Surveillance & Society

Article

Platform Surveillance and Resistance in Iran and Russia: The Case of Telegram

Azadeh Akbari

Heidelberg University, Germany
A.Akbari@stud.uni-heidelberg.de

Rashid Gabdulhakov

Erasmus University, Rotterdam, The Netherlands[1]
gabdulhakov@eshcc.eur.nl

Abstract

Telegram messenger, created by an exiled Russian entrepreneur Pavel Durov, brands itself as a non-mainstream and non-Western guarantor of privacy in messaging. This paper offers an in-depth analysis of the challenges faced by the platform in Iran, with 59.5% of the population using its services, and in Russia, where Telegram is popular among the urban dissent. Both governments demanded access to the platform's encrypted content and, with Durov's refusal, took measures to ban it. Relying on the concept of *surveillant assemblage* (Haggerty and Ericson 2000), this paper portrays how authoritarian states disrupt, block, and police platforms that do not comply with their intrusive surveillance. Additionally, we consider the tools and actors that make up internet control assemblages as well as the resistance assemblages that take shape in response to such control.

Introduction

The cloud-based messaging platform Telegram was created in 2013 to protect its developer, Pavel Durov, from state surveillance in Russia. Durov, an entrepreneur whose successful Facebook-resembling VKontakte social network gave him the title "Russia's Zuckerberg" (Hakim 2014), refused to hand user data to the authorities and, consequently, fell under severe surveillance. In response to these circumstances, Durov developed Telegram with an emphasis on encryption and privacy, integrating diverse communication capacities, such as groups with unlimited members, voice call, polls, and channels for broadcasting public messages to large audiences. Telegram quickly attracted users in Iran and Russia enticed by its ideology, outspoken commitment to internet privacy, and user data protection from third parties, namely the government, marketers, and advertisers (Telegram n.d.) Contrary to its rival platform, WhatsApp, Telegram has deliberately avoided the market-based rules of platform development, such as merging with bigger companies, and receives all of its funding from Durov himself. The platform functions through a complicated web of decentralized companies and, therefore, defies any state regulation. In this sense, Telegram simultaneously positions itself in opposition to the economic outlooks that dominate the global IT market and to the localized restrictions on data privacy. However, this position comes with a price tag, as Telegram was eventually banned in both Iran and Russia.

Despite the extensive body of work on privacy, surveillance, and democracy in Western countries, only recently have these concepts received academic attention in the context of authoritarianism and

[1] Both authors contributed equally to this work.

Akbari, Azadeh, and Rashid Gabdulhakov. 2019. Platform Surveillance and Resistance in Iran and Russia: The Case of Telegram. *Surveillance & Society* 17(1/2): 223-231.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

undemocratic governance. For instance, theories such as *networked authoritarianism* (MacKinnon 2011) investigate China's encompassing surveillance policies as well as online activism in response to it and show how "an authoritarian regime embraces and adjusts to the inevitable changes brought by digital communications" in the context where "the single ruling party remains in control while a wide range of conversations about the country's problems nonetheless occurs on websites and social-networking services" (33). Setting aside the particularities of the Chinese political system, this paper aims to contribute to the field of surveillance studies by demonstrating, through the example of Iran and Russia, how authoritarian states disrupt, block, and police platforms that do not comply with their intrusive surveillance. Additionally, we discuss the tools and actors that make up internet control assemblages, as well as the resistance assemblages that challenge platform surveillance and censorship.

Focusing on the case of Telegram, this paper scrutinizes platform surveillance as a process with social, political, and economic aspects and ramifications. Using the concept of *surveillant assemblage* (Haggerty and Ericson 2000) we assess the state of internet governance and control in both countries. Thus, the paper discusses Iran's *preventive*, *interceptive,* and *reactive* measures (Small Media 2018: 26) that are applied to repress internet use through a complicated and overlapping assemblage of official and semi-official organizations. We also analyze the *online* and *offline* actors of internet control in Russia and demonstrate how the *strategic ownership* of platforms, as well as the *strategic legislation,* are manipulated by the state to curb freedom of expression. Based on such assessments, this research provides an overview of the actors, methods, and tools that are instrumentalized against Telegram by the regimes of both countries; it also seeks to identify some parallels and divergences in platform surveillance and resistance.

Internet Governance in Iran and Russia

Technological development has transformed the methods, approaches, and actors in surveillance. The long praised Foucauldian panopticism fell short of explaining the fluidity and omnipresence of a surveillance that reduces individuals to pure information and imposes its gaze on "groups which were previously exempt from routine surveillance" (Haggerty and Ericson 2000: 606). This paper applies the concept of the surveillant assemblage to emphasize the heterogeneous nature of the objects that *work together* in order to make intrusive undemocratic surveillance possible. Through their attempts to surveil Telegram, both Iran and Russia instrumentalize a multitude of actors and techniques to establish governmental control over information and citizens. In addition to the state, which establishes the hegemonic narrative, a number of other agents, such as users, civil society, regional and international flows, technological advancements, things and code, fabricate other assemblages that interact, converge, and diverge from the surveillant assemblage.

While the rhetoric justifying the ban of Telegram in Iran and Russia is not completely analogous, both governments strive for full control over traditional and social media channels. Iran accuses Telegram of spreading moral decadence and reiterates Russian indictments of Telegram's facilitative role in terrorism by offering anonymity and data protection to its users. The autocratic states take measures to mute, limit, discourage, and otherwise eradicate narratives that challenge their stability. The following section spotlights the techniques and technologies within the surveillant assemblages of Iran and Russia. It also draws attention to the blurring lines between police and citizens, which questions the traditional theorization of state power and suggests new ways of looking at surveillance in undemocratic environments.

Iran: Totalitarian Surveillance

Listed as one of the 15 enemies of the internet (Reporters Without Borders 2016), Iran has a complex assemblage of overlapping governmental and non-governmental institutions that are mandated with the regulation of internet content and access. The Supreme Council of Cyberspace (SCC) stands above any governmental body and works directly under the supervision of Iran's Supreme Leader to set the general policies for internet access and content control. The Commission to Determine the Instances of Criminal Content shares seven members with the SCC and predominantly occupies itself with identifying "online content that violates public morals, contradicts Islam, threatens national security, criticizes public officials

or organizations, or promotes either cyber crimes or the use of circumvention tools" (Small Media 2018: 20). While these two bodies enjoy an extra-legal status, governmental bodies, such as the Information and Communication Technology Ministry, play a solely executive role and lack any decision-making power. Additionally, the Iranian Cyber Police and Cyber Army are exclusively tasked with monitoring content posted on the internet as well as preventing and prosecuting cybercrimes. The Cyber Police (FATA), established in 2011, mainly covers cases of fraud, scams, and harassment. The Cyber Army, an "underground network of pro-regime cyber activists, hackers and bloggers…monitors the internet and launches cyber attacks on opposition and anti-Islamic websites" (Small Media 2018: 20). In this way, what is deemed to be undesirable content according to the regime's ideology, is actively policed and, consequently, many websites, keywords, and social media platforms are blocked.[2]

In addition to controlling content, access to the free internet is also hindered through technical means, such as keeping the bandwidth and the speed of internet intentionally low. Table 1 demonstrates Iran's methods of internet censorship, divided by preventive, interceptive, and reactive methods (Small Media 2018: 26). Resistance to the above-mentioned surveillant assemblage has ranged from erasing digital footprints by using public internet cafes to extensive use of anti-proxy and VPN services. These resistance strategies are chiefly dependent on the contextual circumstances, governmental policies, and technological possibilities. This paper later discusses resistance strategies in the case of Telegram, and through its investigation it also demonstrates the dynamic nature and fluidity of the surveillant assemblage.

Table 1. Methods of Internet Censorship in Iran

Preventative Methods	Interceptive Methods	Reactive Methods
URL "blacklist": When a user attempts to access blocked content, they are automatically redirected to a webpage managed by censors. **DNS redirection:** Telecommunications Infrastructure Company (TIC) is given a list of URLs, which it blocks prior to allocating bandwidth to ISPs.[3] **Content-control software:** Software used by TIC to automatically inspect, filter, and block sites. **HTTP host and keyword filtering**: URLs and headers containing specific text are automatically filtered by TIC. **Broadband speed limitations**: ICT Ministry forbids speeds faster than 128kbps for home users.	**Deep Packet Inspection (DPI):** Technology used to monitor, track, and block internet traffic. **MITM (man-in-the-middle)**: Method used to intercept online communications. **Traffic Analysis**: Analysis of sites that are being viewed most frequently.	**Respond to patterns in user behaviour:** Traffic analysis and DPI surveillance informs the creation of updated blacklists and filtered keywords. **Arrest of internet activists and developers**: The state has arrested a number of cyber activists working against online censorship. **Periodic blocking of SSL[4]**: Websites with SSL security protocols are periodically blocked inside Iran, forcing users to use insecure websites instead. **Connection throttling:** At moments of political or social tension, connection speeds are throttled to limit online engagement.

(Small Media 2018: 26)

[2] Any given URL can be checked in the website below to see if it is blocked in Iran or not. However, the results are not exactly accurate; for example, Facebook is indicated as "working" even though it has been blocked for many years. See: https://www.comparitech.com/privacy-security-tools/blockediniran/#

[3] Internet Service Provider.

[4] Secure Sockets Layer.

Russia: Strategic Surveillance

Russia's internet platform landscape can be described as *a hybrid*, with both domestic and foreign companies providing services. The most prominent domestic social network is Durov's first creation VKontakte, established in 2006 as a Facebook prototype. In 2014, following state pressure that forced its founder into exile (Miller 2015), VKontakte was appropriated by the Kremlin-loyal Mail.ru Group Media Holding, which also owns other popular social media platforms.

Unlike Iran, Russia has not engaged in systematic platform bans, though the country is experiencing "a trend towards the normalization of telecommunications, digital, and internet surveillance" (Lokot 2018: 338). For instance, amendments to the information law in 2012 allowed the state to "blacklist and force offline certain websites without a trial" (BBC News 2012). Furthermore, the so-called "Yarovaya law package" requires platforms to "record and store all communications and activities of all users, and make stored records available to authorized government bodies at their request" (ICNL 2016). Although global platforms[5] function side-by-side Russia's domestic prototypes and alternatives, the 2011 to 2012 anti-government protests have sensitized the ruling regime to new media's mobilization capacities. Consequently, strategic measures have been taken to bring such possibilities under control. These measures range from basic internet filtering to strategic ownership of domestic platforms. Furthermore, the ruling regime is after securing access to user data by forcing foreign platforms to comply with demands for privacy invasion imposed by means of strategic legislation. The law targets users, platforms, content, and data flows. At the threat of losing access to the market, platforms are forced to filter content and share data with the state. As such, Facebook demonstrated compliance with orders for the removal of undesired content (Meduza 2018), while Google evidently relocated some of its servers to data centers in Russia (Razumovskaya 2015). In the meantime, Russia's legislators are proposing new measures for internet sovereignty in the country, which would allow Russia's cyberspace "to continue functioning even if the country is cut off from foreign infrastructure" (Reuters 2019).

In addition to strategic control over platforms, the state targets users and instrumentalizes citizens. In 2014, the State Duma [parliament] passed the so-called "blogger law" that required bloggers with a daily audience of 3,000 or more to register as mass media (BBC News 2014), consequently increasing bloggers' "vulnerability to criminal prosecution" (Lokot 2018). Although the "blogger law" was abolished in 2017, "content generating users" are still obliged to follow other legal acts governing the gathering, processing and dissemination of information (RBC 2017). Targeting the base user of platforms, new initiatives were passed to encourage reporting on crime. The previously "rare and unregulated" (The Moscow Times 2018) practice of financially rewarding citizens for their contributions to crime solving was turned into an official plan by the Ministry of Interior, declaring failure to report a witnessed crime as an act of crime in itself. These measures further encourage snitching and convert ordinary citizens into elements within Russia's surveillant assemblage. Turning users against users not only fades the apparent role of the state in censorship but also serves as a pre-emptive measure for deterring online mobilization.

In addition to the legal approaches, online and offline actors are utilized within the Kremlin's surveillant assemblage. Online actors include groups, such as pro-Kremlin bloggers and trolls, who spread counter-dissent content. Additionally, *kiberdruzhinas* or Cyber Guards screen harmful content online and report it to the authorities (Safe Internet League n.d.). Offline actors include the Cossacks[6] who are recruited to physically suppress activism and opposition. Police forces operate both on- and offline by surveilling vocal citizens "who are already known to the local *Centre E* [counter-extremism] police force, the local FSB (Federal Security Service) branch, or the local district attorney" (Soldatov in Meduza 2016). Considering such comprehensive and strict policies to control cyberspace, Telegram's refusal to play by the Kremlin's rules inevitably turned the platform into a bullseye.

[5] With the exception of LinkedIn, which was blocked in 2016 (Roskomnadzor 2016).

[6] "[R]evival communities of Russians claiming Cossack heritage are increasingly making their mark as conservative shock troops, fighting alongside separatist forces in southeast Ukraine and embracing, and sometimes policing, a return to conservative values under President Vladimir Putin" (Roth 2016).

The Arrival of Telegram

Conflicting with totalitarian and strategic surveillance systems, Telegram entered the scene with a promise of freedom, privacy, and resistance; virtues that are engraved in the platform's design. Telegram's promise of security and its user-friendly design in an environment of extreme censorship and surveillance in Iran created an audience of millions. An official polling agency announced in April 2018 that 59.5% of Iranians use Telegram (ISPA 2018a). Telegram itself announced in January 2018 (Telegram Region 2018) that the application has 40 million monthly and 25 million daily users in Iran, as well as 678 thousand channels in Persian, with two billion visits per day. From these channels, 38% are dedicated to entertainment, 10% to news, and 3% have economic objectives. The platform claimed that 60% of all internet traffic in Iran is spent on Telegram, and advertising revenues reach 100 million USD per year (Telegram Region 2018). These are almost unfathomable figures for one of the most closed internet governance systems in the world.

Such extensive use of a messaging platform was first harshly responded to by reactive methods. Celebrities and public figures were exposed to the scrutiny of the strict Islamic government, in order to warn the public of the omnipresent state surveillance and the consequences of publishing what the state deemed undesirable. As the number of users grew, the government imposed harsher surveillance methods. In May 2016, the Iranian Supreme Council of Cyberspace announced a one-year deadline to all messaging networks to transfer their servers to the country (Isfandiari 2017). Telegram was mentioned nowhere in the ratification, but as the most popular platform, it was obvious that it was the target of the new law. Soon afterward, it was announced that Telegram servers were transferred to Iran. Durov reacted immediately, stressing that "Telegram servers will never 'travel' to countries with internet censorship" (Durov 2017). Although there were occasional collaborations between Iran and Telegram, the platform continued to refuse Iran's interceptive methods of surveillance. Consequently, the situation escalated and resulted in a total ban on Telegram, in May 2018, based on allegedly private plaintiffs that were never disclosed in any court (BBC Persian 2018a).

Telegram faced similar intimidations in Russia. Having developed the VKontakte social network in 2006, Durov was already a controversial figure because of his refusal to collaborate with state security forces. He fled the country, in 2014, as a result of "government pressure to release the data of Ukrainian protest leaders" (Hakim 2014). While in exile, Durov presented Telegram "for people craving privacy and security" (Hakim 2014). The platform soon attracted the attention of the Russian urban dissent. In Moscow, 28% of smartphone owners use Telegram, while the most popular Telegram channels are those reporting on politics and delivering the news (Momri Institute 2018). Over the years, Telegram's penetration in Russia has been steadily increasing; it jumped from 3 million users in September 2016 to 10 million users in September 2017, with current total monthly users of approximately 10 to 13 million (Telegram Region 2018). Telegram remains among the top five most popular messengers in the country and, ironically, was used by Russia's state agencies and representatives as a platform for communicating with citizens. After Durov's refusal to grant encryption keys to the FSB, the Kremlin promised to move its communications to another "convenient" platform (Vesti 2017).[7]

The danger of the encrypted messaging afforded by Telegram has continuously recurred as a theme in Russia's mainstream media discourse. Telegram was, for instance, blamed for being a go-to platform for terrorists and drug dealers (Medvedev 2017; Lyadov 2017). After terrorist attacks in Paris in 2015, Russia's lawmakers appealed to the FSB with the request to block access to Telegram as it facilitated "the process of recruiting Russian citizens to ISIS" (Vesti 2015). The Iranian Judiciary also claimed that the ISIS terrorists who attacked the Iranian Parliament had used Telegram as their means of communication and accused the platform of facilitating "organised espionage" (Tasnim News 2017). In the case of Russia, Durov protested that such accusations are not made against non-Russian applications, like WhatsApp (Vasilchuk 2017).

[7] The last post by the Kremlin.ru channel was made on March 7, 2018 (Accessed in November 2018). Russia's Ministry of Foreign Affairs actively maintains its official Telegram channel.

Reaffirming the inability of the Russian surveillant assemblage to instigate full control and censorship, especially on a global level of interaction, such selective targeting of non-complying platforms serves the purpose of sending a warning signal to other players.

Involuntary Farewells

Following the ban, Durov urged Telegram's Russian users not to delete or reboot the app and promised to introduce built-in systems to circumvent blocking (Durov 2018). The innovative anti-circumvention methods indeed followed shortly after and challenged the attempted ban by making access to other platforms, such as Google, Google Drive, and YouTube, problematic. As a result, businesses suffered economic damage estimated to be 2 billion USD (Novaya Gazeta 2018). Internet experts stated that the only way Roskomnadzor (The Federal Service for the Supervision of Communications, Information Technology and Mass Media) can block Telegram is by "unplugging all the internet in the country" (RBC 2018). As the antagonism grew between the state and Telegram, other instances of resistance arose. People launched a symbolic protest by flying paper airplanes resembling Telegram's logo, in the streets of cities across Russia, to demonstrate their solidarity with the platform and their resentment of state censorship (MacFarquhar 2018). Roskomnadzor reacted by implementing a 300 million USD deep packet inspection (DPI) system that infringe on people's access to Telegram (Zakharov and Reiter 2018). Although usage of such intrusive surveillance technologies was denied, the federal regulator confirmed that some measures were taken for improvement of the control system (Tass 2018).

Similar to the dynamics of control, resistance, attack and retreat in Russia, despite the heated debates on the official level of Telegram use in Iran, 79% of the users continued using the app with the help of VPN[8] services (ISPA 2018b). Consequently, the ICT Ministry ordered all ISPs to block VPN connections and called the usages of such circumvention tools an American plan "to topple the Islamic Republic" (IRNA 2018). Furthermore, one of the well-known international VPN providers, Psiphon,[9] reported that it was once "test" attacked before the ban of Telegram, followed by two more attacks after the ban (Akbarpour 2018). On an individual level, public security police sent text messages to Telegram channel directors, threatening them with legal prosecution (Ronaghi 2018). Reacting on a legal level, a group of independent lawyers sued the government for violating the constitutional rights to freedom of expression (Radio Farda 2018). None of these legal accusations, either by the judiciary or activists, ever received a court hearing.

In addition to prohibitive strategies within its surveillant assemblage, the Iranian government tried active policies of channeling users to cyberspaces that fulfilled the desirable level of governmental surveillance. An internally designed messaging app called *Soroush* was expansively advertised on the state's official TV channels. The app, developed by a company affiliated with Iran's Broadcasting Organization which is the country's exclusive radio and television broadcaster (Soltani 2018), was not the first of several platforms created to replace a popular Western alternative. Either as a result of sanctions against Iran or the government's policies, YouTube, Google Play, iTunes store, and many others were previously replaced with local prototypes. In this case, the massive user pool of Telegram made the state's proactive efforts even more rigorous. For instance, Soroush administrators created fake accounts by using citizens' mobile phone numbers without their knowledge or consent (Ranjbar 2018). Using Telegram was eventually announced illegal, since access to the platform was impossible without the use of circumvention tools (BBC Persian 2018b), which is prohibited by Iran's 2009 Cyber Crime Law; this law criminalizes distribution, sale and guidance on the usage of circumvention tools (Islamic Republic of Iran Parliament 2008).

Due to Iran's rigid political system and lack of freedom of expression, the cyber community responded more actively and innovatively to the ban. An anonymous activist group introduced Telegram Digital Resistance

[8] "A VPN, or virtual private network, is a secure tunnel between two or more devices. VPNs are used to protect private web traffic from snooping, interference, and censorship" (Expressvpn n.d.).
[9] "Psiphon Inc. is a company based in Toronto, producing open-source multi-platform software that helps over 3 million people every week connect to content on the Internet" (Psiphon n.d.).

as a "customized version of Telegram integrating the circumvention tool Psiphon" (TelegramDR n.d.). Although the TelegramDR app was removed from app stores due to its violation of copyright, the idea of integrating Telegram into other applications attracted the attention of state-affiliated platform developers. Thus, Hotgram and Golden Telegram were developed by security forces (DW Persian 2018) with their servers located on Iranian soil (Farda News 2018). Both applications act as a mediatory or bridge between the host application and the original Telegram and, therefore, police the data flow with a free hand. Considering Telegram's popularity, many less tech-savvy users joined the new applications, proving the incredible resilience of the Iranian surveillant assemblage in controlling platforms through subtle tactful approaches.

The complicated dynamics between state actors, official and underground resistance trends, international limitations and corporations, in the case of Telegram, expand the West-centric concept of assemblage by showcasing a more dynamic mass of actors, methods, and technologies. Both states try to use Telegram as an exemplary threat to compel other platforms to comply with their privacy intrusive demands, or as the head of Iranian Supreme Council of Cyberspace has stated "Telegram's destiny will await" them (Young Journalists' Club 2018). Although there are continuous demands by both regimes to host social media servers on their domestic soil and to make data available to the state security apparatuses in order to force global platforms to confront the dilemma of losing the market in Iran and Russia or adapting to the states' demands, Telegram's ban revealed an Achilles' heel in the authoritarian surveillant assemblage. Blocking one platform has impacts on the operations of other platforms. Complete replacement of foreign platforms with domestic alternatives or strategic ownership through a market monopoly would require enormous financial and technological resources. Furthermore, blocking makes citizens more technologically savvy as they adapt to the use of VPNs and proxies to circumvent state-imposed barriers. Telegram's ban demonstrates a complex response to an intricate problem involving not only the surveillant assemblage but also users, experts, economic and political stakeholders, activists, and many other involved parties, forming a resistance assemblage against a surveillant assemblage.

Conclusion

Through the case of Telegram, this paper discussed in detail how surveillant assemblages in Iran and Russia facilitate state control and limit access to information not sanctioned by the state. At the same time, this study demonstrated how, within their networked authoritarianism, Iran and Russia negotiate control of the established platforms and confront the emerging alternatives that are designed to defy such controlling measures. By demanding Telegram to localize its servers and grant them access to user data, both countries have tried to dominate the limits of technological advancement. They have relied on various actors within their surveillant assemblages to police the users and the content, such as the Cyber Police and Cyber Army in Iran, and loyal media, vigilant citizens and Roskomnadzor's communication authority in Russia. While international giants like Google and Facebook seem to have found a common language with the Kremlin, platforms that refuse to domesticate their servers and to follow these regimes' demands are deemed dangerously rogue. That being the case, both countries have banned Telegram, aiming for the complete eradication of a platform that has stubbornly stood outside their surveillance.

As Telegram users in Iran and Russia began to acquire new skills and technological solutions to sustain their access to the platform, both regimes had to adapt and handle these challenges to maintain their autocratic control over new spaces of public interaction. When it comes to the complete ban of platforms, the ruling regime in Russia faces technological challenges, and is cautious not to take measures that would lead to mass protests. In the attempt to overcome these limitations, the new set of legislative measures designed to make Russia's internet more "sovereign" is in the making (Reuters 2019). While facing similar technological limitations, Iran's surveillant assemblage is aggressive and comprehensive in its ubiquitous surveillance and uncompromising control. It actively blocks content and platforms, and follows a Chinese model (MacKinnon 2011: 44) to replace international services with domestic alternatives. Despite such differences, the burning desire to collect citizens' data and secure control over content through any possible means brings Iran and Russia closer together in their outlook. As authoritarian governments tighten their

grip on the free internet, platforms such as Telegram present new possibilities to think, act and post messages alternatively. In doing so, they bring about new challenges for autocratic regimes. Telegram was developed as an ideological resistance to ideological surveillance. The case of Telegram not only presents the ongoing clashes between non-democratic states and users who struggle to access free flows of information but also highlights important issues about platform independence, alternative commercial models of platform development, and the future of platform surveillance across various political contexts.

References

Akbarpour, Nima. 2018. *Twitter,* May 3. https://twitter.com/nima/status/992130640270315525 [accessed July 2, 2018].

BBC Persian. 2018a. Che kasi Telegram ra dar Iran filter kard? [Who Filtered the Telegram?] May 6. http://www.bbc.com/persian/iran-44022670 [accessed November 13, 2018].

BBC Persian. 2018b. Dadsetan Esfehan: Hich Kas Ejazeh Estefadeh az Telegram ra Nadarad [Isfahan Prosecutor: Nobody is Allowed to Use Telegram]. July 4. http://www.bbc.com/persian/iran-44710214 [accessed July 5, 2018].

BBC News. 2012. Russia Internet Blacklist Law Takes Effect. November 1. https://www.bbc.com/news/technology-20096274 [accessed November 15, 2018].

BBC News. 2014. "Draconian" Russian Net Law Enacted. August 1. https://www.bbc.com/news/technology-28583669 [accessed November 20, 2018].

Durov, Pavel. 2017. *Durov's Channel.* https://t.me/durov/51 [accessed November 13, 2018].

Durov, Pavel. 2018. *VKontakte post*, April 13. https://vk.com/wall1_2285269 [accessed November 21, 2018].

DW Persian. 2018. Namayandeh Osoulgaray-e Majles: Hotgram va Telegram Talayee ra yek dastgah-e amniati rah andakhteh ast [Conservative MP: Hotgram and Golden Telegram Are Run by a Security Organization]. November 26. https://www.dw.com/fa-ir/iran/a-46452883 [accessed November 27, 2018].

Expressvpn. n.d. What is VPN? https://www.expressvpn.com/what-is-vpn [accessed November 13, 2018].

Farda News. 2018. Severhay-e Hotgram va Talagram koja gharar darand? [Where Are the Servers of Hotgram and Golden Telegram Located?] July 16. https://bit.ly/2K4IiYH [accessed November 15, 2018].

Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605-622.

Hakim, Denny. 2014. Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile. *The New York Times,* December 2. https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html [accessed November 20, 2018].

ICNL (International Center for Not-for-Profit Law). 2016. *Overview of the Package of Changes into a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism*. http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf.

IRNA. 2018. Bastan Filtershekan ha Shorou Shodeh Ast [VPNs Are Being Shut Down]. May 15. http://www.irna.ir/fa/News/82916267 [accessed July 2, 2018].

Isfandiari, Yousef. 2017. Vagheiat-e Majaray-e enteghal-e serverhay-e Telegram be Iran [The Truth Behind the Transportation of Telegram Servers to Iran]. July 23. https://goo.gl/1afP5W [accessed November 12, 2018].

Islamic Republic of Iran Parliament. 2008. Iranian Cyber Police. *Cyber Crime Law.* https://www.cyberpolice.ir/page/42981 [accessed June 29, 2018].

ISPA. 2018a. 59.5% mardom-e-Iran az shabake-y-e ejtamie-e Telegram estefadeh mikonand [59.5% of Iranians Use Telegram]. April 9. https://goo.gl/TfBYJd [accessed July 2, 2018].

ISPA. 2018b. 79% az estefadeh konandegan Telegram hanouz dar in Shabakeh hozour darand [79% of Telegram Users Are Still Using the App]. June 24. https://goo.gl/poiguc [accessed July 2, 2018].

Lokot, Tetyana. 2018. Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices. *Surveillance & Society* 16 (3): 332-346.

Lyadov, Anton. 2017. Иллюзия анонимности: Telegram стал самым популярным мессенджером у террористов [The Illusion of Anonymity: Telegram Has Become the Most Popular Messenger Among Terrorists]. *Vesti,* June 26. https://www.vesti.ru/doc.html?id=2903369 [accessed November 28, 2018].

MacFarquhar, Neil. 2018. Russia Tried to Shut Down Telegram. Websites Were Collateral Damage. *The New York Times,* April 18. https://www.nytimes.com/2018/04/18/world/europe/russia-telegram-shutdown.html [accessed November 20, 2018].

MacKinnon, Rebecca. 2011. China's Networked Authoritarianism. *Journal of Democracy* 22 (2): 32-46.

Meduza. 2016. In 'Kontakt' with the Cops: When Russian Police Go After Internet Users, Why do They Target People on Vkontakte Almost Exclusively? July 7. https://meduza.io/en/feature/2016/07/07/in-kontakt-with-the-cops [accessed November 20, 2018].

Meduza. 2018. The Russian Government Blocks Navalny's Website, As Instagram Caves to the Censor's Demands and YouTube Wavers. February 15. https://meduza.io/en/news/2018/02/15/the-russian-government-blocks-navalny-s-website-as-instagram-caves-to-the-censor-s-demands-and-youtube-wavers [accessed November 20, 2018].

Medvedev, Andrey. 2017. Опасный Telegram: Закрытость Мессенджера на Руку Террористам и Наркоторговцам [Dangerous Telegram: Privacy of the Messenger Aids Terrorists and Drug Dealers]. *Vesti,* June 25. https://www.vesti.ru/doc.html?id=2902947 [accessed November 20, 2018].

Miller, Christopher. 2015. A Long Way from Moscow. *Mashable,* https://mashable.com/2015/05/18/russias-mark-zuckerberg-pavel-durov/?europe=true#jAq40R99Jaqa [accessed November 20,].

Momri Institute. 2018. Исследование Telegram Аудитории [Telegram Audience Study]. January 16. http://momri.org/2018/momrinews/issledovanie-telegram-auditorii/ [accessed November 20, 2018].

Novaya Gazeta. 2018. Ущерб Бизнеса из-за Блокировки Telegram Оценили В $2 Млрд [Damage to the Business Due to Telegram Blocking Estimated at $2 Billion]. April 26. https://www.novayagazeta.ru/news/2018/04/26/141268-uscherb-biznesa-iz-za-blokirovki-telegram-otsenili-v-2-mlrd [accessed November 13, 2018].

Psiphon. n.d. *About Us.* https://www.psiphon3.com/en/about.html [accessed July 5, 2018].

Radio Farda. 2018. shekayat-e jami az vokalay-e dadgostari az bazpors-e saderkonandeh dastoor-e masdoodsazi-e Telegram [A Group of Lawyers Sue the Prosecutor Who Ordered Telegram Ban]. May 6. https://www.radiofarda.com/a/f4_a_group_lawyers_complain_judge_tilter_telegram/29211595.html [accessed November 27, 2018].

Ranjbar, Mehdi. 2018. *Twitter,* May 24. https://twitter.com/m_ranjbar2/status/999709319380766720/photo/1 accessed July 2, 2018].

Razumovskaya, Olga. 2015. Google Moves Some Servers to Russian Data Centers. *The Wall Street Journal,* April 10. https://www.wsj.com/articles/google-moves-some-servers-to-russian-data-centers-1428680491 [accessed January 10, 2019].

RBC. 2017. Роскомнадзор прекратил вести реестр блогеров. [Roskomnadzor Stopped Keeping a Register of Bloggers]. August 1. https://www.rbc.ru/rbcfreenews/59803d119a79470c2fadefd7

RBC. 2018. Почему Telegram не Удалось Заблокировать: 4 Вопроса о Судьбе Мессенджера [Why Telegram Blocking Failed: 4 Questions About the Fate of the Messenger]. April 17. https://www.rbc.ru/technology_and_media/17/04/2018/5ad5fe429a79471a4d5fa03f [accessed November 17, 2018].

Reporters Without Borders. 2016. The 15 Enemies of the Internet and Other Countries to Watch. January 25. https://rsf.org/en/news/15-enemies-internet-and-other-countries-watch [accessed May 7, 2018].

Reuters. 2019. Russian Lawmakers Back Bill on 'Sovereign' Internet. February 12. https://www.reuters.com/article/us-russia-internet/russian-lawmakers-back-bill-on-sovereign-internet-idUSKCN1Q11RJ [accessed March 5, 2019]

Ronaghi, Hossein. 2018. *Twitter,* May 21. https://twitter.com/HosseinRonaghi/status/998597713498378240/photo/1 [accessed July 2, 2018].

Roth, Andrew. 2016. 4 Things You Need to Know About the Cossacks Fighting Russia's Opposition Groups. *The Washington Post,* May 18. https://www.washingtonpost.com/news/worldviews/wp/2016/05/18/4-things-you-need-to-know-about-the-cossacks-fighting-russias-opposition-groups/?utm_term=.301b35c57d5f [accessed November 29, 2018].

Roskomnadzor. 2016. LinkedIn Направлена на Блокировку Операторам Связи [LinkedIn Sent for Blocking by Communication Operators]. November 17. https://rkn.gov.ru/news/rsoc/news41615/ [accessed November 23, 2018].

Small Media. 2018. Revolution Decoded: Iran's Digital Landscape. In *Small Media,* edited by Bronwen Robertson and James Marchant. https://smallmedia.org.uk/revolutiondecoded/ [accessed June 6, 2018].

Soltani, Yashar. 2018. *Twitter,* May 22. https://twitter.com/yasharsoltani/status/998990745016176641 [accessed July 2, 2018].

Tasnim News. 2017. Hamahangi haye Daesh dar Hamleh be Majles az tarigh-e Telegram bood [The ISIS Terrorists Who Attacked the Parliament Used Telegram for Coordination]. July 26. https://bit.ly/2P48ILi [accessed November 27, 2018].

Tass. 2018. Жаров: Роскомнадзор не тратил 20 млрд рублей на разработку систем блокировки Telegram [Zharov: Roskomnadzor Did Not Spend 20 Billion Rubles on the Development of Telegram Blocking Systems]. *Tass,* December 24. https://tass.ru/ekonomika/5946405 [accessed January 10, 2019].

Telegram. n.d. *Telegram FAQ*. https://telegram.org/faq [accessed January 20, 2019].

TelegramDR. n.d. *TelegramDR.* https://telegramdr.com/ [accessed January 20, 2019].

Telegram Region. 2018. Статистика Аудитории Telegram на Январь 2018 [Telegram Audience Statistics for January 2018]. January 27. https://telegram-region.com/statistika-auditorii-telegram-na-yanvar-2018/ [accessed November 12, 2018].

The Moscow Times. 2018. Russian Police to Reward Informants up to $150K Under New Plan. August 23. https://themoscowtimes.com/news/russian-police-reward-informants-150k-under-new-plan-62629 [accessed November 23, 2018].

Vasilchuk, Tatyana. 2017. Телеграм не ОРИ [Telegram Is Not ORI (Organizer of Information Dissemination]. *Novaya Gazeta,* June 26. https://www.novayagazeta.ru/articles/2017/06/24/72898-telegram-ne-ori [accessed November 23, 2018].

Vesti. 2015. ФСБ Может Ограничить Доступ к Telegram, Которым Пользовались Смертники в Париже [FSB May Restrict Access to Telegram, Which Was Used by Suicide Bombers in Paris]. November 15. https://www.vesti.ru/doc.html?id=2687332 [accessed November 23, 2018].

Vesti. 2017. В Кремле найдут альтернативу *Telegram*. Какую? [The Kremlin Will Find an Alternative to Telegram. Which One?]. June 26. https://www.vestifinance.ru/articles/87271 [accessed November 28, 2018].

Young Journalists' Club. 2018. Firouzabaadi: agar Instagram hamkari nakonad be sarnevesht-e *Telegram* dochar mishavad [Firouzabadi: If Instagram Does Not Cooperate, Telegram's Destiny Will Await It]. September 17. https://bit.ly/2NMjUj0 [accessed November 15, 2018].

Zakharov, Andrei, and Svetlana Reiter. 2018. Роскомнадзор внедрит новую технологию блокировок *Telegram* за 20 млрд рублей [Roskomnadzor Will Implement New Technology for Telegram Blocking at the Price of 20 Billion Rubles]. *BBC,* December 18. https://www.bbc.com/russian/features-46596673 [accessed January 10, 2019].