Encryption, Democracy, and the Peculiar Case of Russia's Telegram

Justin Hiemstra

Submitted in partial fulfillment of the requirements for the degree of

Bachelor of Arts in Russian

Department of Russian

Bryn Mawr College

Spring Semester 2019

Abstract

The Russian Federation outwardly labels itself as a democracy, but given its actions over the past three decades, it should not be considered as such. Vladimir Putin has slowly but successfully worked to transform the democratic foundation established in Russia after the collapse of the Soviet Union into a system that works towards a single goal – keeping Putin in power. Moreover, the steps he has taken toward eroding democracy in Russia are clear and discernible, even if those in power are unwilling to admit as much. However, the proliferation of technologies that make use of encryption and decentralized networks has created a digital public sphere that is nearly impossible to control by any government. This in turn has made the undermining of democratic principles a much more challenging task, and recognizing this, the pro Putin Kremlin has gone to great lengths to curtail the use of these technologies in Russia. In particular, the Russian-built app Telegram has been targeted due to its unwavering committment to strong encryption and privacy. The app's creators, Pavel and Nikolai Durov, who were once put forward on a pedestal by the Russian government for their creation of the successful Russian social media platform Vkontakte, have been condemned by their country of birth for their unwillingness to undermine the right to privacy of Telegram's users. This has not stopped them from designing Telegram in a way such that it has successfully worked around Russia's ban. Moreover, this presents Putin with a dilema, because effectively blocking Telegram would require a total restructuring and isolation of the Russian internet, something that would demand tremendous sums of initial investment and that would have disastrous ramifications for the Russian economy upon completion. In the meantime, it appears as though technologies that make use of strong encryption are here – and in Russia – to stay.

Contents

1 Introduction

After the Soviet Union collapsed in 1991, and after the formation of the Russian Federation, there was widespread hope in Russia that a new era of both economic and personal freedoms, democracy, and international cooperation would ensue. Armed with a new market economy, a population eager for change, and a constitution that promised democratic elections and a free press, it was hard to see what could go wrong. At first it truly seemed that once-communist Russia had finally found footing amongst the international cohort of democratic nations. This narrative, however, would be relatively short lived; over the span of the following several decades, the core of "Russian democracy" would be incrementally hollowed out by Russia's current president, Vladimir Putin, until all that remained was today's hollow semblance of what a true democratic nation should be.

The slow but steady dismantling of democratic principles in Russia has been multi-faceted – consolidating control of the media,[1] widespread and insidious manipulation of public opinion and belief,[2] altering the constitution to extend presidential term limits, unfettered access by Russian security forces to the massive surveillance network known as SORM2,[3] and most recently outlawing public criticism of government officials in an effort to silence critics are only a few of the steps Putin has taken to ensure he remains in power for the foreseeable future. Until recent years, however, one section of Russian life remained relatively free and unaltered by political pressure: the Russian internet (RuNet).[4] For many years the RuNet, which comprises the entire Russian speaking community on the internet, was a haven for all types of

1. M. Lipman and M. McFaul, *"Managed Democracy" in Russia*, 2001.
2. J. Nocetti, *"Digital Kremlin": Power and the Internet in Russia*, 2011.
3. Soldatov A. and Borogan I, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (PublicAffairs, 2015).
4. Lloyd J. Fossato F., *The Web that Failed: How opposition politics and independent initiatives are failing on the internet in Russia* (Reuters Institute for the Study of Journalism, 2008).

politically critical bloggers, voices of dissent, and marginalized groups in Russia. In fact it was even believed by former US president Ronald Reagan that "technology will make it increasingly difficult for the state to control the information its people receive ... the Goliath of totalitarianism will be brought down by the David of the microchip."[5] Unfortunately, recent Russian history has shown the contrary, as Putin has been forced to reckon with the danger of allowing a digital Wild West to grow unchecked beneath his nose. In particular, Putin has had his wary eye on the RuNet ever since the extremely effective use of various social media platforms in promoting and planning widespread protest that threatened the legitimacy of his rule during the 2011 mayoral elections in Moscow, and then again during the 2012 presidential election (which saw Putin reelected after a stint as prime minister).[6]

Nevertheless, Putin's ability to exercise control over the RuNet has met moderate success at best. This is due largely to the many existing digital tools that have been built to avoid censorship and empower individuals who live under almost any form of oppression. Messaging tools like Signal, WhatsApp and Russia's own Telegram, along with internet tools like Virtual Private Networks (VPNS) and The Onion Router (TOR) have strong encryption baked into their very design in a way that makes governmental oversight infeasible. These tools have carved out an almost untouchable digital space that allows people to voice their criticisms, find support in like-minded individuals, organize protests, and a slew of other "subversive" activities, the mere thought of which would cause a pro Putin Kremlin to shudder. In order for Putin clamp down on online dissidence the way he may wish, he would have to wage an outright war against encryption – the underlying tool that guarantees a safe digital

5. Fossato F., *The Web that Failed: How opposition politics and independent initiatives are failing on the internet in Russia.*

6. Petrova M. Enikolopov R. Makarin A., "Social Media and Protest Participation: Evidence from Russia", 2018,

sphere, even from the creators of the tools themselves – and wage a war he has.

For the most part, in keeping with the "democratic shell" Putin seems intent on peddling, this war has been waged in the name of making the lives of Russian citizens better. In an attempt to align public opinion with his agenda, Putin has argued that encryption is unsafe because it is used by criminals and terrorists to commit heinous crimes. To some extent, this is true – some criminal and terrorist organizations undoubtedly do make use of encrypted communication, and Russia can point to several instances where this was believably the case.[7] Moreover, this rhetoric is not unique to Russia: it has in fact been thrown around by other major democracies, including those that champion free speech and privacy, such as the United States. Nevertheless, while some criminals use encryption, the vast majority of users are of a less nefarious sort – they are instead privacy conscious individuals or organizations, journalists, people living under repressive regimes, and many, many people who are unaware that the programs and devices they use house built-in encryption technology[8]. Even so, Russia has joined the ranks of outwardly dictatorial countries like China and Iran by taking its attack on a free internet and on the people who make use of it to an extreme. In particular, the Russian-built messaging app Telegram has come under heavy fire as of late, with Russia attempting to enforce a total blockage of the app since April, 2018.

Maybe more than any other app used by Russians, Telegram embodies the battle between democracy-promoting technologies[9] and the anti-democratic trends present

7. C. Cheang, *Online Extremism in Russia: Assessing Putin's Move*, 2018, `http://hdl.handle.net/10220/46842`.

8. For example, many people are unaware that as of recently, Facebook Messenger, WhatsApp and Instagram have been merged to run as one messenger (with different environments depending on which app is used to access the platform) that incorporates by default strong encryption: Isaac M., "Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger", 2019, `https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html`

9. That is not to say that the apps themselves promote democracy, but rather access to unrestricted digital spaces and strong privacy promotes democratic processes.

in Russia. It provides a very interesting and peculiar case study as to how these types of technologies are developed, by whom, and for what purpose. It also shows the close and interdependent relationship that has formed between the world's big tech firms, such as Google, Amazon and Microsoft, and the role "big tech" plays in creating and protecting secure digital spaces. On the other hand, Telegram, which has found success as the main propagandistic arm of ISIS, highlights the legitimate consequences of "unbreakable" encryption falling into the hands of those who would use it to do evil. Unfortunately, it seems that this is a necessary evil, as there is no way to guarantee encryption's functionality for the innocent masses without making it equally functional for criminals.

The clampdown on internet privileges in Russia under Putin is not by any means limited to Telegram or even the blocking of webpages that cast Putin in a negative light, however. Additional technologies designed to obfuscate both the identity of an online individual and the content of their online habits (such as aforementioned technologies like VPNs and TOR), have also been banned, along with further restrictions being placed on the storage of data and user information. For example, a law enacted in June 2016, commonly referred to as the Yarovaya Law (named after the proposing legislator Irina Yarovaya) requires that all internet companies keep full logs and copies of all internet traffic, including calls, emails, images and videos for six months, and associated metadata for three years. It also requires that tech companies be able to provide the Russian Federal Security Service (FSB) with backdoors into encrypted communications (such as by storing logs of user content or by having access to encryption keys – two things Telegram has refused to do)[10],[11] As a measure of

10. I. Yarovaya, *Federal Law from 06.07.2016 Number 374-F3*, 2016, `https://ru.wikisource.org/wiki/`.

11. International Center for Non-Profit Law, *Overview of the Package of Changes into a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism*, 2016, `http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf`.

scale that shows the level of absurdity this bill entails, it is estimated that following the Yarovaya act would require roughly 158 exabytes of *additional* digital storage space[12] (or 158,000,000,000 gigabytes), when the entirety of Google's storage servers is estimated to be between 10-15 exabytes. This fact has neither gone unnoticed nor un-criticized by the Russian IT industry, which laughs at the ruling as impossible to comply with.[13]

Whether Putin likes it or not, or even whether or not he's willing to admit it, encryption tools tend to be very good at the jobs they set out to complete. Short of digitally isolating Russia, which China has found success in doing, his options to contend with the ever increasing, ever proliferating toolbox of anti-censorship technologies (coupled with an evermore digitally literate citizenry) are extremely limited. If Putin truly wishes to erode this element of freedom to further secure his already solidified grasp on power, he has a long and ugly battle ahead of him.

2 The Role of Digital Media, Communications, and Privacy in Democracy

2.1 Russia as a Democracy

It behooves this investigation into Russia's interference in online privacy and encryption tools to examine Russia's claim to democracy, as universal rights to privacy are often upheld as one of the underpinnings of a successful democracy.[14] Certainly, for

12. Smolaks M., "Putin wants Russia to build storage servers", 2016, `https://www.datacenterdynamics.com/news/putin-wants-russia-to-build-storage-servers/`.

13. K. Ermoshina and F. Musiani, "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era", *Media and Communication* 5, number 1 (2017), ISSN: 2183-2439.

14. United Nations, *Universal Declaration of Human Rights*, 1948.

any outsider looking in, Russia does not seem to function like a true democracy. Yet it claims to be so. In its own words, it is a "managed" or "sovereign" democracy – two Kremlin-coined terms that convey a) the Russian regime functions as a true democracy, and b) this claim must be accepted as fact, and any scrutiny of this fact will be viewed as an act of aggression.[15,16] To consider Russia a true democracy, there are many items that must be checked off from the list of "democratic norms,"[17] but some general items include political equality for all citizens, free, integrous, and sufficiently frequent elections, a free and multi-faceted press, and some forms of limitation on governmental power.[18] Additionally, to be defined as a *liberal democracy*, it must also be the case that Russia guarantees to all people the various freedoms considered to be inalienable human rights, such as freedom of religion, speech, political belief, individual expression, and the right to a private life free from governmental oversight and control.[19] At least outwardly, Russia seems to check a few of these boxes, namely sufficiently frequent elections and a free press.[20] However, while the Russian media may outwardly seem to be "free" in the sense that it is not directly institutionalized within the government, it can hardly be said to be free from an overt influence from Vladimir Putin and his regime. This was not always the case.

After the seizure of power by the first president of the Russian Federation, Boris Yeltsin, the notion of a free press, an unthinkable idea under Soviet authority, was promoted. As it turned out, Yeltsin favored a free press, partially because he saw it as an instrument to retain authority by preventing the communist party from regaining

15. Lipman and McFaul, *"Managed Democracy" in Russia.*
16. M. Lipman, *Putin's 'Sovereign Democracy'*, 2006.
17. Center for Civic Education, *Elements of Democracy: the fundamental principles, concepts, social foundations, and processes of democracy* (Center for Civic Education, 2007), ISBN: 0898182018.
18. Ibidem.
19. Nations, *Universal Declaration of Human Rights.*
20. Ibidem.

power.[21] In fact, even after Vladimir Putin took on the mantle of president of the Russian Federation, he outwardly continued to encourage a free press, even if his encouragement rang hollow. In a foreshadowing of his future attacks on a free press, Putin, in his first address to the Russian parliament in 2000, stated, "Sometimes... [the media] turn into means of mass disinformation and a tool of struggle against the state."[22] Since that address, Putin has frequently, often vehemently, attacked the press for reporting that ran contrary to his agenda, and as the early 2000s wore on, Putin slowly began to consolidate control of the traditional media by forcing out through various means most forms of independent reporting.[23] In several cases this meant the persecution and even murder of those outspoken against him (of whom Anna Politkovskaya, Alexander Litvinenko, and Boris Nemtsov are only several prominent examples).

Putin's attacks on a free press are not the only way in which the early 2000's semblance of budding democracy in Russia was undermined before it had a chance to firmly establish itself. Widespread claims of internal election corruption, especially in the 2011 mayoral election in Moscow and the 2012 presidential election, greatly undermine Russia's claim to an integrous election process.[24,25] Moreover, various transparent moves have been made over the years by Putin and his supporters to consolidate power, such as the restructuring of the Russian constitution to increase presidential terms from four to six years. It is even speculated that the Russian Duma has considered altering the constitution again to allow Putin to run again after his current term's expiration in 2024 – a move that is illegal under the current consti-

21. Lipman and McFaul, *"Managed Democracy" in Russia.*
22. Ibidem.
23. Ibidem.
24. Jim Nichol, *CRS Report for Congress Prepared for Members and Committees of Congress Russia's - March 2012 Presidential Election: Outcome and Implications*, 2012.
25. Herszenhorn D., "Putin Wins, but Opposition Keeps Pressing", 2012, `https://www.nytimes.com/2012/03/05/world/europe/russia-votes-in-presidential-election.html`.

tution.[26,27] It is interesting to note that despite an entrenched opposition to Putin's dictatorial tactics, Russia has been unable to prevent his consolidation of power. This can most likely be explained by post-Soviet history, which saw relative stability give way to economic ruin and mass shortages all across Russia. If anything can be said of Putin, it is that the Russian people believe he can offer stability (there is food on the shelves at the supermarket when a complete lack thereof in the 1990s is still remembered by many Russians) which has been desperately needed by Russia since the collapse of the Soviet Union, even if with that stability comes slow economic and social progression that borders on stagnation.[28] These facts, in conjunction with numerous other avenues that have been taken towards consolidation of power, clearly prevent Russia from being seen as having sufficient internal checks and balances to limit governmental power.

Another box of the "democratic checklist" that Russia, without scrutiny, may seem to check is that it affords many freedoms to its citizens. Among these freedoms that are enshrined in the Russian constitution are the right to life, the right to human dignity, the right to inviolability of private life along with personal and family secrets, the right to free speech, the right to disseminate information (and ironically a ban of censorship), the right to peaceful assembly, and a ban on various forms of supremacist propaganda (From article 29 of the Russian constitution: Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосход-

26. W. Partlett, "The Constitutionality of Vladimir Putin's Third Term", 2012, https://www.brookings.edu/opinions/the-constitutionality-of-vladimir-putins-third-term/.

27. C. Maza, "President for Life? Russia Considering Constitution Changes That Could Allow Vladimir Putin to Remain in Power", 2018, https://www.newsweek.com/president-life-russia-considering-constitution-changes-could-allow-vladimir-1271367.

28. C. Grant, "Putin's Russia: Stability and stagnation", 2013, https://www.cer.eu/insights/putins-russia-stability-and-stagnation.

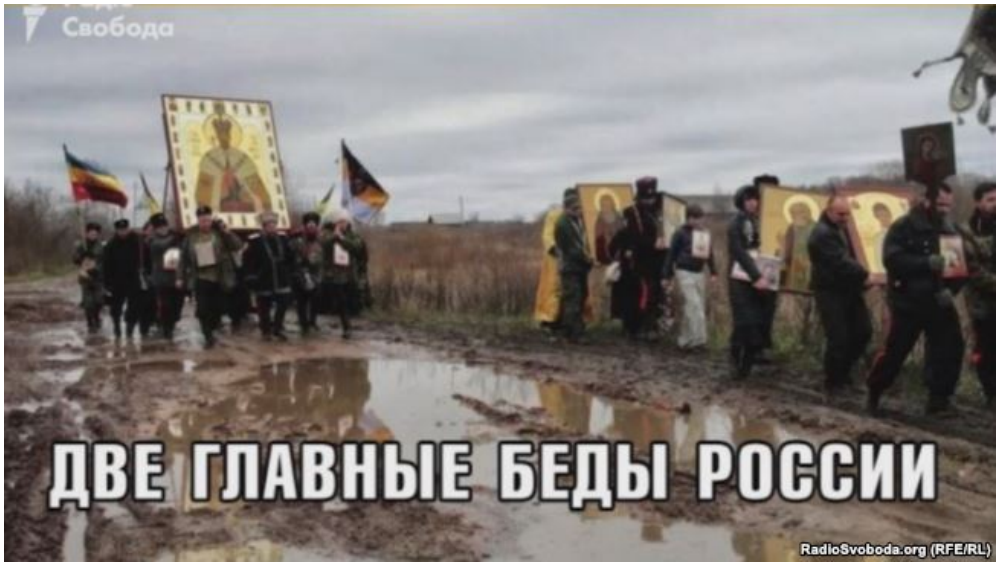
ства[29]). While some of these freedoms are unarguably violated (such as the right to privacy, which is violated by the massive surveillance network – SORM2 – built into the Russian IT infrastructure that can monitor 100% of Russian internet traffic without users' or ISP's knowledge[30]), the violation of others is much more subtle and insidious. One common trend that can be viewed as an infringement of Russian citizens' free speech comes as the consequence of the constitution's article 29, which bans certain types of speech. Two main articles of the Russian criminal code are often pointed to in connection with silencing free speech and stopping the dissemination of information – articles 280 and 282, which are titled Публичные призывы к осуществлению экстремистской деятельности (Public Appeals to Extremist Activity) and Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (Incitement to hatred or enmity, as well as the denigration of human dignity). Specifically, it is often alleged that the Russian courts interpret extremism very loosely and that FSB agents attempt to ensnare Russian citizens unknowingly in so-called "extremist activities."[31,32] Additionally, criticisms of the government or institutions of power are often viewed as acts that incite hatred against various groups. An example of this is outlined at https://ru.krymr.com/a/turma-za-repost-kak-rossia-ohotitsa-na-extremistov/29502428.html, where an individual shared a meme on Vkontakte that showed a picture of Russian clerics traversing a muddy road, along with the caption "The two main misfortunes of Russia" (Две главные беды России):

29. "Constitution of the Russian Federation", 1993, `http://www.constitution.ru/10003000/10003000-4.htm`.

30. A. and I, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*.

31. July D. Naboka M., "Tyurma za repost. Kak v Rossii ohotyatsa na «ekstremistov»", 2018, `https://ru.krymr.com/a/turma-za-repost-kak-rossia-ohotitsa-na-extremistov/29502428.html`.

32. Goble P., "FSB Increasingly Involved in Misuse of 'Anti-Extremism' Laws, SOVA Says", 2015, `http://www.interpretermag.com/fsb-increasingly-involved-in-misuse-of-anti-extremism-laws-sova-says/`.



Essentially, this photo is mocking two forms of corruption in Russia. The first is the Orthodox Church (which is headed by a close ally to Putin), and the poor state of Russian roads (which cannot be repaired due to lack of funding as the result of corrupt fiscal practices in the government).

In this case, the individual responsible for posting the meme faces six years in prison for "inciting hatred" and "insulting the feelings of believers." The poster has also been placed on the official governmental list of extremists. This instance is not isolated, and many other similar instances can be found where bans on inciting hatred or other harmful forms of speech have been twisted to punish those who express anything vaguely critical of Putin or his policies. Finally, in the midst of this project's writing, Putin signed further legislation that outright bans and makes punishable "fake news" and "disrespect of authority and the government," a move that

has been called arrant censorship by many.[33,34,35,36]

In conclusion, it would be tremendously difficult to seriously consider Russia a true democracy, despite its claims and attempts to be seen as one. More appropriately, Russia seems to have more in common with authoritarian-style governments. Nevertheless, Russia still claims it is a democracy despite the clear actions it has taken to undermine democracy not only abroad, but also at home. These claims, coupled with Russia's clearly established set of anti-democratic goals, makes the whole situation stand out as even more strange. Along with the plethora of ways in which Russia fails to be a democracy, it also continues to severely erode freedoms on the internet, which up until recent years was generally considered a more-or-less free space for Russian citizens to voice their dissenting opinions. Included in these "internet freedoms" are general rights to privacy, and specifically, the right to use strong encryption. However, before this can be argued, the case must be made that privacy and encryption are in fact essential components of a functioning democracy.

2.2 The Digital Public Sphere

Jurgen Habermas, renowned German philosopher and sociologist, coined the term "public sphere" in his 1962 book *Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft* (The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society) when examining how public settings such as coffee houses, cafes and salons affected the development

33. "Federal'ny zakon ot 18.03.2019 No. 31-f3", 2019, http://publication.pravo.gov.ru/Document/View/0001201903180031.

34. "Federal'ny zakon ot 18.03.2019 No. 30-f3", 2019, http://publication.pravo.gov.ru/Document/View/0001201903180022?index=0%5C&rangeSize=1.

35. "Putin podpisal zakony o feiknyus i neuvazhenii k vlasti", 2019, https://www.vedomosti.ru/politics/news/2019/03/18/796652-putin-feiknyus-neuvazhenii.

36. S. Sant, "Russia Criminalizes The Spread Of Online News Which 'Disrespects' The Government", 2019, https://www.npr.org/2019/03/18/704600310/russia-criminalizes-the-spread-of-online-news-which-disrespects-the-government.

of democracy in the eighteenth century. He explained that democracy grew out of these locations because they were where common citizens could gather to discuss the issues that were most relevant to them, and through these public discussions, influential public opinions could be formed. Briefly put, the public sphere should play the following role in society:

> Statements [within the public sphere] should consist of arguments, supported by an appropriate reasoning whose validity can then be checked by others. The best arguments should prevail. Participants should try to understand each other's arguments, and aim to see the situation from their point of view. Everybody should be honest and open, making a sincere effort to come to a joint conclusion. All interested parties should be allowed and enabled to participate and it should be possible to discuss all kinds of issues.[37]

Since he published his book, a tremendous amount of scholarly literature has been written about Habermas's thesis, especially his belief that the role of the public sphere is not fulfilled in contemporary society because mass media fails to promote true deliberation by commodifying information and discourse and only covering a small percentage of worthwhile issues.

In the modern day it can be argued that the internet plays much the same role as pubs, cafes and salons played in the propagation of information and opinion in the eighteenth century. As such, many Habermasian scholars have started to consider the validity of a new "digital public sphere" and the role such a notion plays when compared to the "old" public sphere. According to Schafer, much of this scholarship can be broken into two generic camps: "cyber-optimists" and "cyber-pessimists." In

37. Schafer M., *Digital Public Sphere*, 2015.

the cyber-optimist camp are those who believe that the internet provides a wealth of information leading to better public debates, that it gives voice to those traditionally underrepresented in society by making it easy to communicate with large audiences, and that decentralized networks circumvent the commodification of information present in traditional mass media. The cyber-pessimist camp contains those who worry that debate in the digital public sphere lacks diversity because people tend to seek out information they already agree with (this is commonly referred to as the "echo chamber"), that the internet is already as commodified and capitalist as mass media, and that many forms of online communication, such as trolling and hate speech, are counterproductive.

Whether the digital public sphere is conducive or more of a hindrance to democracy remains to be seen, as strong arguments and massive bodies of evidence can be found on both sides. What is undebatable is that individuals across the planet are now more capable of connecting with one another than ever before.

2.3 The Importance of Privacy, and Hence Encryption, in Democracy

It is widely accepted that the right to free speech is necessary for a functioning democracy, and this issue will not be discussed here (even though Russia has passed legislation curtailing citizens' speech rights that amounts to nothing less than censorship[38]). Instead, an argument as to why privacy and encryption are needed to protect free speech will be presented.

Evidence for the importance of privacy, and hence encryption, which is used to protect privacy, can be drawn directly from Russia, where since 2013 the promotion of

38. Sant, "Russia Criminalizes The Spread Of Online News Which 'Disrespects' The Government".

non-heterosexual relations and identities to minors has been illegal.[39] Effectively, the so-called propaganda law has also banned LGBTQ rights advocacy. In the "Ranking Digital Rights Project," Nathalie Marechal highlights how eroded privacy and encryption rights in Russia have affected members of this community:

> [The] de facto criminalization of LGBT rights advocacy ... has contributed to an increase in discrimination and assaults against LGBT Russians. Impunity prevails since hate crimes do not get reported, much less explicitly tagged as such. The Mayor of Sochi's infamous claim in the run-up to the 2014 Olympics, that 'there are no gays in Sochi,' was illustrative of the enforced obscurity endured by LGBT Russians. When the gay community's existence is denied, the idea of gay rights becomes inconceivable. Even among the minority who support LGBT rights, the climate of intimidation and fear has produced a chilling effect where would-be activists refrain from actions that might lead to reprisals, even when their activities are not deemed illegal.

Members of the LGBTQ community in Russia must be constantly on guard and very cautious about whom they share their thoughts with, because as outlined by Marechal, being identified as a member of the LGBTQ community or an LGBTQ advocate can quickly lead to being persecuted or the target of hate crimes. This also means such people must be cautious about how they choose to communicate with others when they aren't meeting face to face. As will be discussed in a later section of this thesis, the Russian SORM2 network acts as the backbone of Russian digital surveillance capabilities, and all unencrypted information that passes through Russian ISPs is capable of being quickly and effectively flagged, reviewed, monitored,

39. Nathalie Marechal, "Ranking Digital Rights Project: Keeping the Internet Safe for Advocacy", *The Fibreculture Journal* 26 (2015), ISSN: 1449-1443.

stored, blocked, and used to identify individuals based on whom they talk to, what they search, their political views, and many other factors. Because of this, activists of all sorts, including members of the LGBTQ community, are susceptible to being persecuted by the government unless they take steps to secure their online communications and identities. Without encryption, which both hides the content of online communications and the identities of the messengers, making discrimination more difficult, these individuals are at serious risk of persecution and imprisonment. This is harmful to democracy because it acts directly against people's ability to engage in freedom of speech, thought, and belief – freedoms without which there can be no public sphere.

It is here that English philosopher Jeremy Bentham's notion of *the panopticon* can be introduced to explain further why widespread, unchecked digital surveillance is harmful to democracy. In 1791 Bentham created a hypothetical circular prison system called a panopticon that entailed prison cells facing inward toward a guard post directly in the center. In a panopticon, the guard's booth is made so that prisoners cannot tell when they are being watched, but are aware that at any given moment they may be under surveillance.

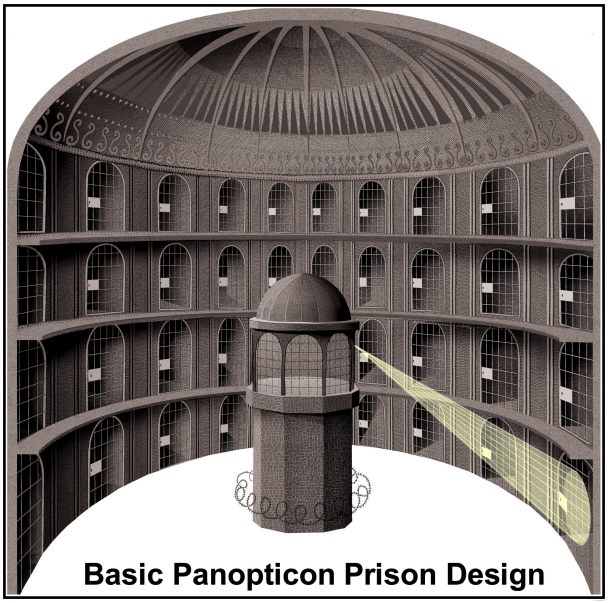


Figure 1: Figure showing the hypothetical setup of a Panopticon, borrowed from https://skyvisionsolutions.files.wordpress.com/2015/04/panopticon-prison-design.jpg

Bentham's hypothesis was that if prisoners knew that they could be monitored at any time without their knowledge, they would self-regulate and behave as though they were being watched constantly, thereby giving the guard the ability to reform an entire prison with minimal effort: "the objective is to assess an individual's likelihood for undesirable behavior, and to monitor, categorize, and rank so as to curb such behavior... producing disciplined and 'rational' (read predictable) citizens."[40] Twentieth century French philosopher Michel Foucault, who rediscovered the panopticon and is largely credited with popularizing it, further wrote that the panopticon's primary goal was "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" through what he termed "self-surveillance."[41]

It is not hard to envision how this theoretical framework translates into the digital

40. Carlson M. Campbell J., "Panopticon,com: Online Surveillance and the Commidification of Privacy", *Journal of Broadcasting and Electronic Media* 46, number 4 (2002).
41. Ibidem.

world, and in fact it was envisioned even before the creation of the World Wide Web. In the 1984 film rendition of George Orwell's novel *1984*, the film's director, Michael Radford, envisioned the panopticon through the telescreens used to monitor citizens (since the screens could be used to surveil anybody without their knowledge). The panopticon has also been used to describe the widespread use of closed-circuit television (CCTV) in shopping centers and public areas, the same crucial idea being that individuals who know they may be under surveillance at any given moment are more likely to act "rationally" than if they knew they were not being monitored (which in this case means not shoplifting).

The problem with a digital panopticon that is employed on a nation-wide scale (such as Russia's surveillance network, SORM2) is that citizens who know that all their online habits, contacts, communications and personas may be under observation at any moment have a tendency to do exactly what Bentham hypothesized prisoners in the panopticon would do – they self surveil and self regulate. This is detrimental for the functioning of a democracy because it prevents the formation of public opinion through open debate by forcing citizens into self-censorship, especially when they know that holding unpopular opinions can be punished by the government, as is the case with Russia. Anonymous speech, and hence encryption "is elementary to a democratic society, precisely because it facilitates the creation of a public communicative sphere of common experiences; precisely because it enables and shapes public discourse; precisely because it is of such vital importance to public interest," and as a result "[anonymous] and encrypted speech on the internet, though fraught with harmful side effects [such as their use by terrorist networks], should be strongly protected in view of its fundamental rights value" because the "result of suppressing a great majority's legal postings on the account of the existence of a minority of people abusing the internet... is an excessive restriction on the freedom of anonymous

speech... [and] treats all people as potential criminals in favour of investigative expediency."[42] The digital panopticon, justified in the name of "investigative expediency" is outright anti-democratic.

2.4 Big Tech's Role in the Digital Public Sphere

The world's biggest tech companies have also played a role in the functioning of democracy, and some would argue this has played out in both positive and negative ways. On the one hand, tech companies like FaceBook have come under fire recently for weakening the foundations of democracy due to their failure in moderating extremist content online and their platform's complicity in Russia's election meddling and misinformation campaigns. On the other hand, when tech companies take a firm stance against unreasonable governmental demands by keeping technology safe for everyone to use in the interest of protecting their users and preserving free speech and privacy online, they ensure democracy still has space to function.

Within this framework, namely the role big tech plays in forming and protecting a digital public sphere, it can be seen that most companies cannot be viewed through a monochromatic lens. For example, in 2015 the FBI officially requested through US courts that Apple create malware that would allow the decryption of San Bernardino attacker Syed Farook's phone, arguing that information on the phone was crucial to the ongoing investigation. Apple refused, claiming that creating decryption malware would weaken the overall security of their devices and create a dangerous precedent – after all, if the US government could force them to decrypt devices, what would stop countries like Russia, Iran, and China from doing the same? In this instance, Apple took a firm stance and protected digital privacy and encryption.[43] However,

42. Christoph Bezemek, *Behind a Veil of Obscurity - Anonymity, Encryption, Free Speech and Privacy*, 2016.

43. Pena R. Schmidt M., "F.B.I. Treating San Bernardino Attack as Terrorism Case", 2015, `https:`

in 2017, Apple announced that it would be removing VPNs, another crucial encryption/privacy tool, from the app store in China after the Chinese government told Apple they would ban iPhones if Apple continued to support subversive activities. In this case, China, which is a massive consumer of Apple products, used Apple's for-profit nature to undermine its citizens' access to information by making access to privacy and encryption much more difficult.[44] By making this decision, Apple is complicit in Chinese censorship, and as such the company plays a part in preventing a true digital public sphere in China from establishing itself.

Other tech companies have structured their services in a way that works around some of the issues companies like Apple face. Namely, these companies have found sustainability models that don't require for-profit decisions at the expense of their users (i.e. they are influenced by monetary concerns to a much lesser extent when compared to companies like Google, Amazon, Facebook and Apple). Some have gone even further, building their companies with strong encryption and decentralized networks that make undermining their users' security and privacy nearly impossible – even by the company itself. Such companies include Telegram, Signal and TOR. These companies go to great lengths, at great cost, to keep their services open to everyone, including people living under the thumbs of oppressive regimes (this will be discussed further in the Telegram section of this thesis).

In Russia specifically, the role big tech plays in carving out a space for free speech has likely been a source of bitter anxiety for Putin ever since the 2011/2012 election cycle. This is when he witnessed first hand the power, and hence danger, of social media as a platform for dissenting voices. During this time, the Russian social media site *Vkontakte*, which is similar in functionality to FaceBook, along with other major

//www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

44. "Apple 'pulls 60 VPNs from China App Store'", 2017, https://www.bbc.com/news/technology-40772375.

sites like Twitter, were used by Putin's opposition to promote and organize widespread protests that took place throughout Russia. Significantly, it is speculated by many that the protests could not have taken place on nearly the same scale had it not been for the unique digital space provided by social media.[45] As will be discussed more thoroughly in the Telegram section of this thesis, big tech's role in this fiasco did not end when the protests did; when Putin demanded information on his opposition, companies like Vkontakte took a firm stance and refused.

3 Crackdown on the RuNet

3.1 A Brief Overview of the RuNet

The World Wide Web and the notion of Russian democracy were born at roughly the same time and at first the two worked hand in hand. It was thought by many that despite Putin's clear intentions to stifle democracy in Russia, the internet would prevent the total erasure of democratic process by creating a space for open dialogue free from oppression and governmental control. The hope was that the "increasing penetration of telecommunication technologies and the growth of their use in Russia [would] allow Russian social forces to organise, to create strong horizontal ties and to empower themselves, in order to join in a debate on the country's governance, culture and society – and in doing so, strengthen civil society."[46] As the independence of the press and mass media in Russia was slowly compromised by Putin's regime, the RuNet remained one of the last free modes of communication to which Russians had

45. Enikolopov R., "Social Media and Protest Participation: Evidence from Russia".
46. Fossato F., *The Web that Failed: How opposition politics and independent initiatives are failing on the internet in Russia.*

access.[47] However, as has been stated, it has come under attack as well.

Effectively, the Russian government seeks to "Russify" the web by more tightly controlling Russian internet users and by building the needed digital infrastructure to have an independent internet.[48] The reasoning behind this is two-fold. First, by more tightly controlling the Russian internet, the Russian government is able to have greater control over its citizens. This has taken many forms, from requiring bloggers to register with the state,[49,50] banning encryption/privacy technologies such as VPNs and TOR, the Yarovaya packet, and strict monitoring of all Russian citizens' online activity through the SORM2 system. In various ways, each of these forms of control helps keep the current regime in power by making access to and propagation of reliable, critical information more difficult. Secondly, the Kremlin recognizes that the US has a tremendous amount of control over the internet as a whole because the biggest players in tech, such as Apple, Google, Amazon, Microsoft, and FaceBook are all American companies. If US-Russian relations were ever to deteriorate to the point that the US considered implementing sweeping digital blockades against Russia, the US could effectively shut down Russia's internet because of Russia's reliance on American companies. Recognizing this, the Kremlin has invested tremendous amounts of money into building its own equivalents of these services, such as the Russian search engine Yandex, the mail server Mail.ru, and the social media platform VKontakte.[51] The Russian government's promotion of Russian apps makes their decision to block Telegram all the more poignant since Telegram is considered by many to be "Russian" due to it's creators' prominent roles in Russian society.

47. Fossato F., *The Web that Failed: How opposition politics and independent initiatives are failing on the internet in Russia.*
48. Nocetti, *"Digital Kremlin": Power and the Internet in Russia.*
49. Ibidem.
50. Fossato F., *The Web that Failed: How opposition politics and independent initiatives are failing on the internet in Russia.*
51. Nocetti, *"Digital Kremlin": Power and the Internet in Russia.*

The Russian executive body in charge of controlling and censoring all forms of public media, from the traditional television and print media to the most modern forms of digital media, is known simply as the *Roskomnadzor* (although its full name is much more intimidating – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, which translates to "Federal Service for Surveillance in the Sphere of Communications, Information Technology and Mass Media"). In particular, the Roskomnadzor is the body in charge of implementing internet censorship, which it does by maintaining a large blacklist of Internet Protocol (IP) addresses that Internet Service Providers (ISPs) are required to filter out. Examples of sites whose IP addresses have been banned (either temporarily or permanently) include Wikipedia, GitHub, the Internet Archive, and Reddit.[52,53,54] At this point it should come as no surprise that these sites were accused of "hosting extremist content" that was seen as critical of Putin's regime.[55]

The crackdown on the RuNet is made especially significant by the role it has come to play in Russian society: "Given the increasing restrictions on offline media and political participation... the [RuNet] has [until now] remained surprisingly free from government interference... [Moreover, the] Russian blogosphere, Twitter and other online media clearly illustrate the emergence of an open, vibrant and diverse online media space that discusses and debates a wide range of political and social issues and that constitutes an independent alternative to broadcast and print media... [as well as] the growing use of digital platforms in social mobilization and civic action.[56]"

52. *TIFU by getting Reddit banned in Russia*, `https://www.reddit.com/r/tifu/comments/3grpdf/tifu_by_getting_reddit_banned_in_russia/`, Accessed: April, 2019.

53. Moody G., "Wayback Machine's 485 billion web pages blocked by Russian government order", 2015, `https://arstechnica.com/tech-policy/2015/06/wayback-machines-485-billion-web-pages-blocked-by-russian-government-order/`.

54. Klikasty, "GitHub snova okazalsya v reestre zapreshenikh v RF saytov", 2014, `https://www.opennet.ru/opennews/art.shtml?num=41171`.

55. P., "FSB Increasingly Involved in Misuse of 'Anti-Extremism' Laws, SOVA Says".

56. Alexanyan K. et al, "Exploring Russian Cyberspace: Digitally-Mediated Collective Action and

In conjunction with the FSB, the Roskomnadzor is also responsible for maintaining the Russian surveillance network, SORM2. SORM2 is the successor of the SORM surveillance network that existed under the Soviet Union. It has been carefully integrated into the Russian communications infrastructure, and is capable of automatic and widespread monitoring of everyone in Russia. This is achieved by forcing ISPs to install hardware at all locations that is capable of automatically scanning, analyzing, flagging, and capturing all in-transit data, both over the internet, and over cellular networks and phone lines.[57][58] Moreover, this data can be accessed by the FSB without a warrant and without notifying either the ISP or the individual whose data is being monitored. The SORM2 network has been widely condemned as a violation of basic human rights – including Russia's own constitution. Some organizations have even boldly fought against the SORM2 network by sending massive amounts of "flaggable" information over it (such as communications containing key words like "bomb," "terrorism," and "opposition") in an effort to overload the systems with false positives.[59]

Once again, these actions paint a clear picture: Putin is intentionally trying to stifle the digital public sphere in an attempt to retain power. If his opponents cannot organize or communicate because they are afraid of being caught by the SORM2 network and being punished, they cannot directly counteract the Kremlin's anti-democratic goals. However, the SORM2 network is not all powerful – it cannot read or analyze encrypted data that passes through it, and this is where technologies like Telegram come into play.

---

the Networked Public Sphere", 2012, `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014998`.

57. A. and I, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*.

58. Ermoshina and Musiani, "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era".

59. Ibidem.

4 Telegram

As has been mentioned, Telegram is a communication app created by Russian brothers Pavel and Nikolai Durov that blends aspects of traditional social media through offering "channels" that can be followed, along with aspects of many other security-focused instant messages by offering encrypted one-to-one and one-to-many messaging. The app is available for download on most platforms, including Android, iOS, Windows, Mac, and Linux. Contrary to the traditional configuration of other security-minded apps, Telegram does not employ end-to-end encryption by default. Rather, an individual must choose to enter a secret chat with the recipient of the would-be messages. At this point, however, messages are coded so that only the sender and receiver(s) are capable of reading a message's content.[60] Moreover, the messages are encoded in such a way that even upon legitimate requests from any law agency, the decrypted contents of messages cannot be turned over because Telegram developers do not have the technical capability for decryption. Even obtaining a legally binding warrant to attempt such an act is extremely difficult by the Durov brothers' design, as the company that houses Telegram has been broken up over various countries and jurisdictions in such a way that greatly reduces any single government's influence. This point is important because Telegram has essentially made itself an extra-judicial, extra-national entity that cannot be controlled by anyone other than Pavel Durov himself – a fact which plays directly into Durov's ideological belief that the internet

60. Although according to largely unverified claims in the Christopher Steele dossier, the very same in which it is claimed that Putin has kompromat of a very "sensitive nature" on Donald Trump, Telegram's encryption has been broken by Russian security services. This is, of course, a claim that Pavel Durov and the Telegram development team fully deny."Intelligence report claims the Kremlin has cracked Telegram service", 2017, `https://www.securitynewspaper.com/2017/01/16/intelligence-report-claims-kremlin-cracked-telegram-service/` While this claim cannot be proven, it is still true that Telegram often scores poorly when audited by security experts because of the way the Durov brothers created their own cryptography, rather than using a widely-accepted, time tested approach approved by mathematicians and cryptographers.

represents its own uncontrollable sovereign nation.[61]

4.1 Background and a Brief History

To understand the history of Telegram, it is first necessary to understand a bit about the history of its primary creators, brothers Pavel and Nikolai Durov. Pavel Durov is known by many as the "Mark Zuckerberg of Russia," largely because he was the primary creator of *Vkontakte*, a Russian social media platform that was created shortly after FaceBook, and which at first looked very similar to Facebook down to the font and the pale blue banner on a white background[62] (in fact, this was no accident - Durov borrowed directly from FaceBook and used it as inspiration for the creation of Vkontakte). Luckily for Durov, Vkontakte (or VK for short) had gained enough of a foothold in Russia by the time FaceBook opened itself to those who did not have a .edu email address that VK for a long time has remained the primary, dominant social media platform in the country. The current breakdown of VK to FaceBook users in Russia is approximately 49.5 to 21.4 million users respectively.[63]

While Pavel Durov may have borrowed from Zuckerberg's FaceBook, it would be remiss to say that he did not have his own vision of what social media (the very idea of which in 2006 was still in its infancy) and Vkontakte would look like. For him, "the best thing about Russia at the time was that the Internet sphere was completely not regulated,"[64] and as a self-declared cyber-libertarian and believer in the cypherpunk

61. N. Marechal, *From Russia with Crypto: A Political History of Telegram*, 2018.
62. Ibidem.
63. McDonald M., "Social Network Matchup: Vkontakte vs Facebook in Russia", 2014, `https://russiansearchmarketing.com/social-network-matchup-vkontakte-vrs-facebook-russia/`.
64. D. Hakim, *Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile*, 2014, `https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html?ref=technology&_r=1`.

movement[65],[66] Durov was determined to allow VK to be a sort of Wild West in the East. One step he took toward this effect was his 2007 decision allowing all VK members to upload and host content on the platform regardless of international copyright laws. As Durov put it, he wanted to "rid society of the burden of obsolete laws, licenses, and restrictions ... the best legislative initiative is absence."[67]

Naturally, having a libertarian, anti-state and anti-government pilot in the cockpit of such a powerful platform for the exchange of thought and information was worrisome to the Kremlin, especially as it was witnessing the early stages of a series of social-media driven uprisings that would eventually be known as the Arab Spring. In 2011 these worries came to fruition when, shortly after announcing that he would run in the presidential election of 2012, Putin was met with massive protests all over Russia that were tens of thousands people strong - protests that were organized and managed in part by the prominent opposition leader Alexei Navalny, who at the time was using VK and other platforms to disseminate information.[68]

Russian security services were quick to respond to this very real threat and demanded that Durov remove Navalny's and other protest oriented pages from VK. Instead, couched in a set of political beliefs that were as contrary to the Kremlin's thought process as possible, and in a move of stubborn, utter defiance, Durov reprogrammed parts of VK to give Navalny's page more visibility, and in a bold move

65. The *cypherpunk* movement stems from the cypherpunk manifesto which was released by activist Eric Hughes in 1993. Essentially, the manifesto states that widespread adoption of encryption and privacy technologies will lead to a digital utopia. The group's mission can be summed up from the manifesto, which is easily found online: "Privacy is necessary for an open society in the electronic age. ... We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy ... We must defend our own privacy if we expect to have any."

66. Marechal, *From Russia with Crypto: A Political History of Telegram.*

67. The magazine that published this excerpt from an interview seems to have deleted the content. However, the original Russian article can be viewed at https://web.archive.org/web/20170827112613/https://www.afisha.ru/article/pavel-durov-vkontakte/

68. Marechal, *From Russia with Crypto: A Political History of Telegram.*

responded on Twitter with a picture of a dog sticking its tongue out and wearing a hoodie:

His official response soon became:

> "If foreign sites continue to exist in a free state, and Russian ones begin to be censored, the RuNet can await only its slow death."[69]

In their traditional style, the FSB showed up ready to break down Durov's door in a heartbeat, and it is here that Pavel came up with the idea of Telegram after realizing that he was unable to securely communicate with his brother and mentor, Nikolai Durov, without the Russian government being able to see everything. In other words, Telegram was created at least in part with the intention of undermining the Kremlin's ability to surveil the Durov brothers' communications:

69. Yaffa J., "Is Pavel Durov, Russia's Zuckerberg, a Kremlin Target?", 2013, `https://www.bloomberg.com/news/articles/2013-08-01/is-pavel-durov-russias-zuckerberg-a-kremlin-target`.

> "In 2012 my brother and I built an encrypted messaging app for our personal use - we wanted to be able to securely pass on information to each other, in an environment where WhatsApp and other tools were easily monitored by the authorities."[70]

Nikolai, who holds two PhDs in mathematics, was able to come up with his own encryption scheme that he and Pavel then coded into a personal app that would eventually serve as the framework for Telegram.

Even armed with the power of secure communication in hand, Pavel's Vkontakte woes didn't cease here. By 2013, still the head of VK, Pavel had fled Russia, and despite continued demands from the FSB for data about Russian and Ukranian citizens involved in protest, Pavel refused to capitulate. In a show of further resentment for the Kremlin and its demands, he released Telegram publicly in that same year. In 2014 he found out through a post on social media that VK had ousted him as head of the company, at which point he was forced to sell his stock to a Russian oligarch with close ties to the Kremlin.[71]

Since then, the Durov brothers have become extremely vocal advocates of encryption and rights to online privacy. They continue to run Telegram from abroad, frequently moving where the project is housed to prevent the app from falling under the purview and jurisdiction of any single government for too long a period. It is also interesting that Telegram, unlike almost any other encrypted messengers, is not tied to Silicon Valley or to the United States Internet Freedom Agenda, nor does it mine user data as a way to generate ad revenue. Instead, the project is completely funded by Pavel Durov himself, who according to the official FAQ on Telegram's website

70. Ermoshina and Musiani, "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era".

71. Marechal, *From Russia with Crypto: A Political History of Telegram.*

"supplied Telegram with a generous donation",[72] likely with the fortune Durov was able to amass in his time as head of Vkontakte. In fact, Telegram as it stands has no way to make money beyond donations, which are primarily solicited through the "Donate Bot" found at an extension of the Telegram website.[73] This situation presents a problem because even Durov's fortune, reported to be around $260 million at the time of giving up VK,[74] cannot be enough to foot the operational costs of a project as big as Telegram forever, and the Telegram team is painfully aware of this. Publicly they have said that they may one day introduce "nonessential paid options to support the infrastructure and finance developer salaries."[75]

In the meantime, and in a natural extension of their already cypherpunk ideology, the Durov brothers turned to the world of blockchain technologies, both as a fix for their funding issue (blockchain technologies, such as cryptocurrency, are capable of amassing tremendous amounts of money very quickly with little risk for developers) and as a way to continue offering their users new functionality. In early 2018 it was announced that Telegram would be holding an Initial Coin Offering (the means by which the very first "coins" of a cryptocurency are sold to those hoping to invest) for their devised cryptocurrency "Gram," which was to be the first of Telegram's blockchain implementations structured under the Telegram Open Network (TON). In a series of both public and secret "presale" offerings, Telegram was able to raise an astonishing $1.7 billion dollars, shortly after which the official ICO was canceled altogether. Investors were never refunded.[76] It is widely speculated that this bold

72. *FAQ: How are you going to make money out of this?*, `https://telegram.org/faq\#q-how-are-you-going-to-make-money-out-of-this`, Accessed: April, 2019.

73. *Telegram Donate Bot*, `https://t.me/telegramdonate`, Accessed: April, 2019.

74. Cook J., "The incredible life of Pavel Durov — 'Russia's Mark Zuckerberg' who is raising $2 billion for his messaging app", 2018, `https://www.businessinsider.com/the-incredible-life-of-pavel-durov-the-entrepreneur-known-as-the-mark-zuckerberg-of-russia-2016-3?r=UK`.

75. *FAQ: How are you going to make money out of this?*

76. Marechal, *From Russia with Crypto: A Political History of Telegram.*

move by the Telegram team to cancel the ICO and then pocket the massive sum obtained by misleading investors was actually a ploy to stay afloat rather than to support the Telegram Open Network.

Shortly after the ICO was cancelled, Telegram announced in a blog post that it had reached 200 million unique users.[77] Much of Telegrams popularity can be attributed to the purchase and monetization of WhatsApp by Facebook, as when this event occurred, there was a surge of new Telegram users who were likely worried about FaceBook's data practices.[78]

4.2 Telegram's Functionality

Today Telegram consists of both a mobile and desktop platform and can be downloaded on iOS, Android, Windows, MacOS, and Linux, and can also be accessed via its website at https://web.telegram.org. Upon download, users must register an account, which requires user verification via a telephone number. Once an account is created, the following screen, minus the pre-existing subscriptions and chats (found along the lefthand column) appears:[79]

77. Durov P., "200,000,000 Monthly Active Users", 2018, `https://telegram.org/blog/200-million`.

78. Ermoshina and Musiani, "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era".

79. This is specifically Telegram downloaded on Linux OS, operating in the GNOME desktop environment

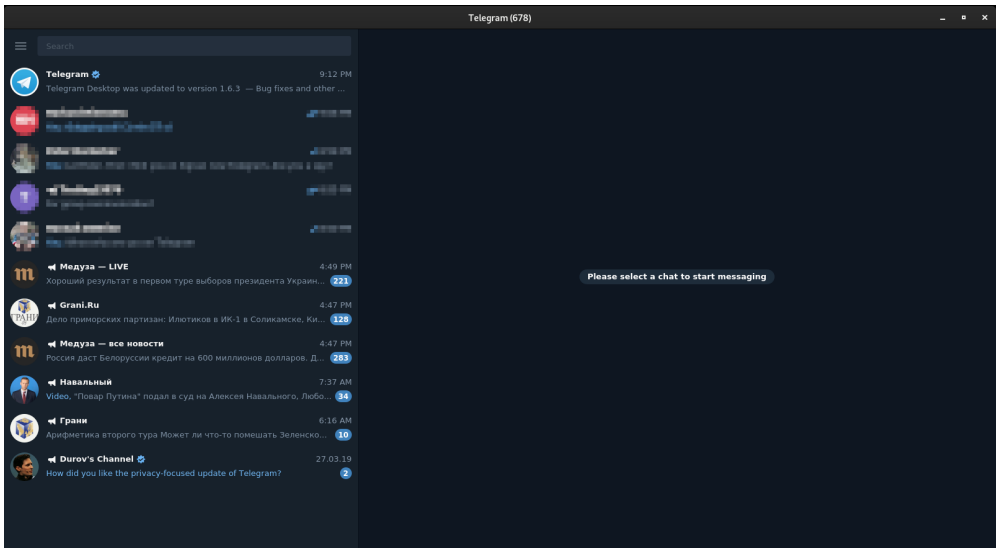


Figure 2: Telegram Opening Screen

Telegram is a multi-functioning app that is rich in features and that has a clean, clear layout. It serves both as a social media platform through its one-to-many messaging capabilities as well as its many-to-many "group chats," and as a direct messenger through its one-to-one messaging capabilities. The one-to-many messaging component of Telegram is made up of *channels*, which can be created by any user and can be made either public, allowing them to be found via the "search" bar, or private, preventing anyone without a direct invitation from joining. Within a channel, only a single user – the channel creator – can post. In general, users can share a wide variety of content, such as written text, links, videos, pictures, audio files, and other downloadable content up to 1.5 gigabytes in size. This feature allows individuals or organizations to create a dedicated news feed to proliferate information that can reach large audiences without channel subscribers having the ability to comment. It also creates a central hub from which content can be made accessible, as content like downloads or photos are easily searchable within a channel. Some example channels include Alexei Navalny's channel, Pavel Durov's channel, and the Meduza news chan-

nel. Any channel can have an unlimited number of followers. Generic group chats, which can have up to 200,000 members and individual messaging work similarly and allow Telegram users to communicate with one another much like other messaging apps. Specific to group chats, users can create simple polls that allow all users to vote on content, whereas specific to individual messaging, users have the added ability to initiate voice calls. Users also have the option to create "secret" chats that use the MTProto mobile protocol for end-to-end encrypted messaging. It should be noted that this is one of the widely-held criticisms of Telegram as a secure messenger, because end-to-end encryption is not enabled by default and requires manual selection by users. Within these secret chats, one can set "destruction timers" so that messages are permanently erased after a predetermined time is up. The most recent addition to Telegram's set of privacy tools which was released on March 27th, 2019 (and not as an early April Fools' day joke, which would be entirely within Pavel Durov's style) is the ability for a user to delete his or her messages – individual or in bulk – from within individual chats or groups. When a user chooses to use this function, they can decide whether to delete messages from only their own devices, or to delete messages from all devices (which would remove messages from others' devices as well). An individual cannot delete other users' content from any device except their own.[80] As of April 1st, 2019, nearly a week after the addition of the feature, an ongoing poll seeking to find whether or not users are happy with this recent addition has an almost even split with 49% voting "Awesome, keep it up!" and 51% voting "Awful, take it back!"

Of important note is the role Telegram played in the Slavic world before it was banned. In many cases, Telegram was used as a channel for dispersing information the Kremlin viewed as undesirable. For example, activists and researchers in Eastern

80. Durov P., Pavel Durov's Telegram Channel, March 27, 2019.

Ukraine used Telegram to communicate and share information related to Russia's annexation of Crimea. Additionally, news platforms such as Grani.ru and Meduza, which were blocked by Roskomnadzor in 2014 as a consequence of their anti-Kremlin and pro-Ukranian views, had dedicated Telegram channels that allowed their readers to continue accessing news that was free from the Kremlin's slant.[81] Moreover, prominent Russian dissidents such as Aleksei Navalny have maintained Telegram channels with a very large group of followers. The combination of Telegram's popularty and wide spread use in Russia, along with its encryption, its dissident users and Pavel Durov's disgraced status in Russia has solidified Telegram as a priority target for the Kremlin, putting it squarely in Putin's line of sight.

4.3 The Ban

While Telegram was officially banned in Russia in 2018, the road that led to its ban took much longer and its start dates back to 2016 with the passing of the Yarovaya laws. Specifically, the laws (or rather, the packet of laws collectively referred to as the Yarovaya packet) made it a legal obligation that all tech companies must store their users' information in such a way that it can be made available to Russian security services upon request. In the case of encryption, this extends to the actual plaintext content of an encrypted message, and not just the encrypted data that actually lives on a given messaging platform's actual servers.[82,83] The Yarovaya packet included a plethora of other requirements, like forcing tech companies to log almost every type of data for various periods of time depending on the type and source of the internet traffic. Of notable importance, this data that is to be stored must be stored on

81. Ermoshina and Musiani, "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era".

82. Yarovaya, *Federal Law from 06.07.2016 Number 374-F3.*

83. Non-Profit Law, *Overview of the Package of Changes into a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism.*

servers that are physically located within Russia, ensuring that the FSB can gain physical access to them should the need arise. Interestingly, LinkedIn, Microsoft's social media platform tailored to professional social networking, was the first foreign website to be banned under the new legislation for failure to move the data it stored from Russian citizens to servers located within Russia. Telegram actually complied with many components of the Yarovaya packet,[84] including the storage requirements, except for the component that forced them to make decryption keys available to the FSB. In fact, this request was futile in the first place, as Telegram does not store encryption keys for its encryption scheme that is based on 256-bit AES, and 2048-bit RSA encryption, as well as Diffie-Helman key exchange. Even if Telegram wanted to, it would be unable to access decryption keys.[85] Needless to say, the Russian government was not sympathetic to this argument, and Telegram was fined under the Yarovaya packet in the amount of 800,000 rubles ($14,000 USD) for being found in violation of the law. In March of 2018 Telegram lost its appeal and in early April, the Russian media watchdog, Roskomnadzor asked the courts to ban the messaging platform altogether. Only seven days later, in an 18-minute court proceeding, the app was officially banned and internet service providers were ordered to start filtering any and all IP addresses associated with the platform.

The Russian courts made no attempt to hide why Telegram was being blocked, stating "Telegram Messenger Limited Liability Partnership не исполнена обязанность по предоставлению в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений[86]" (Telegram

84. Marechal, *From Russia with Crypto: A Political History of Telegram.*

85. *FAQ: So how do you encrypt data?*, `https://telegram.org/faq\#q-so-how-do-you-encrypt-data`, Accessed: April, 2019.

86. *Reshenie imenem Rossiskoy Federatsi, 13 aprelya 2018 goda*, `http://docs.pravo.ru/document/view/103012389/117395823/`, Accessed: March, 2019, 2018.

Messenger Limited Liability Partnership did not fulfill the obligation to provide the Federal Security Service of the Russian Federation with information necessary to decode received, transmitted, delivered and (or) processed communications). However, what the court document *does* attempt to hide is the fact that the entire hearing was sprung on Telegram in such a way that Telegram had almost no time to formally respond, or even to represent itself in court. Specifically, the document states that "Представитель заинтересованного лица Telegram Messenger Limited Liability Partnership в судебное заседание не явился, о дне, времени и месте рассмотрения дела извещен надлежащим образом[87]" (The representative of the interested party Telegram Messenger Limited Liability Partnership did not appear at the hearing, the day, time and place of which were duly notified). This is hotly contested by Telegram.[88] Concluding the court proceding, the judge decided that because Telegram would not cooperate with the FSB, a total blockage of Telegram was necessary:

> [Решил] установить на территории Российской Федерации ограничение доступа к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» и функционирование которых обеспечивается Telegram Messenger Limited Liability Partnership, до исполнения указанным организатором распространения информации в сети «Интернет» обязанности по представлению в федеральный орган исполнительной власти в области обеспечения безопасности информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых элек-

87. *Reshenie imenem Rossiskoy Federatsi, 13 aprelya 2018 goda.*
88. Marechal, *From Russia with Crypto: A Political History of Telegram.*

тронных сообщений.[89]

...

[It has been decided] to establish on the territory of the Russian Federation restriction of access to information systems and (or) programs for electronic computers that are designed and (or) used for receiving, transmitting, delivering and (or) processing electronic messages of Internet users, the functioning of which is ensured by Telegram Messenger Limited Liability Partnership, before the specified organizer of information dissemination on the Internet is obliged to submit to the federal executive body in the category of security information necessary for decoding received, transmitted, delivered and (or) processed electronic messages.

Demanding one thing and successfully carrying it through are two different beasts, and in the case of Telegram, implementing an effective ban has proved too difficult for Russia, even to the time of writing. This is due largely to the fact that Pavel Durov and his team have intentionally structured the app around preventing mass blockages or governmental oversight in general. Moreover, the initial attempt to block Telegram wreaked havoc in Russia and resulted in a near shutdown of the RuNet. Even so, Telegram has remained largely unblockable in Russia because since Iran attempted to block Telegram, it has been using a practice known as *domain fronting*[90] which essentially hides Telegram's content behind the masks of larger tech companies like Amazon and Google (this practice will soon be explained in depth). To do this, Telegram hosts their content on servers provided by large tech companies in a way that allows them to quickly and easily switch their IP addresses if they notice that a particular IP has been blocked in some location, as well as to partially hide the fact

89. *Reshenie imenem Rossiskoy Federatsi, 13 aprelya 2018 goda.*

90. Zenz K., "OOPSIE - Russia Accidentally Sabotages Its Internet", 2018, `https://www.thedailybeast.com/russia-accidentally-sabotages-its-internet`.

that the service is being used by making internet traffic to and from the Telegram servers look more like standard traffic going to and from Google or Amazon. When the Roskomnadzor issued the order to block Telegram, ISPs were given a massive list of IP addresses associated with the service so that they could filter out any attempts to connect to those IPs. In fact, the list of IP addresses that needed to be blocked number approximately 16 million – about 0.45 percent of all possible IP addresses.

Since ISPs had no choice but to follow the Roskomnadzor's orders, they obliged by blocking all 16 million IP addresses. The consequences showed themselves almost immediately: because of the way Telegram was enacting its domain fronting,[91] the list of 16 million IP addresses it had been using were shared by many other tech organizations. When the block against that list was enacted, many services in addition to Telegram (or more so *rather* than Telegram) were also blocked. Included in this list were Nintendo servers, the popular messaging app Viber, several banks' online platforms, online Volvo diagnostics used by dealers, and for some internet users, services like Gmail, YouTube and Spotify. Even online Microsoft-affiliated platforms became inaccessible. Ironically, the messaging app TamTam, which is owned by the Russian tech giant Mail.ru (and is ultimately under the control of Alisher Usmanov, a prominent Putin crony[92]), and which was promoted by the Kremlin as the best alternative to Telegram, was also consequentially shut down during the attempted Telegram block. In a particularly painful sting, the Kremlin completely lost its own

91. In a side note, since the showdown between Telegram and the Russian government, both Google and Amazon Web Services have announced that they will no longer support domain fronting. This has been overwhelmingly criticized many privacy/security/human rights advocates, as domain fronting is one of the primary tools used by communications platforms to circumvent censorship in repressive countries. The announcement to shut down domain fronting has been viewed as major tech companies capitulating to Russia's demands, and came despite calls from authoritative international civil liberties advocates such as the International Network of Civil Liberties Organizations.

92. Savov V., "Russia's Telegram ban is a big, convoluted mess", 2018, `https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban`.

ability to process ticket sales for Kremlin museum tours.[93,94,95] Russian citizens, even politicians with close ties to the Kremlin, quickly and fiercely criticized the move, claiming that it was unjustified for Roskomnadzor to ban lawful citizens from using legal, everyday services for the sake of targeting one company. This is especially poignant for a majority of Russians who were affected given that a state-run poll indicated that only one third of Russian citizens were against the ban, and only 12% of Russians actually used the app regularly in the first place.[96] It was also a point of embarrassment that the Kremlin's main spokesman, Dmitry Peskov, continued to use Telegram after the ban to schedule conference calls and press briefings with Putin himself, claiming that until he was forced to switch to a new platform because Telegram stopped working, he would continue using the app. Specifically, he offered the following excuse: "[У меня] он работает для меня, и ничего в этом такого нет," (which roughly translates to "it works for me and that's all there is to it.")[97,98]

As has been stated, Telegram largely continues to work in Russia according to Reddit users as of early March, 2019 – despite the ban.[99] But even though it works, it still has semi-frequent outages, and depending on the ISP an individual is connected to, it may not work at all. Undeterred, many Telegram users have adopted additional internet privacy and security measures to completely circumvent any at-

93. Burgess M., "Pochemu popytki Rossii zablokirovat' Telegram provalilis'", 2018, https://inosmi.ru/politic/20180429/242119825.html.

94. K., "OOPSIE - Russia Accidentally Sabotages Its Internet".

95. Emmanouilidou L. Maynes C., "Russian authorities want to ban Telegram in the country. But it's not going as well as they had hoped.", 2018, https://www.pri.org/stories/2018-04-17/russian-authorities-want-ban-telegram-country-its-not-going-well-they-had-hoped.

96. *Dannye oprosov: Telegram, proshay!*, https://wciom.ru/index.php?id=236&uid=9062, 2018.

97. M., "Pochemu popytki Rossii zablokirovat' Telegram provalilis"'.

98. MacFarquhar N., "Russian Court Bans Telegram App After 18-Minute Hearing", 2018, https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html?action=click%5C&contentCollection=Europe%5C&module=inline%5C&region=Marginalia%5C&pgtype=article.

99. *Is Telegram still blocked in Russia?*, https://www.reddit.com/r/Telegram/comments/at8tj9/is_telegram_still_blocked_in_russia/, Accessed: April, 2019.

tempt by Roskomnadzor to restrict access. In a way, Russia's ban of Telegram falls under the Streisand effect, whereby the actual attempt to cover up or hide information promotes and makes the information more visible, rather than what was intended. Since Telegram was banned, services like VPNs and TOR have seen a tremendous increase in interest. According to one source, right after the Telegram ban was enacted, online searches for encryption technology through Yandex.ru (Russia's online search engine, roughly equivalent to Google) jumped by an average of 260%, with major VPN providers reporting a three fold increase in new subscribers.[100] It is significant to note that this occurred despite a 2017 ban of all anonymizing software (which includes both conventional VPNs and TOR) in Russia. These services, in addition to allowing users to circumvent traditional censorship and surveillance measures, also allow Telegram users to connect to the app without the Russian government being able to see the activity. Both are also widely used for circumvention in other repressive states where heavy handed state-mandated censorship is enforced, such as China and Iran.

As has been stated, Telegram was initially very successful in skirting the Russian ban (where about 10% of its total users were located as of the ban's enactment)[101] due to a very powerful digital anti-censorship tool called domain fronting. Without getting too technical, domain fronting works via the following principle: when an internet user visits a website, they send three domain name requests over the DNS, TLS, and HTTP(s) protocols (DNS, or Domain Name Service, is the "phonebook" of the internet that translates urls into physical hardware addresses, TLS or Transport Layer

100. Newman S., "vpnMentor Study: Interest in VPNs in Russia Soar After Telegram Ban", 2018, https://www.vpnmentor.com/blog/vpnmentor-study-interest-vpns-russia-soar-telegram-ban/.

101. Rapoza K., "How Messaging App Telegram Gets Around Russia's Ban", 2018, https://www.forbes.com/sites/kenrapoza/2018/04/19/how-messaging-app-telegram-gets-around-russias-ban/#55594d225240.

Security provides users with secure connections, and HTTP(s) or Hyper Text Transfer Protocol (secure) is a protocol used to transfer HTML code that is interpreted by web browsers to build websites on a user's device). Of these, the HTTPs domain name is encrypted, and so a censor cannot see what the eventual address of the HTTPs request is. The other two, however, are sent to a web server that is allowed by censors, such as Google or Amazon web services. Once they arrive, the HTTPs domain request is decrypted, and the internet traffic is allowed to travel to the final destination. Information returning to the main user passes again through the service being used for domain fronting (Google, Amazon, etc), where the source is re-encrypted before it is sent to the initial user. To any censor or anyone who doesn't have control over the domain fronting server, all internet traffic will look like it is moving between the domain front and the user, essentially obfuscating the true nature of the user's online actions.

Only days after the Telegram ban in Russia, domain fronting stopped working not only for Telegram in Russia, but for other major anti-censorship tools across the world. At first the developers of these tools were unsure why it had ceased to work, but after a press release from Google the reason became clear:[102]

> Domain fronting has never been a supported feature at Google, but until recently it worked because of a quirk of our software stack. We're constantly evolving our network, and as part of a planned software update, domain fronting no longer works. We don't have any plans to offer it as a feature.

Shortly after Google's clampdown on domain fronting, Amazon similarly shut it down

102. Finjan Team, "What is Domain Fronting?", 2018, `https://blog.finjan.com/what-is-domain-fronting/`.

on their servers, citing concerns that the tool could be used for the spread of malware:[103]

> Tools including malware can use this technique between completely unrelated domains to evade restrictions and blocks that can be imposed at the TLS/SSL layer.

Many working in the technological industry who advocate for anti-censorship tools speculate that the decision to shut down domain fronting by most of the web's biggest players was not a spontaneous decision, nor that it was truly centered around the need to protect people from potential misuse. Rather, they speculate that the standoff between freedom online and dictatorial governments wishing to crack down on dissent was costing these big tech companies vast sums of revenue, since countries like Russia and Iran had clearly demonstrated their willingness to hold big tech hostage unless they got what they wanted.[104] In this sense, companies like Google and Amazon are culpable in the blockage of encrypted communication tools by dictatorial regimes. As Peter Micek, who is general council for the international internet freedom advocacy group Access Now put it:

> Google knows this block will levy immediate, adverse effects on human rights defenders, journalists, and others struggling to reach the open internet. To issue this decision with a shrug of the shoulders, disclaiming responsibility, damages the company's reputation and further fragments trust online broadly, for the foreseeable future.[105]

103. Team, "What is Domain Fronting?"
104. Claburn T., "Google kills off domain fronting – and so secure comms just got tougher", 2018, `https://www.theregister.co.uk/2018/04/19/google_domain_fronting/`.
105. Access Now, "Google ends "domain fronting," a crucial way for tools to evade censors", 2018, `https://www.accessnow.org/google-ends-domain-fronting-a-crucial-way-for-tools-to-evade-censors/`.

Despite the fact that Telegram can no longer use domain fronting as a tool to evade Russia's blockade on their servers, Telegram has remained accessible to a majority of Russians, and there is another reason for this. After realizing that they could not rely on Google or Amazon for censorship evasion, Pavel Durov started investing vast sums of money in the form of Bitcoin into various online services that also promised to help affected users bypass restrictions, calling the initiative the "Digital Resistance," and stating:

> To support internet freedoms in Russia and elsewhere I started giving out Bitcoin grants to individuals and companies who run socks5 proxies and VPN. I am happy to donate millions of dollars this year to this cause, and hope that other people will follow... For us, this was an easy decision. We promised our users 100% privacy and would rather cease to exist than violate this promise.[106]

However, this initiative may not entirely answer the question of why Telegram has continued to work so well for so many Russians, even for those who don't use digital censorship evasion tools. As it turns out, it may be the case that Russia is not as worried about the strength of Telegram's encryption as it purported to be. In the salacious dossier that was compiled by the British former MI6 agent Christopher Steele, and that claimed the Kremlin is in possession of various forms of compromising material on the current president of the United States, Donald Drumpf, it is alleged that Russia has successfully found a way to circumvent Telegram's privacy and encryption measures.[107] This may suggest that despite the official ban being in effect, the initial level of resources allocated to blocking Telegram was largely for show, because even if encryption keys were not being made available to the FSB, the FSB may have found

106. Durov P., Pavel Durov's Telegram Channel, April 1, 2019.
107. Tim Greene, *Trump doc claims Russia has cracked Telegram messaging service*, 2017.

some work around that allowed them to decrypt content regardless. Of course, this is speculative, as the Steele dossier was compiled in 2016 before the 2018 ban, and has not been verified in its entirety (although many of its key claims have been, which adds to the report's overall veracity).[108,109] It is also wholly possible that any defect in Telegram's security found by the FSB has since been fixed, or that at least this specific element of the report is false, which Telegram spokesman Markus Ra claims is most likely. Another possibility is that the report may be referring to an incident in May of 2016, when the Telegram accounts of two Russian activists were compromised after a hacker was able to capture the login codes sent to the activists' telephones via text message.[110]

4.4 Legitimate Criticisms of Telegram and its Use in Terrorist Organizations

It has been stated that the Russian government has taken a particularly hard stance against Telegram under the guise of anti-terrorism rather than as an affront to democracy. While this is almost definitely not the Kremlin's true motivation (or at least the entirety of its motivation), it is actually true that a legitimate case can be made against Telegram's use by terrorist organizations, notably the Islamic State in Iraq and Syria (ISIS). This is because Telegram has been adopted as the main platform used by ISIS for propaganda, proliferation of "terrorist how-to's" (such as bomb making, maximizing effectiveness of lone wolf attacks and crediting ISIS with attacks

108. Wood P., "Trump Russia dossier key claim 'verified'", 2017, `https://www.bbc.com/news/world-us-canada-39435786`.
109. Sipher J., "The Steele Report, Revisited", 2017, `https://slate.com/news-and-politics/2017/09/a-lot-of-the-steele-dossier-has-since-been-corroborated.html`.
110. Ghosh S., "Telegram says claims it was hacked by Russian spies are 'fake'", 2017, `https://www.businessinsider.com/donald-trump-document-telegram-hacked-russia-fsb-2017-1/`.

that have been successfully carried out), and secure communications between group members.[111] In particular, the group has gravitated towards Telegram because of its unique status as both a social media app and a direct messenger capable of encrypted one-to-one messaging and private one-to-many and many-to-many communications. These functions have been integral to ISIS's refined ability to use digital media and social networks to gain new recruits, disseminate information, and plot in secrecy. According to Shehabat, ISIS has migrated to Telegram because:

1) [it is] seeking encryption,

2) [it is] seeking a channel-supporting platform,

3) [Telegram] enhances ISIS's digital infrastructure against cyber-attacks, and

4) [Telegram] decreases exposure to hacktivism and other information warfare counter-measures.[112]

Isis's use of Telegram has made monitoring ISIS a challenge for governments around the world, especially because of Telegram's privacy focused mission. Because Telegram groups can be created so that joining requires a direct invitation from a group member, it is very difficult for anti-terror organizations to infiltrate the terrorist group's networks. Even Telegram administrators have trouble identifying ISIS-affiliated accounts, and as such in order for accounts to be suspended they must first be reported by the collective of Telegram users.

111. Alzoubi Y. Shehabat A. Mitew T., "Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West", *Journal of Strategic Security* 10, number 3 (2017).

112. In an interesting case of vigilante hacktivism, the loosely-defined hacking collective Anonymous has vowed to take on ISIS via a digital front. Anonymous has successfully targeted many thousands of ISIS's Twitter accounts, often turning them into pro-gay, pornographic and pro-Anonymous Twitter accounts. "Anonymous hacks pro-ISIS Twitter accounts, fills them with gay pride", 2016, `https://www.cbsnews.com/news/anonymous-hacks-pro-isis-twitter-accounts-fills-them-with-gay-pride/`

As this implies, Telegram, in a move that strays from its mostly "hands off" philosophy, has taken a stance against ISIS's use of the platform for furthering its terrorist agenda. Whenever new ISIS channels are identified, they are reviewed by the app's administrators and then removed. However, this strategy has been largely ineffective for a number of reasons. First, removing ISIS-affiliated accounts does not prevent accounts from being recreated. Because of the relative ease with which users can create new accounts, it would be very difficult to pinpoint ISIS members who are trying to recreate deleted accounts. Effectually this has turned removing ISIS members from the platform into a game of whack-a-mole, as they can only be removed once they've popped back up. It is unclear precisely how many ISIS channels have been blocked, but the number is surely in the thousands. Secondly, as Pavel Durov himself has lamented, it may never be truly possible to root out ISIS on the platform because "[Telegram] does not read private information and private messages."[113] Even so, Durov has made little more commitment to combating ISIS on Telegram than removing their publicly identified accounts.

In Russia specifically, there is one notable instance when Telegram was implicated in a terrorist attack (although the attack was not tied to ISIS). The attack, which was carried out by a person who was ethnically Slavic, occurred on 31 October, 2018, in an FSB office in the Russian city of Arkhangelsk. The perpetrator, a teen who ignited an explosive device and consequently died in the attack, had posted to a Russian anarchist community on Telegram seven minutes before the attack claiming responsibility.[114]

Despite encryption's use by terrorists and criminals, there is no way to weaken encryption only in those cases where there is a legitimate reason to monitor (let alone

113. Walt V., "With Telegram, A Reclusive Social Media Star Rises Again", 2016, `http://fortune.com/telegram-pavel-durov-mobile-world-congress/`.
114. Cheang, *Online Extremism in Russia: Assessing Putin's Move*.

the issue inherent in determining who should decide what constitutes such a legitimate reason). This is because the math that makes strong encryption possible cannot be selectively manipulated: if Telegram were to build a back door into its service that allowed international governments to more easily find and eliminate terrorist accounts, there would be nothing stopping a bad actor with vast resources (cue the Russian national anthem) from finding intentional mathematical vulnerabilities and exploiting them for its own purposes. It is for this reason that encryption *must* be made strong for *everyone*, because otherwise it cannot fulfill its role in ensuring a digital public sphere that is truly governed by the public.

5 Conclusion

The current status of free speech, privacy and encryption in Russia can be used to make the case that history is in fact cyclical, as much of what can be said of today's Russia in these fields could also be said of Russia under the Soviet Union. A key difference, however, is that the Soviet Union was outwardly anti-democratic, whereas the Russian Federation attempts to strike a different tune. Putin would have both his own public and the rest of the world believe that Russia is a free, democratic country. Clearly this is not the case.

There is yet another striking difference between the USSR and Russia – the battle of suppression and censorship Putin faces if he chooses to continue denying his public the democracy they desire will be much more grueling than the battle faced by his predecessors. The evolution of digital technology has paved the way for decentralized, difficult-to-control, and impossible-to-monitor spaces that nurture, if not outright promote, a strong and organized opposition. These voices of dissent, which have continued to act as a thorn in Putin's side despite his efforts to quell them

through both the state apparatus and through extra-legal measures, have been given a platform that allows them to reach an extensive audience and that Putin himself has been largely unable to reign in.

This is not to say that the de facto use of technology promotes democracy or even that it is a good thing. On the contrary, the proliferation of insecure communication technologies through the internet has given governments worldwide an unprecedented ability to surveil, censor, and punish ordinary citizens. The argument to be made is that as the technological arms race between censor and citizen evolves, it seems that the citizen has finally found the upper hand. For every step backaward, there are two steps forward. Hopefully it can one day be said that this incremental progress brings humanity to the point where any act of censorship is so futile that no governing body bothers even to attempt it. Nevertheless, even upon the realization of this utopian ideal, strong privacy tools, be they through encryption or through as yet unthought-of means, will be vital to protect human rights, because where there is the potential for someone to consolidate and abuse power, there will be someone attempting to do exactly that.

6 References

A., Soldatov, and Borogan I. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. PublicAffairs, 2015.

al, Alexanyan K. et. "Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere", 2012. `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014998`.

"Anonymous hacks pro-ISIS Twitter accounts, fills them with gay pride", 2016. `https://www.cbsnews.com/news/anonymous-hacks-pro-isis-twitter-accounts-fills-them-with-gay-pride/`.

"Apple 'pulls 60 VPNs from China App Store'", 2017. `https://www.bbc.com/news/technology-40772375`.

Bezemek, Christoph. *Behind a Veil of Obscurity - Anonymity, Encryption, Free Speech and Privacy*, 2016.

Campbell J., Carlson M. "Panopticon,com: Online Surveillance and the Commidification of Privacy". *Journal of Broadcasting and Electronic Media* 46, number 4 (2002).

Cheang, C. *Online Extremism in Russia: Assessing Putin's Move*, 2018. `http://hdl.handle.net/10220/46842`.

Civic Education, Center for. *Elements of Democracy: the fundamental principles, concepts, social foundations, and processes of democracy*. Center for Civic Education, 2007. ISBN: 0898182018.

"Constitution of the Russian Federation", 1993. http://www.constitution.ru/10003000/10003000-4.htm.

D., Herszenhorn. "Putin Wins, but Opposition Keeps Pressing", 2012. https://www.nytimes.com/2012/03/05/world/europe/russia-votes-in-presidential-election.html.

Dannye oprosov: Telegram, proshay! https://wciom.ru/index.php?id=236&uid=9062, 2018.

Enikolopov R., Petrova M., Makarin A. "Social Media and Protest Participation: Evidence from Russia", 2018.

Ermoshina, K., and F. Musiani. "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era". *Media and Communication* 5, number 1 (2017). ISSN: 2183-2439.

FAQ: How are you going to make money out of this? https://telegram.org/faq\#q-how-are-you-going-to-make-money-out-of-this. Accessed: April, 2019.

FAQ: So how do you encrypt data? https://telegram.org/faq\#q-so-how-do-you-encrypt-data. Accessed: April, 2019.

"Federal'ny zakon ot 18.03.2019 No. 30-f3", 2019. http://publication.pravo.gov.ru/Document/View/0001201903180022?index=0%5C&rangeSize=1.

"Federal'ny zakon ot 18.03.2019 No. 31-f3", 2019. http://publication.pravo.gov.ru/Document/View/0001201903180031.

Fossato F., Lloyd J. *The Web that Failed: How opposition politics and independent initiatives are failing on the internet in Russia*. Reuters Institute for the Study of Journalism, 2008.

G., Moody. "Wayback Machine's 485 billion web pages blocked by Russian government order", 2015. https://arstechnica.com/tech-policy/2015/06/wayback-machines-485-billion-web-pages-blocked-by-russian-government-order/.

Grant, C. "Putin's Russia: Stability and stagnation", 2013. https://www.cer.eu/insights/putins-russia-stability-and-stagnation.

Greene, Tim. *Trump doc claims Russia has cracked Telegram messaging service*, 2017.

Hakim, D. *Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile*, 2014. https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html?ref=technology&_r=1.

"Intelligence report claims the Kremlin has cracked Telegram service", 2017. https://www.securitynewspaper.com/2017/01/16/intelligence-report-claims-kremlin-cracked-telegram-service/.

Is Telegram still blocked in Russia? https://www.reddit.com/r/Telegram/comments/at8tj9/is_telegram_still_blocked_in_russia/. Accessed: April, 2019.

J., Cook. “The incredible life of Pavel Durov — ’Russia’s Mark Zuckerberg’ who is raising $2 billion for his messaging app”, 2018. https://www.businessinsider.com/the-incredible-life-of-pavel-durov-the-entrepreneur-known-as-the-mark-zuckerberg-of-russia-2016-3?r=UK.

J., Sipher. “The Steele Report, Revisited”, 2017. https://slate.com/news-and-politics/2017/09/a-lot-of-the-steele-dossier-has-since-been-corroborated.html.

J., Yaffa. “Is Pavel Durov, Russia’s Zuckerberg, a Kremlin Target?”, 2013. https://www.bloomberg.com/news/articles/2013-08-01/is-pavel-durov-russias-zuckerberg-a-kremlin-target.

K., Rapoza. “How Messaging App Telegram Gets Around Russia’s Ban”, 2018. https://www.forbes.com/sites/kenrapoza/2018/04/19/how-messaging-app-telegram-gets-around-russias-ban/#55594d225240.

K., Zenz. “OOPSIE - Russia Accidentally Sabotages Its Internet”, 2018. https://www.thedailybeast.com/russia-accidentally-sabotages-its-internet.

Klikasty. “GitHub snova okazalsya v reestre zapreshenikh v RF saytov”, 2014. https://www.opennet.ru/opennews/art.shtml?num=41171.

Lipman, M. *Putin’s ’Sovereign Democracy’*, 2006.

Lipman, M., and M. McFaul. *"Managed Democracy" in Russia*, 2001.

M., Burgess. “Pochemu popytki Rossii zablokirovat’ Telegram provalilis’”, 2018. https://inosmi.ru/politic/20180429/242119825.html.

M., Isaac. “Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger”, 2019. https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html.

M., McDonald. “Social Network Matchup: Vkontakte vs Facebook in Russia”, 2014. https://russiansearchmarketing.com/social-network-matchup-vkontakte-vrs-facebook-russia/.

M., Schafer. *Digital Public Sphere*, 2015.

M., Smolaks. “Putin wants Russia to build storage servers”, 2016. https://www.datacenterdynamics.com/news/putin-wants-russia-to-build-storage-servers/.

Marechal, N. *From Russia with Crypto: A Political History of Telegram*, 2018.

Marechal, Nathalie. “Ranking Digital Rights Project: Keeping the Internet Safe for Advocacy”. *The Fibreculture Journal* 26 (2015). ISSN: 1449-1443.

Maynes C., Emmanouilidou L. “Russian authorities want to ban Telegram in the country. But it’s not going as well as they had hoped.”, 2018. https://www.pri.org/stories/2018-04-17/russian-authorities-want-ban-telegram-country-its-not-going-well-they-had-hoped.

Maza, C. “President for Life? Russia Considering Constitution Changes That Could Allow Vladimir Putin to Remain in Power”, 2018. https://www.newsweek.com/president-life-russia-considering-constitution-changes-could-allow-vladimir-1271367.

N., MacFarquhar. “Russian Court Bans Telegram App After 18-Minute Hearing”, 2018. https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html?action=click%5C&contentCollection=Europe%5C&module=inline%5C&region=Marginalia%5C&pgtype=article.

Naboka M., July D. “Tyurma za repost. Kak v Rossii ohotyatsa na «ekstremistov»”, 2018. https://ru.krymr.com/a/turma-za-repost-kak-rossia-ohotitsa-na-extremistov/29502428.html.

Nations, United. *Universal Declaration of Human Rights*, 1948.

Nichol, Jim. *CRS Report for Congress Prepared for Members and Committees of Congress Russia's - March 2012 Presidential Election: Outcome and Implications*, 2012.

Nocetti, J. *"Digital Kremlin": Power and the Internet in Russia*, 2011.

Non-Profit Law, International Center for. *Overview of the Package of Changes into a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism*, 2016. http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf.

Now, Access. “Google ends “domain fronting,” a crucial way for tools to evade censors”, 2018. https://www.accessnow.org/google-ends-domain-fronting-a-crucial-way-for-tools-to-evade-censors/.

P., Durov. Pavel Durov's Telegram Channel. March 27, 2019.

———. Pavel Durov's Telegram Channel. April 1, 2019.

P., Durov. “200,000,000 Monthly Active Users”, 2018. https://telegram.org/blog/200-million.

P., Goble. “FSB Increasingly Involved in Misuse of ‘Anti-Extremism’ Laws, SOVA Says”, 2015. http://www.interpretermag.com/fsb-increasingly-involved-in-misuse-of-anti-extremism-laws-sova-says/.

P., Wood. “Trump Russia dossier key claim ’verified’”, 2017. https://www.bbc.com/news/world-us-canada-39435786.

Partlett, W. “The Constitutionality of Vladimir Putin’s Third Term”, 2012. https://www.brookings.edu/opinions/the-constitutionality-of-vladimir-putins-third-term/.

“Putin podpisal zakony o feiknyus i neuvazhenii k vlasti”, 2019. https://www.vedomosti.ru/politics/news/2019/03/18/796652-putin-feiknyus-neuvazhenii.

Reshenie imenem Rossiskoy Federatsi, 13 aprelya 2018 goda. http://docs.pravo.ru/document/view/103012389/117395823/. Accessed: March, 2019, 2018.

S., Ghosh. “Telegram says claims it was hacked by Russian spies are ’fake’”, 2017. https://www.businessinsider.com/donald-trump-document-telegram-hacked-russia-fsb-2017-1/.

S., Newman. “vpnMentor Study: Interest in VPNs in Russia Soar After Telegram Ban”, 2018. https://www.vpnmentor.com/blog/vpnmentor-study-interest-vpns-russia-soar-telegram-ban/.

Sant, S. "Russia Criminalizes The Spread Of Online News Which 'Disrespects' The Government", 2019. https://www.npr.org/2019/03/18/704600310/russia-criminalizes-the-spread-of-online-news-which-disrespects-the-government.

Schmidt M., Pena R. "F.B.I. Treating San Bernardino Attack as Terrorism Case", 2015. https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

Shehabat A., Alzoubi Y., Mitew T. "Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West". *Journal of Strategic Security* 10, number 3 (2017).

T., Claburn. "Google kills off domain fronting – and so secure comms just got tougher", 2018. https://www.theregister.co.uk/2018/04/19/google_domain_fronting/.

Team, Finjan. "What is Domain Fronting?", 2018. https://blog.finjan.com/what-is-domain-fronting/.

Telegram Donate Bot. https://t.me/telegramdonate. Accessed: April, 2019.

TIFU by getting Reddit banned in Russia. https://www.reddit.com/r/tifu/comments/3grpdf/tifu_by_getting_reddit_banned_in_russia/. Accessed: April, 2019.

V., Savov. "Russia's Telegram ban is a big, convoluted mess", 2018. https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban.

V., Walt. "With Telegram, A Reclusive Social Media Star Rises Again", 2016. http://fortune.com/telegram-pavel-durov-mobile-world-congress/.

Yarovaya, I. *Federal Law from 06.07.2016 Number 374-F3*, 2016. https://ru.wikisource.org/wiki/.