted on an e-government website, a director of Uztelecom’s information security department said the company was “not responsible for the due or proper operability of third-party resources.” The ministry said that that “servers of multimedia services like Skype, WhatsApp, Viber, and others are located in foreign states. National ISPs (operators and providers) in the Republic of Uzbekistan might be held responsible by the law for the functioning and accessibility of segments of the internet network, however, they cannot influence the quality of the aforesaid service.”

\textbf{ICT Market}

There are numerous legal, regulatory, and economic obstacles to competitive business in the ICT sector. As of January 2017, there were 654 companies classified as providing data or telecommunications services including the internet, down from 854 in 2016.\textsuperscript{21} This figure includes internet cafes and does not indicate the number of private ISPs.

The state controls much of the telecommunications market. Five mobile phone operators share the market in Uzbekistan, including Uzmobile, a brand of Uztelecom, and three privately owned operators: Perfectum Mobile (owned by the Uzbek company Rubicon Wireless Communication), Beeline (owned by the Amsterdam-based VimpelCom), and Ucell (under the part-Swedish government owned Telia Company AB, formerly TeliaSonera). Beeline and Ucell operate 2G, 3G, and 4G mobile networks and currently lead in terms of subscribers. A fifth subscriber, UMS (Universal Mobile Services), was controlled by Russian telecom giant Mobile TeleSystems OJSC (MTS) until August 2016, when it sold that share to the Uzbek government. Telia is preparing to exit the Uzbek market.\textsuperscript{22} However, competition is expected to increase following a May 2017 decision by the

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{18} “Uzbekistan: what to do with a problem called internet,” Eurasianet, January 8, 2016, http://www.eurasianet.org/node/76741
\item \textsuperscript{19} “Отключение мобильного интернета скажется на работе терминалов,” (Disconnection of mobile internet will affect terminals) Gazeta, July 31, 2016, https://www.gazeta.uz/ru/2016/07/31/uzcard
\item \textsuperscript{20} “Why doesn’t Skype work?” UzMetronom, October 17, 2014, Uzmetronom.com, http://www.uzmetronom.com/2014/10/17/pochemu_so_skype_snjal_skalp.html
\item \textsuperscript{22} “TeliaSonera to retreat from Central Asia,” Reuters, September 17, 2015, http://www.reuters.com/article/teliasonera-eurasia- idUSLSN11NO8U20150917
\end{enumerate}
\end{footnotesize}
National Council for Radio Frequencies to implement a more equitable redistribution of frequencies among the four remaining mobile providers.23

Service providers are required to have a license to operate, and in 2005, the Cabinet of Ministers adopted Resolution No. 155, which stipulates that telecommunications providers must register as a legal entity before being issued a license. Licensing is often encumbered by political interests.24

Other factors impeding telecommunications company operations include an unstable regulatory environment, intricate customs procedures for the import of ICT equipment, and rules limiting currency conversion. Local authorities have also required international telecommunications companies to contribute to the cotton harvest, which watchdog groups say involves forced labor, as a condition of doing business.25 Telia declined to comply in 2015.26

Regulatory Bodies

Regulation of the internet has never been independent. Since February 2015, the Ministry for the Development of Information Technologies and Communications (MININFOCOM) regulates telecommunications services related to the internet.

The Ministry combines the functions of a policy maker, regulator, and content provider, with no separation of regulatory and commercial functions. It is responsible for licensing ISPs and mobile phone operators, promoting technical standards for telecommunication technologies such as 4G (LTE), and providing e-governance services.

The Computerization and Information Technologies Developing Center (Uzinfocom) under the Ministry administers the "uz" top-level domain. Thirteen private ISPs were authorized to provide registry services in the "uz" domain zone as of May 2017.27 Rules for the assignment, registration, and use of the country’s top-level domain create an obstacle to internet access.28

The Ministry is responsible for internet content regulation in order to prevent, among other things, the Internet’s “negative influence on the public consciousness of citizens, in particular of young people.” To do so, the Ministry promotes development of the national segment of the internet (the intranet), with “modern national websites on different issues, including information resources to satisfy informational and intellectual needs of the population, particularly of the youth.”29 Uzinfocom remains the largest provider of web hosting services, including for the e-government project, government-backed intranet, national search engine, and social-networking sites.30

28 Law RU “On Telecommunications,” at Arts. 8, 11.
UZBEKISTAN

Limits on Content

The government of Uzbekistan monitors and controls online communications, and engages in pervasive and systematic blocking of independent news and any content that is critical of the regime, particularly related to human rights abuses. The opaque system offers few details on how decisions are made or what websites are blocked at any given time.

Blocking and Filtering

Significant blocking and filtering limits access to online content related to political and social topics, particularly those related to human rights abuses in Uzbekistan. Other measures like a state-run search engine have been introduced over the years to limit access to information.31 Decisions to block content are non-transparent. State officials have denied that the government is involved in blocking content online.32

The websites of the international broadcasters Deutsche Welle, Fergana News Agency, Radio Free Europe/Radio Liberty, and the Uzbek services of the BBC and Voice of America have been permanently inaccessible in Uzbekistan since 2005,33 following a violent government crackdown on peaceful anti-government protests in Andijan.34 Websites of Uzbek human rights and opposition groups in exile are also blocked. Websites of international human rights organizations, such as Amnesty International, Freedom House, and Human Rights Watch, among others, are also blocked. Many users access blocked websites using proxies or VPNs. In August 2015, the United Nations Human Rights Committee expressed concern that websites with content on "controversial and politically sensitive issues" are blocked in Uzbekistan.35

Several government-linked entities monitor and control online communications, though the opaque system offers few details on how decisions are made or what websites are blocked at any given time. The Center for the Monitoring of the Mass Communications Sphere takes various measures to maintain compliance with national legislation that restricts free expression.36 Among its key objectives are “to analyze the content of information disseminated online and ensure its consistency with existing laws and regulations.”37 The center has contributed to the takedown of independent websites.38 The Expert Commission on Information and Mass Communications, a secretive body

35 See UN Docs. CCPR/C/UZB/CO/4, at para. 23.
established in August 2011, oversees the monitoring center.\textsuperscript{39} The commission is not independent and must submit quarterly reports to the Cabinet of Ministers.\textsuperscript{40} Its membership is not public,\textsuperscript{41} although it is reportedly comprised exclusively of government employees. The commission is mandated to evaluate online publications for content with a “destructive and negative informational-psychological influence on the public consciousness of citizens;” content which fails to “maintain and ensure continuity of national and cultural traditions and heritage;” or aims to “destabilize the public and political situation,” or commit other potential content violations.\textsuperscript{42}

The commission also assesses publications referred to it by the monitoring center or other state bodies, including the courts and law enforcement, drawing on a designated pool of government-approved experts.\textsuperscript{43} Commission members vote on whether or not a violation has been committed based on reports from those experts. State bodies act on the commission’s decision, including courts and “other organizations,” presumably private ISPs.\textsuperscript{44} There are no procedures in place to notify those whose content is blocked, and no clear avenue for appeal.

It is not clear to what extent authorities filter text messages or other content transmitted via mobile phones. In March 2011, some news reports said mobile phone operators were required to notify the government of any attempts to circulate mass text messages with “suspicious content.”\textsuperscript{45}

### Content Removal

Intermediaries can be held liable for third-party content hosted on their platforms and can be forced to remove such content. Under the 1999 Law on Telecommunications and several other government resolutions, the licenses of lower-tier ISPs may be withheld or denied if the company fails to take measures to prevent their computer networks from being used for exchanging information deemed to violate national laws, including ones that restrict political speech. Under Order No. 216 passed in 2004, ISPs and operators “cannot disseminate information that, \textit{inter alia}, calls for the violent overthrow of the constitutional order of Uzbekistan, instigates war and violence, contains pornography, or degrades and defames human dignity.”\textsuperscript{46} Given these broad restrictions, many individuals and organizations prefer to host their websites outside the country.\textsuperscript{47}

September 2014 amendments to the Law on Informatization brought bloggers and online news providers, including freelance citizen journalists, under state regulation subject to content removal requirements. By the law’s broad definition, any person may qualify as a blogger by disseminating information “of socio-political, socio-economic and other character” to the public through a

---


\textsuperscript{40} Ibid, Annex II, art. 31.

\textsuperscript{41} Ibid, Annex I, contains a list of the Commission’s members that is not made public.

\textsuperscript{42} Resolution of the Cabinet of Ministers RU, No. 228, at art. 1 and Annex II, art. 5. See note 50 above.

\textsuperscript{43} Ibid, at art. 1 and Annex II, art. 14.

\textsuperscript{44} Ibid, at Annex II, art. 26 and 29.

\textsuperscript{45} Murat Sadykov, “Uzbekistan Tightens Control over Mobile Internet,” \textit{Eurasianet}, March 15, 2011, \url{http://www.eurasianet.org/node/63076}.


\textsuperscript{47} According to government figures, only about 30 percent of websites with “.uz” domain names were hosted on servers based in Uzbekistan as of December 2011. See Uzinfocom, “Толькоцифры,” [Only Numbers] \url{http://bit.ly/1jRuww}.
website. The law requires bloggers to substantiate the credibility (‘dostovernost’) of “generally accessible information” prior to publishing or even reposting it, and obliges them to “immediately remove” information if it is not considered credible. The law entitles a special governmental body to limit access to websites that do not comply.

Media, Diversity, and Content Manipulation

Though the online media environment remains severely restricted, citizens may now air their grievances and make suggestions directly to government representatives through “virtual offices” a new online portal system introduced by the government in September 2016. Hundreds of thousands of complaints have been registered through the portal, many of which have been addressed by authorities, according to news reports. Observers have noted that the virtual offices are helping to create a more permissive environment with respect to criticism of authorities, with some news outlets even publishing select complaints submitted through the portal. Self-censorship nevertheless remains pervasive, given the government’s tight controls over the media and harsh punishment of those who report on topics deemed “taboo,” including criticism of the president, revelations about corruption, or health education. As a result of the government’s history of harassing traditional journalists, as well as their families, many online writers are cautious about what they post. The editorial direction of the online versions of state-run news outlets is often determined by both official and unofficial guidelines from the government.

Under 2007 amendments to the 1997 law “On Mass Media,” any website engaged in the dissemination of mass information periodically (at least once every six months) is considered “mass media” and is This procedure is generally known to be content-based and arbitrary, and inhibits editors and readers from exercising their freedom of expression and right to access information. As of January 2017, 395 news-oriented websites, including online versions of traditional news media outlets, were registered as mass media in Uzbekistan. Financial sustainability of independent online media outlets largely depends on diminishing foreign funding that is subject to vigorous state control. The parliamentary “Public Fund for Support and Development of Independent Print Media and News Agencies of Uzbekistan” allocates state subsidies and grants primarily to the state-owned and progovernment mass media, which publish state propaganda.

48 Law RU No. 3РУ-373, SZRU (2014) No. 36, item 452.
49 "В Узбекистане уволены десятки чиновников, проигнорировавшие обращения граждан" ("Dozens of high officials who haw ignored appeals of citizens were dismissed"), May 8, 2017, https://rus.ozodlik.org/a/28473138.html
54 See Uzbek Agency for the Press and Information, "Состояние и динамика развития СМИ, издательств и полиграфических предприятий Узбекистана (01.01.2015г.);" last accessed on 27 May 2015, http://www.api.uz/ru/ru/content/licence/statistics/
Independent news websites have been subject to arbitrary closure or retroactively unregistered. A news site Olam, once Uzbekistan’s second most-visited news site, was permanently closed in January 2013 after the authorities opened criminal proceedings against its editor-in-chief and the website owner. At the time of its closure, Olam was reporting on state appropriation in the telecommunications sector. In May 2015, a court ordered the closure of the news media website Noviyvek, a weekly newspaper established in January 1992 and known for its balanced news reporting. Independent online media outlets are often forced to operate overseas to escape government repression, including Centre1, which is based in Germany.

Facebook, YouTube, Twitter, and the Russian social networks Odnoklassniki and VKontakte are available and widely used. Since 2014, Facebook has been the fourth most visited website in the country, followed by Odnoklassniki, VKontakte, and YouTube. As social-networking sites and blogging platforms have grown in popularity, the government attempts to influence the information circulated on them by creating and promoting Uzbek alternatives to popular global or regional brands. The most recent example is Davra launched in June 2016 by Uzinfocom (see Regulatory Bodies). Davra resembles Facebook, and enables users to post photos, videos, and comments, but requires users to register their personal information and national IDs, facilitating monitoring by the authorities. The platform has gained little popularity, with less than 20,000 users registered in the first year.

Digital Activism

The stringent ideological policies of the government regarding the use of the internet and social media by Uzbek youth discourage digital activism as a significant form of political engagement. However, a handful of political activists and regime critics actively use the internet and social media as channels to reach supporters in and outside of Uzbekistan. Their efforts may raise awareness, but their actual impact on social mobilization is limited, largely due to the repressive environment for freedom of speech and assembly. Political Twitter and Facebook accounts are generally administered by Uzbek dissidents living abroad, rather than activists on the ground. Nevertheless, the #WithUzbeks hashtag gained traction on social media in 2015 to share opposition to the government, which had promoted a #WithKarimov hashtag prior to elections. Additionally, a popular Facebook group called “Qorgmaymiz” (We are not afraid) was launched by exiled Uzbek activists in 2014, and continues to be a popular forum with more than 15,000 members. Hundreds of members have posted photos of themselves holding an “I am not afraid” sign.

Violations of User Rights

State measures to silence dissent include persecution and criminal prosecution of regime critics and independent journalists, often on fabricated charges. The government has broad powers to punish...
expression online, and recently amended the criminal code to increase penalties for threatening security and order through telecommunications networks or mass media. The security services systematically eavesdrop on citizens' communications over email, mobile phone and Skype, in online forums, and social networks.

Legal Environment

Uzbekistan’s constitution protects the rights to freedom of expression and of the mass media, and prohibits censorship. Article 29 of Uzbekistan’s constitution guarantees the right to gather and disseminate information. However, the implementation of these protections remains minimal. National courts have generally failed to protect individuals, including professional journalists, against government retaliation for exercising their free speech rights. Rampant corruption, particularly within law enforcement bodies, as well as weak legislative and judicial bodies, continue to have a deleterious impact on freedom of speech. Courts and executive agencies also operate without transparency, depriving the public of access to legal decisions and opportunities for appeal.

The Uzbek criminal code contains several provisions that have been used extensively to prosecute reporters and internet users for threatening constitutional order (Article 159); the prohibition of propaganda for national, racial, ethnic and religious hatred (Article 156); the production and dissemination of materials containing a threat to public security and order with foreign financial help (Article 244); slander (Article 139), insult (Article 140), and insult of the president (Article 158). Both slander and insult are punishable with fines ranging from 50 to 100 times the minimum monthly wage, correctional labor of two to three years, detention for up to six months, or prison sentences of up to six years. Further restrictions typically placed on journalists and internet users are based on vague information security rules.

On April 25, 2016, amendments to Article 244(1) of the criminal code increased the penalty for the “manufacture, storage, distribution or display of materials containing a threat to public security and public order” committed using mass media or telecommunication networks from 5 to 8 years imprisonment. The vaguely formulated offense prohibits “any form of dissemination of information and materials containing ideas of religious extremism, separatism and fundamentalism, calls for pogroms or violent eviction, or aimed at spreading panic among the population, as well as the use of religion to violate civil concord, dissemination of defamatory fabrications, and committing other acts against the established rules of behavior in society and public safety, as well as dissemination or demonstration of paraphernalia or symbols of religious-extremist, terrorist organizations.” Observers, including the OSCE, regarded this as a further move to suppress freedom of expression online.

Prosecutions and Detentions for Online Activities

The regime's hostility towards its critics, including independent journalists, human rights activists,
and critically-minded internet users, is notorious.\footnote{Human Rights Watch, "The very end," September 26, 2014, http://bit.ly/UIXpa50} New arrests were reported under President Shavkat Mirziyoyev, though some long-serving detainees were also released.

In the confusion surrounding initial reports of late President Islam Karimov’s death in August 2016, more than a dozen people were briefly detained and in interrogated for commenting on the unconfirmed news on Telegram and WhatsApp prior to any official announcement. Those detained were held on charges of “disseminating information that threatens the public order and deliberately spreading false information through communication networks.” It appears that those detained were soon released, though authorities encouraged school administrators to instruct students to delete Telegram and WhatsApp from their devices.\footnote{People detained in Uzbekistan after commenting on the death of President Karimov” [in Russian] Radio Ozodlik, September 9, 2016, https://rus.ozodlik.org/a/27975877.html}

Uzbek authorities continued targeting individuals found to have religious materials on their phones. In May 2016, Zukhriddin Abduraimzhonov was detained at the Uzbekistan-Kyrgyzstan border for having forbidden religious sermons stored on his phone. The sermon was reportedly delivered by religious leader Abdulla Domla on the topic of child-rearing in Islam. Three months after his arrest, Abduraimzhonov received a three year prison sentence.\footnote{Relatives of a man from Osh sentenced to three years in prison hope for his release under an amnesty” [in Russian] Radio Ozodlik, November 3, 2016, https://rus.ozodlik.org/a/28092515.html} Separately, Kazakh citizen Akmal Rasulov was handed a five year prison sentence in July 2016 for “smuggling forbidden materials” into Uzbekistan. Akmal reportedly had several religious sermons saved on his phone.\footnote{“In Tashkent, a Kazakh man was convicted of storing banned sermons on his phone” Radio Ozodlik, December 12, 2016, https://rus.ozodlik.org/a/28168795.html}

At least one online journalist remains in jail on criminal charges international observers say were fabricated in retaliation for critical reporting. Dilmurod Saiid, a freelance journalist who reported for independent outlet \textit{Uznews}, is serving a 12.5 year sentence imposed in July 2009 on extortion charges.\footnote{OSCE Representative welcomes positive step releasing another journalist in Uzbekistan” OSCE, March 1, 2017http://www.osce.org/fom/302371.} Before his detention, he had reported on government corruption in Uzbekistan’s agricultural sector for local media and independent news websites.\footnote{Committee to Protect Journalists, “Uzbek appeals court should overturn harsh sentence,” September 3, 2009, http://cpj.org/x/34ea} In a positive development, several independent journalists were released from detention under the Mirziyoyev administration, though many had already served long sentences, and the releases did not appear to signal a change of policy regarding politically-motivated prosecutions. Independent journalist Jamshid Karimov, who had written for online outlets \textit{Fergana}, \textit{Uznews}, and the Institute of War and Peace Reporting, was released from forced detention in a psychiatric hospital in February 2017. Well-known as a fierce critic of Uzbek authorities, Karimov had been detained in the institution since 2005, apart from a brief release in late 2011.\footnote{“Karimov’s nephew released from a psychiatric hospital” Radio Ozodlik, March 1, 2017, https://rus.ozodlik.org/a/28341844.html} In another case, Solidzhon Abdurakhmanov, a journalist who had reported for \textit{Uznews}, an independent news website forced to shut down in December 2014, was released in October 2017. Abdurakhmanov, 67, had served nine years of a ten-year sentence for allegedly selling drugs, though he consistently maintained his innocence.\footnote{“Independent Uzbek journalist released after nine years in prison” RFE/RL, October 5, 2017 https://www.rferl.org/a/uzbekistan-journalist-abdurahmonov-released/28775300.html} Prior to
his arrest, he had reported on human rights and economic and social issues, including corruption in the Nukus traffic police office.\textsuperscript{71}

### Surveillance, Privacy, and Anonymity

Government surveillance of ICTs is extensive. Although Article 27 of the constitution guarantees the privacy of “written communications and telephone conversations,” there is no data protection legislation in Uzbekistan. Article 27 further guarantees respect for human rights and the rule of law, though these are frequently violated in surveillance operations.

Since 2006, the national security service (SNB) has conducted electronic surveillance of the national telecommunications network by employing the “system for operational investigative measures” (SORM), supposedly for the purposes of preventing terrorism and extremism.\textsuperscript{72} ISPs and mobile phone companies must install SORM and other surveillance equipment on their networks in order to obtain a license.\textsuperscript{73} Telecommunications providers are prohibited by law from disclosing details on surveillance methods and face possible financial sanctions or license revocation if they fail to design their networks to accommodate electronic interception.\textsuperscript{74}

Human rights defenders and online journalists frequently report attempts to compromise their online accounts. Dmitry Tikhonov, an Uzbek human rights defender who had worked on a project documenting forced labor during the cotton harvest, found that private information from his email account and personal Google Drive had been published online. Authorities subsequently initiated administrative proceedings against Tikhonov based on the leaked information, forcing him to flee the country in early 2016.\textsuperscript{75}

The Israeli branch of the U.S. Verint technology company, and the Israel-based NICE systems, supply the Uzbeki security services with monitoring centers allowing them direct access to citizens’ telephone calls and internet activity, according to UK-based Privacy International. Privacy International reported that Verint Israel has also carried out tests on behalf of the SNB to gain access to SSL-encrypted communications, such as those now offered by default by Gmail, Facebook, and other service providers, by replacing security certificates with fake ones using technology supplied by the U.S.-based company Netronome.\textsuperscript{76} In July 2015, documents leaked from the Milan-based surveillance software company “Hacking Team” revealed that NICE systems was supplying Hacking Team’s Remote Control System (RCS) spyware to Uzbekistan.\textsuperscript{77} RCS offers the ability to intercept user communications, remotely activate a device’s microphone and camera, and access all of the phone’s content including contacts and messages without the user’s knowledge.

\textsuperscript{71} Committee to Protect Journalists, “Government increases pressure on Uzbek journalists,” letter, February 17, 2010, \url{http://cpj.org/x/37de}

\textsuperscript{72} Resolution of the President RU, О мерах по повышению эффективности организации оперативно-розыскных мероприятий в сфере телекоммуникаций Республики Узбекистан, [On Measures for Increasing the Effectiveness of Operational and Investigative Actions on the Telecommunications Networks of the Republic of Uzbekistan] No. ПП-513, November 21, 2006, at Preamble and art. 2-3.

\textsuperscript{73} Ibid, art. 58. Also, tax and custom exemptions apply for import of the SORM equipment by domestic ISPs, see Tax Code of RU, art. 208, 211, 230 part 2, and 269.

\textsuperscript{74} See Law RU, “On Telecommunications”.

\textsuperscript{75} Amnesty International, “We will find you, anywhere: the global shadow of Uzbekistani surveillance” March 2017.

\textsuperscript{76} Privacy International, „Private Interests: Monitoring Central Asia“, Special Report, November 2014, at pp. 38-43, \url{https://www.privacyinternational.org/sites/default/files/Pri_ate%20Interests%20with%20annex_0.pdf}

\textsuperscript{77} Edin Omanovic, “Eight things we know so far from the Hacking Team hack,” Privacy International, July 9, 2015, \url{https://www.privacyinternational.org/node/619}
There is no independent oversight to guard against abusive surveillance, leaving the security service wide discretion in its activities. If surveillance is part of a civil or criminal investigation, content intercepted on telecommunications networks is admissible as court evidence. Opposition activist Kudratbek Rasulov was sentenced to 8 years in prison on charges of extremism in 2013, based on intercepted digital communications with an exiled opposition group. The law requires a prosecutor’s warrant for the interception of telecommunication traffic by law enforcement bodies; however, in urgent cases, the authorities may initiate surveillance and subsequently inform the prosecutor’s office within 24 hours.

There is limited scope for anonymous digital communication, and the government strictly regulates the use of encryption. Proxy servers and anonymizers are important tools for protecting privacy and accessing blocked content, although they require computer skills beyond the capacity of many ordinary users. In September 2012, Uztelecom started blocking websites offering proxy servers, including websites listing free proxies that operate without a web interface.

There are few options for posting anonymous comments online, as individuals are increasingly encouraged to register with their real names to participate in discussions forums such as Uforum, which is administered by the state-run Uzinfocom. Individuals must also provide passport information to buy a SIM card.

ISPs and mobile operators are required to store user data for three months. Since July 2004, operators of internet cafes and other public internet access points are required to monitor their users and cooperate with state bodies. Under regulatory amendments introduced in March 2014, operators of internet cafes and public access points must install surveillance cameras on their premises to “ensure [the] safety of visitors.” Additionally, they are required to retain a “registry of internet web-resources (logfiles)” used by customers for three months.

Intimidation and Violence

---


85 MTC Uzbekistan, “How to subscribe,” http://www.mts.uz/ru/subscribe

86 See Resolution of the SCCITT RU, “О внесении изменений и дополнений в Положение о порядке предоставления доступа к сети Интернет в общественных местах использования [On making amendments and additions to the Regulations on the procedure for providing access to the Internet in the public areas of use],” March 19, 2014, No. 79-мх, SZRU (2014) No. 13, item 150.
Online journalists and bloggers continue to face violence and retaliation for their work. Photojournalist Timur Karpov working for independent online agency Fergana News was apprehended and detained by police in October 2016. Karpov was working in eastern Uzbekistan when he was placed in custody for ten hours and beaten by police. Karpov said police erased all photos and videos from his mobile phone.87

In April 2017, artist and blogger Alexander Barkovskii was beaten by unknown assailants as he photographed a street artist in Tashkent. The attackers accused Barkovskii of publishing photos on the internet and spying.88

In the past, SNB offices were reported confiscating electronic media devices at the airport, checking browsing histories on travelers’ laptops, and interrogating individuals with a record of visiting websites critical of the government.89 Law enforcement officials invited journalists and human rights activists and ordinary citizens to “prophylactic talks” which often include warnings and threats.90

Technical Attacks

Distributed denial-of-service (DDoS) attacks on independent news media websites reporting on Uzbekistan, including Centrasia, UzMentronom, the Fergana News agency, and Ozodlik, the Uzbek service of Radio Free Europe/Radio Liberty, have been frequent in the past, though there were no prominent examples in the past year.

The state-run Information Security Center, established in September 2013, ensures the security of “the national segment of the internet” and state information networks, including the e-governance infrastructure.91 The Center took over most of the functions of the Uzbekistan Computer Emergency Readiness Team (UZ-CERT), established in 2005.92 The Center collects and analyzes information on computer incidents, including DDoS attacks, and alerts internet users to security threats. Moreover, the Center interacts with domestic ISPs, mobile phone operators, and state bodies—including law enforcement agencies—on the prevention and investigation of “unsanctioned or destructive actions in information space.”93

90 “Около 150 тысяч человек взяты на учет в Узбекистане”, (Approximately 150,00 people were taken for registration in Uzbekistan) March 25, 2016, Radio Ozodlik, http://rus.ozodlik.org/a/27634490.html
91 Resolution of the Cabinet of Ministers of RU “О мерах по организации деятельности Центра развития системы Электорнное правительство и Центра обеспечения информационной безопасности при Государственном комитете связи, информатизации и коммуникационных технологий Республики Узбекистан” [On Measures Establishing the Development Centre on “E-governance” System and Cybersecurity Centre at the State Committee on the CITT], No. ПП-2058, September 16, 2013, SZRU (2013) No. 38, item 492, at Art. 3.
92 See Resolution of the President RU No. ПП-2058, note 39 above (check cross-reference), at Annex 3, Art. 1.

15 www.freedomonthenet.org