From Russia With Crypto: A Political History of Telegram[1]

Nathalie Maréchal, *University of Southern California*

Abstract

This paper offers a political history of Telegram, a platform that combines aspects of social networking with secure messaging, and whose vocal commitment to user privacy and freedom of expression has brought it into open conflict with a number of governments, most recently in Iran and Russia. A detailed project history traces Telegram's roots to Pavel Durov's ouster from Vkontakte, the social networking site he had founded, at the behest of the Kremlin. The paper then analyzes Telegram's ideology and politics by focusing, in turn, on Telegram's emergence in the context of Vladimir Putin's crackdown on technologically-enabled civil society; on Pavel Durov's cyber-libertarianism; and on Telegram's peculiar business model. The analysis shows that while Telegram's rhetoric emphasizes user security, privacy, and freedom of expression, the company fails to demonstrate that it actually lives up to these commitments. Rather than earning user trust through transparency and accountability, Telegram's value proposition hinges on blind trust on Pavel Durov's good intentions and his team's stated credentials.

1. Introduction

Many governments are increasingly willing and able to surveil internet users and to control the flow of information within and across their borders. In response, various groups are developing software tools to maintain privacy and/or access to the open internet and preserve an important "coordination good" — an activity people engage in to win power, but that governments can restrict in order to undermine disruptive social movements without excessive repercussions on the economy (Bueno de Mesquita and Downs, 2006). These "digital rights technologies" (Maréchal, 2018) allow individuals to better protect their privacy, access the information they wish to access notwithstanding censorship attempts by nation-states or other actors, express themselves as they wish in both the public sphere and in private, or any combination of the above. Controversially, many such tools have institutional, financial, or ideological ties to the U.S. Internet Freedom agenda, to Silicon Valley corporations, or both, raising vital questions about the relationship between U.S. power, social movements, and international relations in the 21st century. But unfortunately, much of the discussion about digital rights technology fails to adequately distinguish between Internet Freedom as a component of U.S. foreign policy, the commercial interests of Silicon Valley corporations, and digital rights as a normative commitment to human rights online. Understanding these new digital rights technologies, their development histories, their business models, and the ideologies that discursively sustain them is vital for understanding communication, politics, and power in the 21st century.

This paper, which is part of a broader study on the political economy of digital rights technology (see Maréchal, 2018), examines one tool that lacks any connections to the Internet Freedom agenda, to Silicon Valley, or to the United States: Telegram, a platform that combines aspects of social networking with secure messaging. In fact, founder Pavel Durov has been publicly critical of the Internet Freedom agenda as an ideology, arguing that U.S. government funding renders tools like Signal and Tor fundamentally untrustworthy (Levine, 2017). But even as Telegram rejects the discourse of liberation technology (Diamond, 2010), it positions itself as an alternative to Silicon Valley platforms and to tools linked to the U.S. Internet Freedom agenda for users who value "freedom," particularly freedom from a heavy-handed state (Durov, 2018), discursively linking itself to related concepts like emanci-

[1] This conference paper is adapted from Chapter 8 of my PhD dissertation (2018), titled *Use Signal, Use Tor? The Political Economy of Digital Rights Technology*. The study explores the political economy surrounding some of the new communications tools undergirding 21st century social movements through four case studies focused on digital rights technology projects: Psiphon, Tor, Signal, and Telegram.

patory communication practices (Milan, 2013) and freedom technologists (Postill, 2014). Indeed, Telegram grew out of an effort to thwart Russian state surveillance, and the literature supporting Telegram's early 2018 Initial Coin Offering (ICO) positions the company as an explicitly libertarian project (Telegram, 2018). It thus provides an interesting contrast to other digital rights technology projects, whose cyber-libertarian leanings are tempered by the rhetoric of human rights and by the transparency and oversight requirements associated with nonprofit status, contractual obligations, and/or grant reporting requirements.

We begin with an overview of basic information about Telegram: what it is, what it does, and how. Next, a detailed project history traces Telegram's roots to Pavel Durov's ouster from Vkontakte, the social networking site he had founded, at the behest of the Kremlin. The following sections analyze Telegram's ideology and politics by focusing, in turn, on Telegram's emergence in the context of Vladimir Putin's crackdown on technologically-enabled civil society; on Pavel Durov's particular brand of cyber-libertarianism and its cypherpunk roots; and on Telegram's peculiar business model, which allows Telegram to operate without answering to any higher authority than Pavel Durov himself.

1.1. Data, sources and methods

This study is based on content analysis of Telegram's publications and of public statements by the Durov brothers (many communicated via Telegram itself), analysis of media coverage, and secondary sources, as well as select interviews with cryptographers and others with expertise on the subject matter. Most of the consulted sources were in English, and I used Google Translate on a small number of Russian-language sources.

Following the walkthrough method for studying apps described by Light et al. (2016), I downloaded the Telegram app on my personal iPhone.[2] The user interface is very simple, featuring a contacts list, a list of chats (groups and individual interlocutors), and the settings interface. In addition to exchanging messages with individual contacts or groups of contacts, users can also subscribe to large group chats known as Channels, which can include up to 100,000 users. These public Channels are akin to email distribution lists and are notably used in Iran to circumvent restrictions on the traditional mass media. The Telegram app lacks a discovery mechanism, however, and it seems that most users select Channels to follow through word-of-mouth or by consulting lists maintained online. I followed "Durov's Channel," which Pavel Durov uses to communicate with users directly, throughout the fieldwork period. Telegram's API is open, allowing the use of third-party clients.

1.2. The basics: What is Telegram?

Telegram is a smartphone and desktop application that combines "secure" messaging with elements of a social networking site, developed by Russian-born brothers Pavel and Nikolai Durov and launched in August 2013 (though Telegram's security claims merit further scrutiny). As of March 2018, Telegram boasted 200 million monthly active users (Durov, 2018). Its all-male, 15-person development team is currently based in Dubai, and reportedly comprises "ethnic Russians" exclusively (Telegram, 2018; Walt, 2016).

The Durovs had previously founded the social networking site Vkontakte or VK, but were forced out by the Kremlin after the platform was used to organize mass protests against the results of the 2011 legislative elections, widely suspected of being rigged in favor of Vladimir Putin's United Russia party. The FSB, Russia's security service and a successor agency to the KGB, asked VK to turn over user information and to remove certain content relating to the protests, which Vkontakte CEO Pavel Durov refused to do. He was subsequently forced to sell his interest in VK to an oligarch close to the Kremlin, after which the shares were sold to the Russian internet company mail.ru.

The brothers have been living in exile ever since, and Telegram's team has operated from a variety of loca-

[2] The walkthrough method is "grounded in a combination of science and technology studies with cultural studies" (Light et al, 2016, p. 1), and "is a way of engaging directly with an app's user interface to examine its technological mechanisms and embedded cultural references to understand how it guides users and shapes their experiences" (p. 2). The process invites the researcher to engage with the app in the same way that a new user would, from initial sign-up, to usage, to exiting from the app (including terminating one's user account, if applicable).

tions around Europe before recently moving to Dubai (Telegram, 2018; Walt, 2016). Telegram was entirely funded by Pavel Durov himself until early 2018, when the company announced an ambitious plan to develop a blockchain-based ecosystem comprising encrypted cloud storage, censorship-resistant technology, and a cryptocurrency called the "Gram" (Telegram, 2018). As of early April 2018, an Initial Coin Offering (ICO) presale had raised over $1.7 billion, after which the formal ICO itself was cancelled, possibly as a way to sidestep Securities and Exchange Commission (SEC) requirements (Jeffries, 2018; Moore, 2018).

2. Project history

Telegram is the brainchild of Russian brothers Nikolai and Pavel Durov, who previously founded the social site Vkontakte or VK (meaning "in contact," in Russian). The sons of a university classics professor, the brothers spent part of their childhood in Italy before returning to their native St. Petersburg. The eldest, Nikolai, holds two PhDs in mathematics, while Pavel studied linguistics at St. Petersburg State University and learned computer programming from his brother. After university, he "trained in propaganda" as part of his compulsory military service, immersing himself in the writings of Sun Tzu, Genghis Khan, and Napoleon (Hakim, 2014; Yaffa, 2013).

Pavel Durov was in his early 20s when Facebook first launched on American college campuses, and he was among a handful of Russian developers racing to build the first Russian social networking site. VKontakte launched in 2006, with a graphic user interface that is noticeably similar to Facebook's, down to the blue-and-white color palette. By the time Facebook opened itself to all users — and not just those with a .edu email address — VKontakte had cornered the market on the Russian-speaking internet, known as the RuNet.

The Western media often calls Pavel Durov "the Russian Mark Zuckerberg," and his personal philosophy does indeed have much in common with Silicon Valley cyber-libertarianism. He started VK during the fleeting period of time when it seemed that Russia might be transitioning to a functional democracy, telling the New York Times that "the best thing about Russia at that time was the Internet sphere was completely not regulated. In some ways, it was more liberal than the United States" (Hakim, 2014). Since then, of course, the state has clamped down on all forms of media, including the internet, as we will see in the next section. "Since I'm obviously a believer in free markets," Durov told the New York Times, "it's hard for me to understand the current direction of the country" (Hakim, 2014).

Durov says that he's "not a big fan of the idea of countries" (Hakim, 2014), and often seems to thumb his nose at the idea of national sovereignty, particularly at the idea that national laws apply online, bringing to mind J.P. Barlow's Declaration of the Independence of Cyberspace (1996). For example, in 2007, Durov decided to allow VK users to upload music and videos regardless of copyright, drawing opprobrium from the U.S. government and lawsuits from the recording industry. The company didn't start proactively enforcing copyright laws until late 2013, after the Duma, Russia's legislature, passed a law ordering that sites that facilitate copyright violations be blocked (Dredge, 2014; Hakim, 2014; Yaffa, 2013). In a 2012 manifesto published in the magazine *Afisha*, Durov argued that Russia should "rid society of the burden of obsolete laws, licenses, and restrictions … the best legislative initiative is absence" (Durov, 2012, cited in Yaffa, 2013).

By 2011, Vkontakte was Russia's leading internet property. Like elsewhere, internet users in Russia took advantage of the platform's affordances to create groups and organize events of all kinds, including many dedicated to politics and social causes. In a country where civic and political activities had long been strictly controlled by the ruling Communist Party, this newfound ability for ordinary citizens to self-organize represented a threat to the status quo. Moreover, Russian political elites were highly suspicious of the internet, which it held responsible for a host of perceived maladies as varied as youth suicide, drug usage, homosexuality, and critiques of traditional society and religion (Maréchal, 2017; Ognyanova, 2015). Vladimir Putin had then been prime minister for three years, following two terms as president (2000-2008). In September 2011, the Duma extended presidential terms from four to six years, and Putin announced that he would run for president in the 2012 election. For many Russians as well as foreign

observers, the announcement dashed what hopes remained that Russia would complete its democratic transition. The legislative elections that December were marred by reports of widespread voter fraud, and tens of thousands of Russians took to the streets in Moscow and other cities to protest both the flawed election and the increasingly autocratic United Russia party, to which both Putin and president Dmitry Medvedev belonged. Opposition leader and blogger Alexei Navalny was particularly active on social media, using VK among other platforms to organize protests and to disseminate information related to his many grievances against the government. It was starting to look like Russia may be about to have its own "Color Revolution," which some dubbed the "Snow Revolution" (Ioffe, 2011; White & McAllister, 2014).

Less than a year after the start of the Arab Spring, the received wisdom at the time was that social media "caused" revolutions, or at the very least made them possible in otherwise stable autocracies (see Shirky, 2011). There was little to be done about foreign platforms like Facebook and Twitter, at least in the short term, but the Russian security services quickly pressured Vkontakte to shut down Navalny's page and other groups used to plan demonstrations. Instead, the rebellious Durov modified the site to give Navalny's posts greater visibility, and posted his "official reaction" on Twitter: an image of a hoodie-wearing dog, sticking its tongue out. He later issued an "open letter" couching his refusal to cooperate in business terms: "If foreign sites continue to exist in a free state, and Russian ones begin to be censored, the RuNet [Russian-language Internet] can await only its slow death" (Durov, 2011, cited in Yaffa, 2013). The security forces appeared at his door soon after; Durov refused to let them in.

Durov says that this is the moment that Telegram was conceived. "The no. 1 reason for me to support and help launch Telegram was to build a means of communication that can't be accessed by the Russian security agencies," he told Tech Crunch (Tsotsias, 2014). With police threatening to break down his front door, Durov called his brother Nikolai. "I realized I don't have a safe means of communications with him," he told the New York Times. "That's how Telegram started" (Hakim, 2014). Before long, the pair "cobbled together" an encrypted messaging system to avoid surveillance by the FSB (Walt, 2016). The fact that the Durovs "rolled their own crypto" rather than building on established protocols and consulting expert cryptographers looms large in technical critiques of the platform's security.

Protests continued for several months, occasionally punctuated by mass arrests and by counter-protests in support of Putin and United Russia. Putin won the May 2012 presidential election, appointing his predecessor Medvedev as prime minister (Soldatov & Borogan, 2015).

In April 2013, Pavel Durov fled Russia for Buffalo, New York, after being charged with allegedly running over a police officer's foot with a car, and focused his attention on the tool that would eventually become Telegram. The charges were quickly dropped, as they had achieved their objective: running Durov out of the country. He was still nominally the head of VK and owned 12% of the company, but he mostly kept a low profile. One exception came in August, when he publicly offered Edward Snowden (who had recently landed in Moscow after blowing the whistle on U.S. mass surveillance programs) a job at VK. The announcement was made via a VK post, characteristically (Boyette, 2013).

The pressure on Vkontakte and on Durov continued, with the FSB notably demanding information about users belonging to VK groups focused on the Euromaidan protest movement in Ukraine. Durov once again refused, saying: "To give the personal details of Ukrainians to the Russian authorities would not only be against the law, but also a betrayal of all those millions of people in Ukraine who trusted us. The freedom to disseminate information is an inalienable right of a postindustrial society" (The Moscow Times, 2014).

Amid these tensions, Telegram launched in August 2013. Fortuitously for Telegram, its launch was followed a few months later by the announcement that Facebook had acquired WhatsApp, Telegram's principal competitor. Concerned about Facebook's data monetization plans, many users turned to alternative messaging applications, resulting in over 8 million Telegram

downloads across the iOS and Android platforms in just a few days (Tsotsias, 2014). As we will see, one of Telegram's key value propositions is that unlike many other messaging applications it lacks any financial or institutional relationships to the U.S. government or to American technology companies.

Still abroad, Durov submitted a resignation letter in March 2014, announced he was stepping down as VK's CEO on April 1, then claimed it was all an "April Fool's joke" a few days later. Within a few weeks, the company's board announced that Durov was no longer the CEO, as the letter withdrawing his previous resignation was "not in accordance with all the rules" (The Moscow Times, 2014). The move was widely interpreted as Durov losing his stand-off with the Kremlin.

The brothers have been living in exile ever since, acquiring citizenships in St. Kitts in exchange for $250,000 donations apiece to the Caribbean island's Sugar Industry Diversification Foundation. The passports allow for unlimited visa-free travel across Europe (Walt, 2016). The company is registered as a British LLP, and uses a series of shell companies registered around the world. This structure is designed to help the company evade government requests for user information and for content restrictions (Hakim, 2014) and, more generally, to stay one step ahead of government attempts to regulate or control the company:

> Durov originally based Telegram out of a small Berlin office, but the staff now works out of a series of houses and apartments rented mostly on Airbnb.com, or out of swank hotels like the one in London; in the summer they might be found in a rented house on a lake in Finland. After a month or two at any one place, they move on. Durov describes his team as "nomads." He says Telegram is registered in several countries including the U.K.
>
> Durov explains the peripatetic lifestyle as a way of preventing the company from becoming embroiled in the politics or economic ups and downs of any single country—a lesson he says he learned from the turmoil in Russia that upturned his life and lost him his first company. "I did not want to make the same mistake of relying on a single jurisdiction," he says. "No matter how good a place looks, you don't know what crazy new regulation they will introduce" (Walt, 2016).

As of mid-2018, Telegram's 15-man team — there are no women — is based in Dubai (Telegram, 2018), though who knows how long that will last. The United Arab Emirates is far from a bastion of free expression or online privacy, and it seems likely that Telegram will eventually run afoul of local regulations or otherwise displease the authorities, particularly if the Emirati population starts using the platform for political purposes, as Telegram's large Iranian user base has done.

Indeed, Telegram is one of the most popular communication services in Iran, with roughly half of the country's population of 80 million using the platform, which plays a unique role in the country's communication ecosystem:

> Since 2009, Iranians have become experts in avoiding censorship and circumventing government controls. And Telegram, available outside Iran's "filternet" and with its high performance at low internet speeds, has become a uniquely potent and ubiquitous agent of communication and information dissemination in the cat-and-mouse game between the people and those trying to control them. It's easy to store and share large files—like videos—on the platform; it works well with Persian's [right-to-left] script; and it offers the ability to develop Persian-language bots and stickers (fun memes and images shared in chats) on top of a simple interface. Unlike Twitter, millions of Iranians use Telegram in their everyday lives—around 40 million monthly users in a country of 45 million overall online users, according to the latest ITU statistics. They often rely on Telegram's private group chats to stay in touch with friends or family; receive their news from local and diaspora Persian news sources on the platform's public channels; or subscribe to traffic, weather, shopping or entertainment updates from their neighbor-

hood (Alimardani, 2018a).

After street protests broke out in a number of cities across the country in December 2017, Iran's minister of ICT asked Telegram to censor the channel of independent news outlet AmadNews for "encouraging hateful conduct, use of Molotov cocktails, armed uprising, and social unrest." The channel was linked to the Green Movement, and its stated mission was to "expose the corruption of the regime and its clandestine activities." Hardliners within the Iranian government had been pushing for the channel's removal for several months, and were gratified when Telegram finally complied on December 30 (Alimardani, 2018a). Nonetheless, Telegram was blocked (via technical means) in Iran the very next day. The block lasted until January 13 (Alimardani, 2018b).

Iran has blocked Twitter since the 2009 Green Movement protests, with hardliners attacking the American platform as a core component of the "cultural NATO" that is waging a "Soft War" against Iran (see Alimardani & Milan, 2017; Price, 2015). Unlike Psiphon, Twitter, and many other online communication tools, Telegram lacks financial or ideological ties to the United States and its foreign policy apparatus, and had been tolerated in Iran until the recent ban. Clearly, hardliners within the Iranian government now feel threatened by Telegram as well.

3. Analysis

3.1. Telegram's Russian origins

As seen in the previous section, Telegram is the product of founders Pavel and Nikolai Durov's contentious relationship with the Russian state. This relationship is itself shaped by Russia's unique approach to information and communication policy, which long predates the Russian Federation itself. The recent history of Russian information and communication policy is thus important context for understanding Telegram (see Maréchal 2017 for a more detailed discussion of that history).

The Russian approach to information policy is rooted in the country's imperial and Soviet past (Maréchal, 2017). Under the USSR, information was considered a dangerous commodity to be feared and controlled, rather than a right and a public good. Contrary to liberal conceptions of a free press serving as a fourth branch of governance and fostering a Habermasian public sphere (Habermas, 1989), the Soviet regime saw the media as a danger to be tightly controlled, with only select elites permitted access to objective news or to foreign publications (Gorny, 2007; Soldatov & Borogan, 2015). For example, ownership and use of photocopiers were tightly restricted in an attempt to prevent the distribution of samizdat, photocopied pamphlets of "subversive" material (Hanson, 2008).[3]

The Soviet Union collapsed in 1991, and print and broadcast media were briefly liberalized during the Yeltsin era, though many were owned by —and beholden to — various oligarchs. Nonetheless, the variety of influences over the media ushered in an era of relative media freedom. Former KGB colonel Vladimir Putin took office in late 1999, and promptly reasserted the Kremlin's control over the media under the auspices of "liberating" the press from the oligarchs. For many Russia experts, understanding Putin is key to understanding Russia today. Putin served in the Soviet intelligence agency, the KGB, for 16 years, rising to the rank of colonel, and he spent much of the pivotal perestroika years outside of Russia. His views on governance, the rule of law, the role of information in society, and the Russian national interest are very much influenced by the KGB's authoritarian traditions, themselves grounded in the authoritarianism of imperial Russia (Soldatov & Borogan, 2015).

The end of the Cold War and collapse of the USSR, which also marked the end of Russia's superpower status, was a sore spot for the Russian elite, who perceived the U.S.'s success in exporting its cultural products as a threat to national sovereignty. Elites also resented growing U.S. influence in Eastern Europe and Central Asia, which they saw as Moscow's rightful sphere of influence, as well as the European Union's eastward expansion into the former Eastern Bloc. Over the course of his first presidency (2000–2008), during which time domestic internet access grew considerably, Putin came to see the information revolution as "one of the most pervasive components of U.S. expansionism in the post-Soviet sphere, most notably in Russia itself" (No-

[3] See Peters, 2016 on the history of computing and cybernetics in the Soviet Union

cetti, 2015, p. 129). Where others might have seen opportunities for innovation and growth, Putin saw threats to the status quo and his hold on power, thus following in the footsteps of his Soviet and pre-bolshevik predecessors alike. However, Russia's political classes did not understand the internet well enough to regulate it, and the RuNet flourished outside of government control for the first decade of the Putin era.

Putin switched posts with his prime minister, Dmitry Medvedev, in 2008 to circumvent constitutional term limits. A series of "color revolutions" and the Arab Spring solidified Putin's understanding of the internet as a threat to political order and national sovereignty. He notably saw the mass protests of 2011-2012 as a component of American "information aggression" orchestrated from Washington, specifically by then-Secretary of State Hillary Clinton (Nocetti, 2015).

Russian internet policy—in both the domestic and foreign policy spheres—is rooted in the premise that Western countries (mainly the U.S.) use the internet to overthrow governments in "countries where the opposition is too weak to mobilize protests" (Nocetti, 2015, p. 114)— or, in other words, countries living under authoritarian regimes. Russian foreign policy hews to a strict interpretation of Westphalian nation-state sovereignty, at the core of which is the principle of non-intervention. The free and open internet threatens that principle, allowing foreign and potentially subversive viewpoints to circulate across Russia. The "color revolutions" of the early 21st century and the Arab Spring have further fueled concerns that the internet represents a threat to the status quo and that it poses a threat to Russian political leaders (Howard & Hussain, 2013; Nocetti, 2015). Indeed, opposition groups led by Alexei Navalny used Facebook to coordinate street protests in the aftermath of the 2011 legislative elections, and while the protests failed to coalesce into a lasting social movement, such an outcome was not completely outside the realm of possibility (Soldatov & Borogan, 2015; White & McAllister, 2014). Moreover, there is good reason to believe that Putin sees the U.S., and specifically then-Secretary of State Hillary Clinton, as directly responsible for fomenting these protests. Under this paradigm, such interference in Russia's domestic politics constitutes a violation of national sovereignty tantamount to information warfare. Likewise, U.S. policy initiatives like democracy promotion and the Internet Freedom agenda are seen as promoting political projects that are aligned with U.S. interests, almost invariably at the expense of Russia's own interests (Nocetti, 2015).

Putin won the 2012 presidential election in spite of the protests, and intensified his efforts to control the internet. It soon became clear that the traditional mechanisms for information control — censorship and intimidation of key individuals, resulting in chilling effects — were inadequate in the social media era (Maréchal, 2017; Ognyanova, 2015; Soldatov & Borogan, 2015). Intimidation and financial pressure had successfully wrestled control of Vkontakte from libertarian Pavel Durov and replaced him with management that was

more willing to cooperate with the FSB's demands, but foreign platforms like Twitter and Facebook remained outside the security services' reach.

> But Facebook and Twitter don't store their user data in Russia, keeping it out of SORM's reach (Soldatov and Borogan, 2013, para. 20).

The 2012 reform of the SORM[4] surveillance system, first launched in 1995 to monitor telephone and internet communications, brought social networking sites under the mass surveillance system's purview, which already required internet service providers to deploy Deep Packet Inspection (DPI) technology[5] to monitor all communications originating or terminating in Russia (Soldatov & Borogan, 2015). As Soldatov and Borogan note, the tools used to monitor social networking sites at the time had a crucial flaw:

> These systems were developed for searching structured computer files, or databases, and only afterwards adapted, some more successfully than others, for semantic analysis of the Internet. Most of these systems were designed to work with open sources and are incapable of monitoring closed accounts such as Facebook.
>
> The FSB discovered early on that the only way to deal with the problem was to turn to SORM. The licenses require businesses that rent out site space on servers to give the security services access to these servers via SORM, without informing the site owners. With this provision, the FSB has had few problems monitoring closed groups and accounts on Russian social networks Vkontakte and Odnoklassniki.

This desire to gain access to Russian users' online activities was the key motivation for data localization laws promulgated in the aftermath of the Snowden revelations. While the laws' proponents claimed to be motivated by a desire to protect Russians' personal data from the U.S. National Security Agency (NSA), these requirements do nothing to impede NSA spying while facilitating the SORM system's access (Maréchal, 2017; Sargsyan, 2016). Russian media regulator Roskomnadzor began enforcing data localization requirements for foreign companies in 2017, and foreign companies face with the possibility of being blocked in Russia if they don't comply. LinkedIn (owned by Microsoft) became the first foreign site to be banned for failing to comply with the data localization requirement in October 2016 (Rothrock, 2016).

In 2016, Russia passed a draconian legislative package, known as the Yarovaya Laws after one of its sponsors, that further restricts privacy and freedom of expression both offline and online. Among other things, the laws require "information dissemination services" to register with the state media regulator, to store all message content for six months and metadata for three years, and to preemptively make decryption keys available to the authorities (International Center for Not-for-Profit Law,

---

[4] System of Operational-Investigatory Measures

[5] As Laura DeNardis puts it, "DPI is a transformational technology that creates unprecedented regulatory possibilities for controlling the flow of content online" (2014, p. 206). Demonstrating why this is the case requires a basic understanding of the technology itself. Information (whether it's text, voice, or something else) is transmitted over the internet as packets, small bundles of data that are individually routed from the sender to the receiver, then put back together in the correct order. Packets consist of both payload (the actual content of the communication) and a header, which contains the packet's metadata: its origin, destination, and not much else. The header is analogous to an envelope, telling each piece of equipment along the way where the payload should be delivered. Until fairly recently, computing power limited the types of analyses that routers, switches and other network hardware could perform on passing traffic, but advances in this domain have made it possible for hardware to simultaneously process millions of packets, reading not just the headers but the payload as well. Unless the packet is encrypted, the only impediment to stopping a DPI-capable machine from reading the payload are social and legal norms against this type of surveillance—which are absent in Russia. From there it is possible to block or throttle back traffic based on its origin, destination, file type (text, voice, multimedia), protocol (P2P, FTP, HTML, SMTP) or the content of the message itself (DeNardis, 2014).

2016).[6] Telegram complied with the registration requirement, but refused to share decryption keys, for which it was fined 800,000 rubles (roughly $14,000 USD). The company lost its appeal in March 2018, and on April 6 the media regulator filed suit against Telegram in an effort to ban the platform in Russia (Krishna 2017a, 2017b, 2018a, 2018b). On April 13, after an 18 minute hearing, the court ordered Russian ISPs to start blocking Telegram, though the RuNet was abuzz with instructions for circumventing the ban within hours (Stubbs & Ostroukh, 2018).

This court battle is but one example of how internet technologies challenge traditional conceptions of sovereignty: countries can block services or content, but enforcing these blocks is technically complex and very expensive. The case also illustrates two important things about the company and its co-founders. The Durovs' lawyers advanced two lines of argumentation: first, that the requirement to share decryption keys was unconstitutional, and second, that Telegram was unable to comply with the requirement because it did not itself possess the decryption keys: the end-to-end encrypted Secret Chats (which users must actively select, in contrast to other messaging apps which encrypted all communication by default) use keys that Telegram cannot access, and the keys used to secure "normal" chats and public channels while in transit are stored in a distributed fashion across multiple legal jurisdictions (Telegram, n.d.). As we will see in the next section, these are deliberate design choices that reflect Pavel Durov's libertarian political ideology.

3.2. Telegram's ideology

This section delves further into Telegram's ideological underpinnings to draw connections between this ideology and Telegram's design choices, policy decisions, and how people use the platform to political ends. I argue that Telegram is a cyber-libertarian project in the cypherpunk tradition that is untempered by regulation, corporate governance, or accountability to any higher authority than Pavel Durov himself. This appears to be an intentional feature, not a bug, albeit one that should give users pause.

Cyber-libertarianism is "the belief that individuals—acting in whatever capacity they choose (as citizens, consumers, companies, or collectives)—should be at liberty to pursue their own tastes and interests online," with the goal "to minimize the scope of state coercion in solving social and economic problems and looks instead to voluntary solutions and mutual consent-based arrangements" (Thierer & Szoka, 2009, para. 1-2). David Golumbia, an outspoken critic of cyber-libertarianism, summarizes the ideology as "computerization will set you free," and identifies a number of corollaries to this central tenet, including: "a resistance to criticism of the incorporation of computer technology into any sphere of human life; a pursuit of solutions to perceived problems that takes technical methods to be prior to analytic determination of the problems themselves; a privileging of quantificational methods over and above, and sometimes to the exclusion of, qualitative ones; the use of special standards for evaluating computational practices that differ from those used in evaluating non-computational ones; and an overarching focus on the power of the individual and individual freedom, even when that individual is understood to be embedded in a variety of networks" (2013, p. 1).

As we saw in the Project History section of this case study, Telegram originated as a way for the Durov brothers to communicate securely while they (and Vkontakte) were engaged in a high-stakes standoff with Russian authorities in late 2011. The platform launched in mid-2013, and became the Durovs' sole focus within a year, as Pavel was ousted from VK the following spring.

Media portrayals of Pavel Durov have described his political leanings as "the sort of techno-utopian, libertarian ideas popular in Silicon Valley" (Yaffa, 2013). Indeed, the White Paper issued in advance of the Telegram ICO is clear about Telegram's ideological underpinnings: "Telegram was founded in 2013 by libertarians to preserve freedom through encryption" (Telegram, 2018, p. 5). The idea of "freedom through encryption" is, of course, the basic tenet of the cypherpunk ideology. Grounded in the writings of David Chaum (1985), Tim May (1995), J. P. Barlow (1996), and Eric Hughes (1997), among others, the

[6] The requirement to store message content came into effect on July 1, 2018. Other requirements were already in force.

cypherpunk movement is materially and discursively sustained through the Cypherpunk Mailing List and technologically embodied in computer programs like Pretty Good Privacy, anonymous remailers, and cryptocurrencies. The cypherpunks envisioned a world where computer code — specifically encryption — would help end the nation-state's dominion over individual lives and bring about a libertarian utopia predicated on individual autonomy and free association (Levy, 2001; West, 2018).

Pavel Durov has long been vocal in his rejection of the nation-state as a legitimate source of authority. He says that he considers himself "a legal citizen of the world," and has take a number of steps to sidestep national regulation, including his purchase of citizenship in St. Kitts and Nevis. At the same time, he seems to have some degree of national pride: "My dream is to break the national inferiority complex, proving that products from Russia can be massively claimed all over the world" (Kononov & Igumenov, 2011).

In 2012, Durov "published a manifesto in the magazine *Afisha* that called on Russia to "rid society of the burden of obsolete laws, licenses, and restrictions … the best legislative initiative is absence." (Durov, 2012, cited in Yaffa, 2013). Durov's biographer Nikolai Kononov describes the VK founder's impression of Mark Zuckerberg, after the two met in San Francisco:

> Durov asked Zuckerberg: "What do you think about Twitter?" Zuckerberg did not discuss Twitter and started talking about social networks. The libertarian Durov felt in him a revolutionary brother. "We had more in common than [I did] with the business characters [within Facebook]," he said after. "Mark is an anarchist, but not in terms of denying power and order, but in terms of understanding the outdated nature of the state." The architects agreed that social networks are a superstructure over humanity, allowing information to spread past the centralizing horns of the state (Kononov, 2013, cited in Forbes Staff, 2012).

Durov and Zuckerberg both seem to view the nation-state as an obsolete legacy of a bygone era, soon to be replaced as the main organizing logic for human societies by technological platforms like their own creations (incidentally, placing vast amounts of wealth and power into their own hands). But the two men are the products of very different circumstances, and their careers — as well as the platforms they each spawned — would be shaped by dramatically different social, political, and economic contexts. While Pavel Durov chiefly turns to his brother Nikolai for advice, Zuckerberg has long been surrounded by venture capitalists, lawyers, business school graduates, and other products of late American capitalism who molded Facebook into the (largely) law-abiding surveillance capitalism behemoth it is today (see Vaidhyanathan, 2018).

In contrast, Durov has sought to keep his companies out of reach of both the law and the market. Under his leadership, Vkontakte resisted enforcing copyright laws, and for a time hosted over half of the copyrighted audio and video content on the RuNet. He only agreed to remove copyrighted content — upon request from the rights holder — after pressure from VK's shareholders, who were concerned that enabling copyright violations at scale would stand in the way of an IPO on Western stock exchanges (Kononov & Igumenov, 2011). As for Telegram, both the company's legal structure and its technical architecture deliberately span multiple jurisdictions as a way to avoid being subjected to any one government's authority (or so Telegram's public documentation claims).

Durov rejects not only the nation-state, but also surveillance capitalism, the business model based on targeted advertising that sustains companies like Google, Facebook, and a growing cross-section of firms in other sectors (Zuboff, 2015). This is an important contrast to Mark Zuckerberg, who infamously declared that "privacy is dead" and has vociferously (and incorrectly) denied any causal relationship between his company's business model and the current misinformation crisis (Vaidhyanathan, 2018). He resisted an advertising-based business model for VK as long as possible, finally relenting in 2008 (Kononov & Igumenov, 2011), and Telegram pledges never to seek advertising revenue, charge user fees, or sell traditional shares in the company (Telegram, n.d.). Telegram presents this choice in a positive light, arguing that users should trust the platform because Durov is accountable only to his own ideals, rather than to shareholders' hunger for dividends or advertisers' voracious appetite for user data. While

this implicit critique of capitalism resonates with many audiences, Telegram's value proposition requires complete faith in the Brothers Durov, their good intentions, and their technical capacity to deliver on their promises.

The online FAQ defines privacy in opposition to the Silicon Valley business model, offering an ironclad commitment to privacy, albeit one for which it provides scant evidence, much less an accountability mechanism:

> **Q: What are your thoughts on internet privacy?**
>
> Big internet companies like Facebook or Google have effectively hijacked the privacy discourse in the recent years. Their marketers managed to convince the public that the most important things about privacy are superficial tools that allow hiding your public posts or your profile pictures from the people around you. Adding these superficial tools enables companies to calm down the public and change nothing in how they are turning over private data to marketers and other third parties.
>
> At Telegram we think that the two most important components of Internet privacy should be instead:
>
> 1. Protecting your private conversations from snooping third parties, such as officials, employers, etc.
>
> 2. Protecting your personal data from third parties, such as marketers, advertisers, etc.
>
> This is what everybody should care about, and these are some of our top priorities. Telegram's aim is to create a truly free messenger, without the usual caveats. This means that instead of diverting public attention with low-impact settings, we can afford to focus on the real privacy issues that exist in the modern world (Telegram, n.d.).

While Telegram is right to point out that Silicon Valley corporations rhetorically redefine privacy as being about other users as a way to avoid discussing their surveillance-based business model, the company fails to prove that it lives up to its own commitments.

For now, Telegram is not completely free from national regulation, though it has taken a number of steps to distance itself from governmental attempts to assert power. Though it claims to operate as a non-profit, Telegram is structured as a for-profit British LLP that is itself owned by a complex series of shell companies registered in various tax havens. Its decentralized technical architecture is likewise designed to store user data and encryption keys across several jurisdictions,[7] thus thwarting government requests for user information:

> **Q: Do you process data requests?**
>
> Secret chats use end-to-end encryption, thanks to which we don't have any data to disclose.
>
> To protect the data that is not covered by end-to-end encryption, Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions are required to force us to give up any data.
>
> Thanks to this structure, we can ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world.

[7] This architecture emulates earlier projects like MojoNation and BitTorrent — see Beyer & McKelvey, 2015.

> To this day, we have disclosed 0 bytes of user data to third parties, including governments (Telegram, n.d.).

Telegram thus rejects all government oversight, even when constrained by the rule of law and judicial review. This position goes well beyond the demands of most digital rights campaigners, who argue that intermediaries should only turn over user information pursuant to a court order or equivalent legal process, and that companies should publish figures on requests for user data and on their own compliance with such requests, thus holding both companies and governments accountable to a web of civil society organizations (MacKinnon, Maréchal & Kumar, 2016).

Public channels can be accessed by anyone with a Telegram account, so the concern here relates to private conversations between users. Telegram supports end-to-end encryption in its Secret Chats, but this isn't enabled by default, a choice for which Telegram is criticized by many privacy advocates. One privacy and encryption expert I interviewed told me that he believes this is a political choice designed to placate governments concerned about terrorists and criminals using the platform to coordinate their activities.[8] Indeed, Telegram has been widely criticized for supposedly being the "terrorists' app of choice," following disputed media reports that Telegram had been used to plan attacks in Paris, Nice, London, and elsewhere. Telegram stresses that it has never turned over user information (including chat logs) to any government, but enabling end-to-end encryption by default would further protect users' communications content from state surveillance. Pavel Durov disputed the notion that Telegram bore any responsibility for the attacks in a virulently xenophobic statement imbued with a classically libertarian rejection of taxation:

> The French government is as responsible as the Islamic State for this because it is their policies and carelessness that eventually led to the tragedy. They take money away from hardworking people of France with outrageously high taxes and spend them on waging useless wars in the Middle East and on creating a parasitic social paradise for North African immigrants (Quénelle, 2016).

Similarly, the company rejects any responsibility to moderate user content, with the exception of narrowly defined "public content" and content related to terrorism, notably ISIS. Telegram deleted 78 different ISIS-related channels shortly after the November 2015 Paris attack, and continues to monitor such content closely and periodically shuts down channels related to terrorism. It seems to do so proactively, however, rather than in response to government requests, despite not having a Terms of Service Agreement of community standards codifying user content. This paragraph from the Telegram website's FAQ page is all the platform communicates to users about content removals:

> **Q: Wait! 0_o Do you process take-down requests from third parties?**
>
> Our mission is to provide a secure means of communication that works everywhere on the planet. To do this in the places where it is most needed (and to continue distributing Telegram through the App Store and Google Play), we have to process legitimate requests to take down illegal **public** content (e.g., sticker sets, bots, and channels) within the app. For example, we can take down sticker sets that violate intellectual property rights or porn bots.
>
> User-uploaded stickers sets, channels, and bots by third-party developers are not part of the core Telegram UI. Whenever we receive a complaint at abuse@telegram.org or dmca@telegram.org regarding the legality of public content, we perform the necessary legal checks and take it down when deemed appropriate.
>
> Please note that this does **not** apply to local restrictions on freedom of speech. For example, if criticizing the government is illegal in some country, Telegram won't be a part of such politically motivated censorship. This

[8] Phone interview, March 31, 2018.

> goes against our founders' principles. While we do block terrorist (e.g. ISIS-related) bots and channels, we will not block anybody who peacefully expresses alternative opinions (Telegram, n.d.).

Unlike other platforms like Facebook, Twitter, and even Vkontakte, Telegram does not provide any further details about the types of content (beyond copyrighted materials subject to the Digital Millennium Copyright Act, or DMCA) it might remove nor the process for evaluating such requests. Nor does it publish so-called "transparency reports," which list the number of government requests for content removal that a platform has received, complied with, or both. This practice was pioneered by Google in 2010, and has since become standard practice in the technology sector, though civil society continues to push companies for more transparency about how their policies and practice impact users' rights to privacy and freedom of expression. Telegram's opacity in this regard is one of the critiques leveled against the company by digital rights advocates.

As my co-authors and I have argued elsewhere (MacKinnon, Maréchal & Kumar, 2016), this transparency serves to create mechanisms by which companies, governments, and civil society groups hold one another accountable for meeting their respective commitments to respect and protect human rights in the digital age, thus bridging a critical governance gap in global society. Telegram simultaneously rejects such a compact even as it falls short of the open source standards that form the cornerstone of the cypherpunk ideal. Pavel Durov would have Telegram's users trust Telegram without subjecting the company's code or business operations to any outside scrutiny.

Finally, Pavel Durov's paradigmatic view of the world seems to combine cyber-libertarianism with an idiosyncratically Russian understanding of politics. In an interview with Yasha Levine, an outspoken critic of the Internet Freedom agenda and the digital rights movement, Durov said that "he could not understand how people could trust a supposedly anti-government weapon that was being funded by the very same U.S. government it was supposed to protect its users from" (Levine, 2017). Levine drew an analogy to the Soviet era:

> Imagine if the KGB funded a special crypto fax line and told Aleksandr Solzhenitsyn and dissident samizdat writers to use it, promising that it was totally shielded from KGB operatives. Then imagine that Solzhenitsyn would not only believe the KGB, but would tell all his dissident buddies to use it: "It's totally safe." The KGB's efforts would be mercilessly ridiculed in the capitalist West, while Solzhenitsyn would be branded a collaborator at worst, or a stooge at best (Levine, 2017).

Durov agreed with the assessment: "I don't think it's a coincidence that we both understand how naïve this kind of thinking is, and that we were both born in the Soviet Union" (Levine, 2017).

The problem with Levine's analogy is that it assumes that governance works the same way in 21st century America as it did in the Soviet Union. It is impossible to prove a negative, of course, and I can't categorically rule out the NSA making a pact with Moxie Marlinspike to "backdoor" the Signal Protocol, for example, but it seems highly unlikely, especially since Signal's codebase is entirely open-source and is regularly scrutinized by the world's top cryptographers.[9] Durov's (and Levine's) apparent belief that the U.S. government is a unitary actor whose actions are internally consistent and coordinated at a high level is consistent with an idiosyncratically Russian understanding of politics rooted in the country's Soviet heritage. As Andrei Soldatov and Irina Borogan write in *The Red Web*,

> [The KGB] were trained to think that every person was only driven by baser, inferior motives. When confronting Soviet dissidents, they looked for money, dirty family secrets, or madness, as they couldn't accept for a second that someone could challenge the political system simply because they believe in their cause.

[9] Field notes, 2015-2018.

> Putin is a product of this thinking. He doesn't believe in mankind, nor does he believe in a benign society — the concept that people could voluntarily come together to do something for the common good. Those who tried to do something not directed by the government were either spies — paid agents of foreign hostile forces — or corrupt — i.e. paid agents of corporations (Soldatov & Borogan, 2017, p. 336).

This seems to be the lens through which Durov and Levine view the relationship between the Internet Freedom agenda and the digital rights movement: it is nearly unthinkable to them that civil society actors would develop digital rights tools without being directed to do so. According to this logic, the financial relationship between these actors and government institutions implementing the Internet Freedom agenda proves this causal link. (Though out of scope for this conference paper, the relationship between the U.S.-led Internet Freedom agenda and the grassroots transnational social movement for digital rights is a central concern of the larger study from which the present paper is excerpted.)

3.3. Crypto controversies

While media coverage of Telegram makes much of its encrypted Secret Chats, linking the affordance to terrorism, criminality, and the like, cryptography experts have cast doubts on the robustness of the Durovs' MProto encryption protocol, dubbed MProto. Though a technical evaluation of the protocol's shortcomings would fall beyond the scope of this paper (and of the author's expertise), it is important to underscore that Telegram's claims to unbreakable encryption have come under serious attack from respected experts.

The core of the critique of MProto is that rather than building on established encryption protocols and collaborating with experienced experts, the Durovs "rolled their own crypto," thus breaking the "cardinal rule of cryptography" (Clary, 2016; Cox, 2015). As Runa Sandvik, Director of Information Security at the New York Times and former Tor developer, told Motherboard,

> Asking why you should not roll your own crypto is a bit like asking why you should not design your own aircraft engine. The answer, in both cases, is that well-studied and secure options exist. Crypto is hard and I would rather rely on encryption schemes that have been studied and debated than schemes that are either secret or have yet to receive much, if any, attention (Cox, 2015).

Additionally, Telegram has failed to provide the necessary documentation for independent cryptographic evaluations. The code for the application itself (i.e. the app that users install on their ow machines) is open source, but the documentation is reportedly incomplete (see Couprie, 2013). Moreover, code for the server-side software is not available, with Telegram's FAQ merely stating that "all code will be released eventually" (Telegram, n.d.). Evaluations of the portions of Telegram's code that are publicly available have uncovered a number of serious flaws, notably leaving the platform's users vulnerable to man-in-the-middle (MITM) attacks (Jakobsen, 2015). Until Telegram makes all its code available to outside review, security-conscious users would do well to exercise caution.

3.4. Telegram's libertarian business model

Durov's commitment to keeping Telegram free to use, aversion to lose control of the company to outside investors (as he did with VK) rule out the revenue streams that sustain many tech start-ups. Moreover, his hostility to state sovereignty in general and to U.S. foreign policy specifically preclude the types of grants and products that sustain the other projects analyzed in my larger study (Psiphon, Tor, and Signal), leaving very few avenues for revenue generation. This context explains Telegram's embrace of the cryptocurrency craze. The 2018 Initial Coin Offering (ICO) promised not only a much-needed influx of no-strings-attached cash, but also a cypherpunk, cyber-libertarian future where Telegram controls its own technical infrastructure, keeps nation-states at arms' length, and even issues its own currency. Given Pavel Durov's professed libertarianism, it is perhaps unsurprising that Telegram is turning to cryptocurrency to secure its financial future. Indeed, as early as 2012, Durov called the idea of national currency "anachronistic" (Durov, 2012, cited in Yaffa, 2013).

For the nearly five years of its existence, Telegram

seems to have been solely financed by Pavel Durov, who made a reported $300 million from the forced sale of his shares in Vkontakte. The company, which is legally structured as a British LLP, is privately held and maintains "a deliberately complex structure of scattered global shell companies intended to keep it a step ahead of subpoenas from any one government" (Hakim, 2014). There are no financial statements (audited or not) available publicly, and Pavel Durov's public statements are the sole source of information about Telegram's finances.

If Durov is to be believed, Telegram is not a commercial venture designed to earn its creators money but an ideological one. A recent blog post explained:

> This is why you – our users – have been and will always be our only priority. Unlike other popular apps, Telegram doesn't have shareholders or advertisers to report to. We don't do deals with marketers, data miners or government agencies. Since the day we launched in August 2013 we haven't disclosed a **single byte** of our users' private data to third parties.
>
> We operate this way because we don't regard Telegram as an organization or an app. For us, Telegram is an **idea**; it is the idea that **everyone on this planet has a right to be free**.
>
> Above all, we at Telegram believe in **people**. We believe that humans are inherently intelligent and benevolent beings that deserve to be trusted; trusted with freedom to share their thoughts, freedom to communicate privately, freedom to create tools. This philosophy defines everything we do (Durov, 2018; emphasis in the original).

Durov has alleged that he has turned down offers of financial backing from some of "the most famous" venture capital firms in Silicon Valley. Instead, he prefers to fund Telegram himself, spending a reported $1 million a month on salaries, infrastructure costs, and other expenses (Walt, 2016). However, this is not sustainable indefinitely.

The FAQ page has long left open the possibility that Telegram might "introduce non-essential paid options to support the infrastructure and finance developer salaries," stressing that "making profits will never be an end-goal for Telegram" (Durov, 2018). In 2016, he told Fortune's Vivienne Walt that "We still have a few years," he says. "But it would be responsible for us to come up with a business model within a year or two from now" (Walt, 2016).

Telegram seems to have found its business model in the hype surrounding blockchains and cryptocurrencies. A blockchain is a distributed ledger system whose entries are cryptographically verified, thus protecting the entries from later tampering. Rather than residing in a centralized database, the information stored on the blockchain is distributed among a large number of machines that verify each other's work. The blockchain is the core technology behind Bitcoin, Ethereum, and other cryptocurrencies, which facilitate anonymous monetary transactions over the internet. There has also been intense interest in other potential applications over the past few years, such as digital identity schemes and so-called "smart contracts." In 2016, creators of new cryptocurrencies began raising startup funds thoughts Initial Coin Offerings (ICOs), which are similar to Initial Public Offerings (IPOs), with a key difference: rather than company shares and a promise of future dividends, investors receive tokens, or units of the future currency, that they are often prohibited from selling for a predetermined period of time under the terms of the ICO. If the cryptocurrency takes off, investors will eventually be able to use their tokens for purchases. If it doesn't, the value of the investment is lost.

Amid a growing frenzy of ICOs, the U.S. Securities and Exchange Commission (SEC) released an Investor Bulletin cautioning potential investors that "new technologies and financial products, such as those associated with ICOs, can be used improperly to entice investors with the promise of high returns in a new investment space" (U.S. Securities & Exchange Commission, 2017). The Investor Bulletin emphasized that many tokens offered as part of ICOs were securities subject to federal securities laws. Notably, ICOs may be restricted to "accredited investors" who can demonstrate either $200,000 in annual income or a net worth of at least $1 million (U.S. Securities & Exchange Commission, 2017).

In January 2018, the specialized blockchain/cryptocurrency press started buzzing with news concerning a "Telegram ICO." The public ICO, planned for March 2018, would be preceded by a "pre-sale" limited to accredited investors willing to invest large sums of money, with a floor as high as $20 million. Investors would receive tokens called "Grams," which would eventually be the unit of exchange for Telegram's native cryptocurrency economy. The public ICO in March would be open to anyone (Constine, 2018). The pre-sale raised a record $850 million from 81 different investors, and was followed in February by a second "secretive" pre-sale, which also raised $850 million, from 94 different investors (Jeffries, 2018; Moore, 2018). Having thus raised $1.7 billion in pre-sales, Telegram cancelled the public ICO, possibly as a way to evade Securities and Exchange Commission (SEC) requirements (Liao, 2018).

The funds raised are intended to finance the development of the new Telegram Open Network (TON), described in a leaked Technical White Paper authored by Nikolai Durov:

> The Telegram Open Network (TON) is a fast, secure and scalable blockchain and network project, capable of handling millions of transactions per second if necessary, and both user-friendly and service provider-friendly. We aim for it to be able to host all reasonable applications currently proposed and conceived. One might think about TON as a huge distributed supercomputer, or rather a huge "superserver", intended to host and provide a variety of services (Durov, 2017, p. 1).

The 132-page document provides a complex technical explanation of TON, heralding its potential as "a truly scalable general-purpose blockchain project, capable of accommodating essentially any applications that can be implemented in a blockchain at all," (Durov, 2017, p. 78). Attempting to evaluate TON on its technical merits would be well beyond the scope of this project; however, some experts are skeptical. Cryptographer Matt Green, who teaches at Johns Hopkins University, told The Verge: "So to their credit, Telegram has shown that it can execute and get software written. That's actually a big deal when it comes to blockchain projects. That plus millions of dollars means they could pull something off. But I'll be honest, the white paper reads like someone went out on the internet and harvested the most ambitious ideas from a dozen projects and said 'let's do all of those but better!' It feels unachievable, at least at the scale they're aiming for now" (Jeffries, 2018). Indeed, the White Paper "promises an Ethereum-like ecosystem with apps, services, and a store for digital and physical goods," as well as "a suite of blockchain-based products including file storage, a DNS service, and an ad exchange" (Jeffries, 2018). But it isn't clear that this ambitious scheme will actually come to fruition, and some suspect that the ICO is primarily a mechanism to generate cash flow for Telegram:

> Others have speculated that Durov is not really raising money for a new blockchain-centric venture, but simply to keep Telegram afloat. Durov was reportedly self-funding the company with his earnings from selling VK.com, the Russian Facebook clone that he founded. "With growing user base, he would've eventually run out of money. Therefore he opted for an ICO as a mechanism to raise funds without getting outside investors into Telegram's shareholder capital," Gregory Klumov, CEO of the government blockchain company Stasis, told *Bloomberg* (Jeffries, 2018).
>
> Some in the crypto community remain skeptical of TON. "I just think this is the CEO's way of monetizing Telegram, basically," says Jackson Palmer, the founder of early cryptocurrency Dogecoin (Constine, 2018).
>
> "It really felt like it was one of these start-ups that's burning through cash and needs a way to bring money in to keep funding their operations," said [Digital Currency Group's Travis] Scher. "This is how they decided they're going to do it" (Levy, 2018).

Indeed, the SEC Form D ("Notice of Exempt Offerings of Securities") lists the intended "Use of Proceeds" as "the development of the TON Blockchain, the devel-

opment and maintenance of Telegram Messenger and the other purposes described in the offering materials" (Palmer, 2018; SEC Form D submitted by TON Issuer Inc., 2018), and there doesn't appear to be an "alpha" version of the TON platform yet (Dale, 2018).

Telegram has ambitious plans for the next 18 months: launching the "Telegram External Secure ID," the "Minimal Viable Testing Network of TON," and Telegram Wallet by the end of 2018, and creating a "TON-based economy in Telegram" as well as launching "TON Services, TON Storage, and TON Proxy" in the first half of 2019 (Telegram, 2018, p. 15). Whether these plans are realistic remains to be seen, but what seems clear is that the ICO pre-sale has generated enough income to sustain Telegram's existing activities for the foreseeable future. Whether Telegram's "investors" will actually receive any Gram tokens is an open question.

4. Conclusion

Telegram is unique among major digital rights technology projects: its founders hail from outside of North America, it lacks any institutional or financial connection to the U.S. Internet Freedom agenda, and its opaque business model places complete control of the project in the hands of its founders. Moreover, its ideological commitment to "freedom" is rooted in libertarian principles rather than a commitment to human rights. This is significant because Pavel Durov's brand of cyber-libertarianism recognizes no higher authority than himself: he defers to neither the laws of nation-states nor international human rights standards. Moreover, while Telegram claims to be open source it fails to provide enough information (i.e. code) to allow others to verify the company's claims, and cryptography experts have expressed serious reservations about the security of its Secret Chats in particular.

Yet Telegram meets the definition of "digital rights technology" that I presented at the beginning of this paper: hardware and software tools that allow individuals to better protect their privacy, access the information they wish to access notwithstanding censorship attempts by nation-states or other actors, express themselves as they wish in both the public sphere and in private, or any combination of the above. Telegram was explicitly created to help Pavel and Nikolai Durov avoid Russian state surveillance, and company documentation frequently references Telegram's non-commercial mission and commitment to libertarianism. In Russia, Iran, and elsewhere, Telegram's public Channels are used to disseminate news and political content that would be censored in the traditional media, and Secret Chats (supposedly protected by "unbreakable" encryption) provides a space for mass mobilization. Aßcute political and legal battles over Telegram are a testament to the growing role that the platform plays in the political life of many societies.

Its mission of providing freedom through encryption places Telegram in the cypherpunk tradition, even though patchy disclosure of source code is at odds with that tradition. Like the original cypherpunks, Durov's discourse sees the relationship between the state and its citizens as inevitably authoritarian and oppressive, leaving no room for the idea of democratic, rights-respecting governments constrained by the consent of the governed. Nor does it recognize civil society as an independent political actor, declining to engage in transparency reporting (and therefore be held accountable by globally networked non-profit watchdogs) and casting aspersions on other digital rights projects based on their funding models. In my view, Telegram's ideology precludes the possibility of political projects designed for the broader good of society. Durov seems resigned to a vision of politics and policy-making as a zero-sum game with winners and losers, and it appears that after losing his battle against the Kremlin for control of VKontakte, he is now determined to remain firmly in control of his newest venture and, just as importantly, beyond the reach of the state. This is certainly understandable, from his perspective, but is unlikely to do much for global human rights, peace, or prosperity. Like many other tech pioneers, Durov seems woefully uneducated about political philosophy, social theory, and the finer points of policymaking, and his concerted efforts to place himself beyond all accountability should be cause for concern.

References

Alimardani, M. (2018a, January 1). What Telegram owes Iranians. *Politico*. Retrieved from https://www.politico.com/magazine/story/2018/01/01/irans-telegram-revolution-216206

Alimardani, M. (2018b, March 8). Evidence says Iran throttled Telegram connections after January protests. Retrieved April 5, 2018, from https://advox.globalvoices.org/2018/03/08/evidence-says-iran-throttled-telegram-connections-after-january-protests/

Barlow, J. P. (1996, February 8). A declaration of the independence of cyberspace. Retrieved from https://www.eff.org/cyberspace-independence

Beyer, J., & McKelvey, F. (2015). Piracy & Social Change! You Are Not Welcome Among Us: Pirates and the State. *International Journal Of Communication, 9*, 19. Retrieved from http://ijoc.org/index.php/ijoc/article/view/3759/1340

Boyette, C. (2013, August 5). Russia's Mark Zuckerberg offers Edward Snowden a job. *CNN Tech*. Retrieved from http://money.cnn.com/2013/08/05/technology/social/snowden-vkontakte/

Chaum, D. (1985). Security without identification: Transaction systems to make Big Brother Obsolete. *Communications of the ACM*, *28*(10), 1030–1044.

Clary, G. (2016, January 4). The flaw in ISIS' favorite messaging app. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2016/01/isiss-favorite-messaging-app-has-a-security-problem/422460/

Constine, J. (2018, January 8). Telegram plans multi-billion dollar ICO for chat cryptocurrency. *Tech Crunch*. Retrieved from https://techcrunch.com/2018/01/08/telegram-open-network/

Couprie, G. (2013, December 17). Telegram, AKA "Stand back, we have Math PhDs!" Retrieved July 12, 2018, from http://unhandledexpression.com/2013/12/17/telegram-stand-back-we-know-maths/

Cox, J. (2015, December 10). Why you don't roll your own crypto. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/wnx8nq/why-you-dont-roll-your-own-crypto

Dale, B. (2018, January 16). Big money, murky governance: Kicking the tires of Telegram's token sale. *Coindesk*. Retrieved from https://www.coindesk.com/big-money-murky-governance-kicking-tires-telegrams-token-sale/

DeNardis, L. (2015). *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Dredge, S. (2014, April 3). Major labels sue Russian social network vKontakte for "large-scale" music piracy. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2014/apr/03/major-labels-vkontakte-russia-music-piracy

Durov, N. (2017, December 3). Telegram Open Network. Telegram. Retrieved from https://drive.google.com/file/d/1lqVlrgiztnA5dkOHP7-ENDKT1FgZuCUV/view

Durov, P. (2012, May 18). Музыканты, писатели, журналисты, поэты и другие жители страны о том, что делать: Павел Дуров, основатель «ВКонтакте». *Afisha*. Retrieved from https://www.afisha.ru/article/pavel-durov-vkontakte/

Durov, P. (2018, March 22). 200,000,000 monthly active users. Retrieved April 2, 2018, from https://telegram.org/blog/200-million

Forbes Staff. (2012, November 22). Kod Pavla Durova: pyat istorii iz zhizni Vkontakte i ee sozdatelya [Pavel Durov's code: Five stories from the lives of Vkontakte and its creator]. *Forbes Russia*. Retrieved from http://www.forbes.ru/sobytiya-opinion/lyudi/212150-kod-pavla-durova-pyat-istorii-iz-zhizni-vkontakte-i-ee-sozdatelya

Golumbia, D. (2013, September). *Cyberlibertarianism: The extremist foundations of 'Digital Freedom.'* Talk, Clemson University. Retrieved from http://www.uncomputing.org/wp-content/uploads/2014/02/cyberlibertarianism-extremist-foundations-sep2013.pdf

Gorny, E. (2007). The Russian Internet: Between Kitchen-Table Talks and the Public Sphere. *Art Margins*.

Habermas, J. (1989). *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*. Cambridge, Mass.: MIT Press.

Hakim, D. (2014, December 2). Once celebrated in Russia, the programmer Pavel Durov chooses exile. *The New York Times*. Retrieved from https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html?ref=technology&_r=1

Hanson, E. C. (2008). *The information revolution and world politics*. Lanham: Rowman & Littlefield.

Howard, P. N., & Hussain, M. M. (2013). *Democracy's fourth wave?: digital media and the Arab Spring*. Oxford; New York: Oxford University Press.

Hughes, E. (1997). A cypherpunk's manifesto. In *The electronic privacy papers* (pp. 285–287). John Wiley & Sons.

International Center for Not-for-Profit Law. (2016). *Overview of the package of changes into a number of laws of the Russian Federation de-*

signed to provide for additional measures to counteract terrorism. Washington D.C.: International Center for Not-for-Profit Law. Retrieved from www.icnl.org/research/library/files/Russia/Yarovaya.pdf

Ioffe, J. (2011, December 10). Snow Revolution. *The New Yorker*. Retrieved from https://www.newyorker.com/news/news-desk/snow-revolution#entry-more

Jakobsen, J. B. (2015). *A practical cryptanalysis of the Telegram messaging protocol* (Master's thesis). Aarhus University, Aarhus, Denmark. Retrieved from https://cs.au.dk/~jakjak/master-thesis.pdf

Jeffries, A. (2018, February 21). Exclusive: Telegram is holding a secretive second pre-ICO sale. *The Verge*. Retrieved from https://www.theverge.com/2018/2/21/17037606/telegram-open-network-app-ico-cryptocurrency-ton

Kononov, N. (2013). *Kod Durova: real'naia istoriia sotsseti "VKontakte" i ee sozdatelia [Durov's code: the real story of "Vkontakte" and its creator]*. Moscow: Izdatels'tvo "Mann, Ivanov i Ferber."

Kononov, N., & Igumenov, V. (2011, June 24). Kod Pavla Durova [Code of Pavel Durov]. *Forbes Russia*. Retrieved from http://www.forbes.ru/ekonomika/kompanii/69666-kod-pavla-durova

Krishna, S. (2017a, June 26). Telegram will register with Russia but won't share secure data. *Engadget*. Retrieved from https://www.engadget.com/2017/06/28/telegram-not-sharing-secure-data-russia/

Krishna, S. (2017b, October 16). Telegram fined after refusing to provide user data to Russia. *Engadget*. Retrieved from https://www.engadget.com/2017/10/16/telegram-fined-by-russian-court/

Krishna, S. (2018a, February 20). Telegram loses appeal over encryption keys in Russia. *Engadget*. Retrieved from https://www.engadget.com/2018/03/20/telegram-encryption-keys-russia-supreme-court/

Krishna, S. (2018b, April 6). Russia is getting closer to banning Telegram. *Engadget*. Retrieved from https://www.engadget.com/2018/04/06/russia-block-telegram-filed-lawsuit/

Levine, Y. (2017a, September). The crypto-keepers: How the politics-by-app hustle conquered all. *The Baffler*, (36). Retrieved from https://thebaffler.com/salvos/the-crypto-keepers-levine

Levine, Y. (2017b, September 7). My story in The Baffler: Pavel Durov, CIA-funded privacy and the paranoid grift of crypto politics. Retrieved March 31, 2018, from https://surveillancevalley.com/blog/baffler-pavel-durov-cia-privacy-crypto-grift-mass-politics-by-app

Levy, A. (2018, February 15). Secretive messaging app Telegram is selling a $2 billion crypto dream -- but skeptics smell a "ploy." *CNBC*. Retrieved from https://www.cnbc.com/2018/02/15/telegram-the-2-billion-crypto-offering-thats-dividing-tech.html

Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. New York: Penguin Books.

Liao, S. (2018, May 2). Telegram cancels its much-hyped initial coin offering. *The Verge*. Retrieved from https://www.theverge.com/2018/5/2/17312046/telegram-initial-coin-offering-ico-cancelled

Light, B., Burgess, J., & Duguay, S. (2016). The walkthrough method: An approach to the study of apps. *New Media & Society*, 146144481667543. https://doi.org/10.1177/1461444816675438

Maréchal, N. (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication*, *5*(1), 29. https://doi.org/10.17645/mac.v5i1.808

Maréchal, N. (2018). *Use Signal, Use Tor: The political economy of digital rights technology*. Dissertation, Los Angeles, CA.

May, T. (1995). The crypto anarchist manifesto. Retrieved from http://www.spunk.org/library/comms/sp000151.html

Moore, J. (2018, April 3). Telegram ICO sells-out 2nd round allocation, closes in on $2bn. *CryptoNews Review*. Retrieved from http://cryptonewsreview.com/telegram-ico-sells-out-2nd-round-allocation-closes-in-on-2bn/

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111–130.

Ognyanova, K. (2015). In Putin's Russia, Information Has You: Media Control and Internet Censorship. In M. M. Merviö (Ed.), *Management and Participation in the Public Sphere* (pp. 62–78). Hershey, PA: IGI Global. Retrieved from http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-4666-8553-6

Palmer, D. (2018, February 19). $850 million raised in ICO so far, says Telegram. *Coindesk*. Retrieved from https://www.coindesk.com/850-million-raised-in-ico-so-far-says-telegram/

Peters, B. (2016). How not to network a nation: the uneasy history of the Soviet internet. Cambridge, Massachusetts: MIT Press.

Price, M. E. (2015). *Free expression, globalism, and the new strategic communication*. New York, NY: Cambridge University Press.

Quénelle, B. (2016, June 6). Pavel Durov's war on state power. *The World Weekly*. Retrieved from https://www.theworldweekly.com/reader/view/2862/pavel-durovs-war-on-state-power-

Rothrock, K. (2016, October 25). Russia Is Reportedly Banning LinkedIn. *Global Voices*. Retrieved from https://globalvoices.org/2016/10/25/russia-is-reportedly-banning-linkedin/

SEC Form D submitted by TON Issuer Inc. (2018). Retrieved from https://www.sec.gov/Archives/edgar/data/1729650/000095017218000030/xslFormDX01/primary_doc.xml

Shirky, C. (2011). The political power of social media: technology, the public sphere, and social change. *Foreign Affairs*, *90*(1), 28–41.

Soldatov, A., & Borogan, I. (2013). Russia's Surveillance State. *World Policy Journal*. Retrieved from http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Soldatov, A., & Borogan, I. (2015). *The red web: the struggle between Russia's digital dictators and the new online revolutionaries* (First edition). New York: PublicAffairs.

Soldatov, A., & Borogan, I. (2017). *The red web: the Kremlin's wars on the internet* (First Edition, First Trade Paperback Edition). New York: PublicAffairs.

Stubbs, J., & Ostroukh, A. (2018, April 13). Russia to ban Telegram messenger over encryption dispute. *Reuters*. Retrieved from https://www.reuters.com/article/us-russia-telegram-block/russia-to-ban-telegram-messenger-over-encryption-dispute-idUSKBN1HK10B

Telegram. (n.d.). Telegram FAQ. Retrieved April 4, 2018, from https://telegram.org/faq

Telegram. (2018). Telegram Primer. Retrieved from https://gramfoundation.io/whitepaper.pdf

Thierer, A., & Szoka, B. (2009, August 12). Cyber-libertarianism: The case for real internet freedom. Retrieved February 24, 2018, from https://techliberation.com/2009/08/12/cyber-libertarianism-the-case-for-real-internet-freedom/

Tsotis, A. (2014, February 24). Telegram saw 8M downloads after WhatsApp got acquired. *Tech Crunch*. Retrieved from https://techcrunch.com/2014/02/24/telegram-saw-8m-downloads-after-whatsapp-got-acquired/

U.S. Securities and Exchange Commission. (2017, July 25). Investor Bulletin: Initial Coin Offerings. Retrieved from https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings

Vaidhyanathan, S. (2018). *Antisocial media: how facebook disconnects US and undermines democracy*. New York, NY, United States of America: Oxford University Press.

Vkontakte founder Pavel Durov learns he's been fired through media. (2014, April 22). *The Moscow Times*. Retrieved from https://themoscowtimes.com/articles/vkontakte-founder-pavel-durov-learns-hes-been-fired-through-media-34425

Walt, V. (2016, February 23). With Telegram, a reclusive social media star rises again. *Fortune*. Retrieved from http://fortune.com/telegram-pavel-durov-mobile-world-congress/

West, S. M. (2018). *Do ciphers have politics? A cultural history of encryption, 1963-2013*. Unpublished Manuscript, Los Angeles, CA.

White, S., & McAllister, I. (2014). Did Russia (Nearly) have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism: A Facebook Revolution in Russia in 2011? *Politics*, *34*(1), 72–84. https://doi.org/10.1111/1467-9256.12037

Yaffa, J. (2013, August 7). Is Pavel Durov, Russia's Zuckerberg, a Kremlin target? *Bloomberg Businessweek*. Retrieved from https://www.bloomberg.com/news/articles/2013-08-01/is-pavel-durov-russias-zuckerberg-a-kremlin-target

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5