Selling internet control: the framing of the Russian ban of messaging app Telegram

Mariëlle Wijermars

Aleksanteri Institute, University of Helsinki, Helsinki, Finland

ABSTRACT
How are extensive internet control, surveillance and restricted online anonymity reconceptualized into virtues of effective state governance, rather than violations of civic rights? The Russian government has instrumentalized ostensibly sound legitimations – countering terrorist and extremist propaganda, combatting child pornography – to bring about a dramatic decline in internet freedom. While these policies have been widely studied, scholarship examining how the Russian government legitimates and cultivates popular support for restricting online freedoms remains scarce. This article therefore studies how restrictions of internet freedom are framed in political and media discourses. It focuses on the case of Telegram, a popular messaging application that was banned in Russia in April 2018 for its refusal to provide the FSB with access to encrypted messages in compliance with anti-terrorism legislation. It finds that media framing of the ban was more diverse than the official governmental line. While national security framing was important, the ‘rule of law’ frame occurred most frequently, and conspiracy framing was markedly infrequent.

ARTICLE HISTORY
Received 26 November 2019
Accepted 4 May 2021

KEYWORDS
Internet governance; Russia; policy framing; messaging apps; Telegram; surveillance

1. Introduction
How are extensive internet control, surveillance and restricted online anonymity reconceptualized into virtues of effective state governance, rather than violations of civic rights? Against the backdrop of a global trend towards increased governmental control over the internet, this article investigates internet policy legitimation on the example of Russia. The Russian government has instrumentalized ostensibly sound legitimations – countering terrorist and extremist propaganda, combatting child pornography – to bring about a dramatic decline in internet freedom since 2012, enacting extensive infringements upon the freedom of speech, the right to information and privacy (Author, 2020a; Lonkila et al., 2020; Sherstoboeva, 2020). This expanding body of legislation and regulatory practices has been widely studied (Author, 2021; Nocetti, 2015; Sivetc, 2020; Soldatov, 2019), along with the Russian government’s perspective on cybersecurity...
(Claessen, 2020; Pigman, 2019) and online privacy (Lokot, 2020), as well as the consequences of its internet policy for citizens, political opposition and activists (Van der Vet, 2020). Studies have also highlighted the role citizens and non-governmental organizations play in effectuating (Daucé et al., 2019; Gabdulhakov, 2020) and resisting internet control (Ermoshina & Musiani, 2017; Lokot, 2018a).

Managing popular ‘appetite’ for internet control (Nisbet, 2015) is an important factor in determining Russia’s ability to restrict internet freedom with limited or manageable consequences for regime legitimacy (Shen, 2017). Moreover, as a ‘electoral autocracy’ (Gelman, 2015), Russia invests significant efforts in presenting its policies as reasonable and necessary and claims to act in response to popular demands for regulating the internet. For example, in 2017, the necessity of a proposed law regulating social media was justified by referring to societal concerns about ‘death groups’ on social media inciting teenagers to commit suicide (State Duma, 2017). Studies examining how the Russian government legitimates and seeks to cultivate popular support for restricting online freedoms are, however, lacking.

Mass media play a key role in shaping public perceptions of internet policy. Survey research indicates that Russians who rely on state-controlled federal TV news perceive the internet as a threat more often and indicate higher support for political censorship online (Nisbet et al., 2017). Yet, TV coverage and the strategies media employ to shape public perceptions of internet policy have not yet been studied. This article therefore analyses how restrictions of internet freedom are framed in Russian political and media discourses. It focuses on the case of Telegram, a popular messaging application that was banned in Russia in April 2018 for its refusal to provide the Russian Federal Security Service (FSB) with access to encrypted messages in compliance with anti-terrorism legislation. The relative bandwidth of initiative and interpretation that federal media have in shaping their coverage – simultaneously interpreting and co-constituting the preferred official line on policy issues (Wijermars, 2020a; Tolz & Teper, 2018) – further warrants analysing media framing of internet policy as a factor shaping internet control in Russia.

The article is structured as follows. I first review online information control in Russia and the cyberthreats its government claims to address, and examine the conflict between Telegram and Russian authorities in further detail. Then, I outline the methodology of the study, before discussing the findings of the qualitative frame analysis of the media corpus. The study finds that media framing of the ban was more diverse than the official governmental line. While national security framing was important, the ‘rule of law’ frame occurred most frequently, and conspiracy framing was markedly infrequent.

2. Online information control in Russia and the construction of cyberthreats

The internet in Russia remained relatively free up until the protest movement of 2011–2013, which was prompted by electoral fraud in the parliamentary elections of December 2011 and facilitated by social media (Author, 2020a). Whereas traditional media had been brought under increasingly strict state control after 2000, on the internet unwanted discourses were, instead, actively manipulated by authorities, a strategy that has since
been exported (Deibert & Rohozinski, 2010; Kurowska & Reshetnikov, 2018). From 2012 onwards, Russia began complementing these tactics with legal restrictions, including website blocking (Lonkila et al., 2020).

The initial list of grounds for ‘blacklisting’ a website, i.e., adding it to a central register and requiring internet service providers to block access to it, was limited: child pornography, promotion of drug use and information on committing suicide. Subsequent legislation soon expanded the list of prohibited types of information to include political and other loosely formulated categories, such as calling for unsanctioned protests and offending the feelings of religious believers (Sivetc, 2020). Citizen volunteers and non-governmental organizations have contributed to effectuating these control mechanisms through vigilantism collectives, so-called Cyber Guards (kiberdruzhiny), aiming to ‘clean’ the internet by tracking down and reporting illegal content (Daucé et al., 2019; Gabdulhakov, 2020). While the enforcement of prohibitions has been partial and arbitrary, it has, among other outcomes, resulted in the prosecution of citizens for posting or sharing content on social media and violates Russia’s obligations for the protection of freedom of speech under the European Convention on Human Rights (Sherstoboeva, 2020; Van der Vet, 2020).

The fact that (overt) online censorship was limited before 2012 should not be mistaken for a lack of state control over the internet at that time, quite the contrary: The FSB has been able to monitor and intercept all digital communications since the introduction of the second generation of the System for Operational-Investigative Activities (SORM II) in 1999 that extended previously existing telecommunications surveillance powers to the internet (Nocetti, 2015). End-to-end encryption interferes with this ability to intercept online communications and is therefore perceived as a security threat. This is reflected in the Russian government’s view of data privacy that ‘sees its citizens as vulnerable data subjects with little agency, whose private identities and communications should be protected from “foreign interference,” but must always remain visible and accessible to the state’ (Lokot, 2020, p. 320). It should be stressed, however, that Russia’s critical stance on encryption is far from exceptional. Most states agree that some form of exceptional access is desirable to ensure effective law enforcement. Estonia and the Netherlands are the sole countries to have declared explicit support for end-to-end encryption without a ‘backdoor’ (Veen & Boeke, 2020).

The surveillance prerogatives of the Russian state were expanded as part of the 2016 anti-terrorism legislation package commonly referred to as the Yarovaya Law (named after member of parliament Irina Yarovaya). Among other measures, it imposed extensive data storage requirements on telecom providers (Lehtisaari, 2020). While the Yarovaya Law has yet to be implemented in full as a result of technical difficulties and financial constraints, the decision to block Telegram for not providing access to encrypted communications has been one of its most visible outcomes, as will be discussed in below. To further consolidate control over the internet, Russia has, among other measures, imposed the legal requirement to store personal data of Russian citizens on servers located on the territory of the Russian Federation (Federal Law No. 242 of 21 July 2014) and banned VPN services that provide access to blacklisted websites (Federal Law No. 276 of 29 July 2017). These measures are in line with the aim to establish a ‘sovereign’ Russian internet, capable of operating independently from the global internet in case of a substantial outside threat to its integrity (Author, 2020b; Federal Law No. 90 of 1 May 2019).
According to Pigman (2019), the thinking of Russia’s political elites is guided by three perceived cyberthreats, that shape policy making in this domain: threats to regime security, public safety and societal norms and values. The first, Pigman finds, is the most prominent and concerns the threat of foreign interference by means of digital tools to ‘exploit and even foment internal conflict so as to create conditions in which Russia’s legitimate government can be overthrown’ (Pigman, 2019, p. 25). The second perceived threat stipulates that the freedoms permitted by the internet are exploited by extremists and criminals, thereby posing a threat to public safety. Here, the ‘national security costs of anonymity and encryption of communications’ resulting from their hindrance of ‘law enforcement efforts to monitor and police the malign activities of criminals and extremists in cyberspace’ are considered to outweigh any benefits in terms of citizens’ privacy (Pigman, 2019, p. 26). Finally, the internet is thought to threaten social norms and cohesion through, first, the various kinds of offensive content that can be found online and, second, the anti-social behaviors that are supposedly promoted by conditions of online anonymity.

These and other legitimating frames appear to have been successful in maintaining a substantial level of support for internet control. A study conducted at the Annenberg School for Communication at the University of Pennsylvania found that 49 percent of Russians supported internet censorship (Nisbet, 2015, p. 8). Trust in the motivations behind governmental policy was significant: 51 percent of respondents indicated that ‘the primary motivation of the government legislation creating a blacklist of websites is the maintenance of political stability,’ while only 13 percent were of the opinion that its primary objective, instead, was ‘limiting democratic freedoms’ (Nisbet, 2015, p. 8). Other polls sketch a similar picture. Independent pollster Levada Center found that, in October 2016, 60 percent of respondents were in favor of restricting online communications (Konobeevskaya, 2016). Only a third of respondents thought website blocking could be used against civil activists (Levada Center, 2016). In a 2017 poll connected to the proposal to introduce an age-limit for social media use, mentioned earlier, 62 percent supported the initiative (VTsIOM, 2017).

Popular resistance to the expansion of Russia’s system of internet controls, moreover, long remained limited. The case of Telegram, in fact, was the first instance when an act of restricting internet freedom was met with popular protest. An estimated 7,500–10,000 persons took part in a demonstration against the decision on 30 April 2018, while videos and images of flying paper planes – in reference to the messenger’s logo – were shared online. One year later, some 15,000 persons participated in a Moscow protest rally against the ‘sovereign internet law’ that was adopted by the State Duma in its first reading in the month before, while smaller protests occurred in several other cities (BBC Russian, 2019).

### 3. The blocking of Telegram

Telegram offers end-to-end encrypted private messaging and has been linked by the Russian government to the organization of terrorist attacks, including bombings in the St. Petersburg metro system on 3 April 2017. The app was launched in 2013 and by March 2018 reached 200 million users, according to a company statement (Durov, 2018). Telegram’s founders, the brothers Pavel and Nikolai Durov, who previously
founded Russia’s most popular social networking site VK (previously known as VKontakte), have a strained relationship with Russian authorities. In 2014, Pavel Durov ‘was forced to sell his shares and resigned as the company’s CEO following his continued refusal to cooperate with the Russian authorities by sharing user information’ (Wijermars, 2020a, p. 6).

The legal conflict between Telegram and Russian authorities was protracted over a year. Telegram, among other arguments, claimed it is technically impossible for the company to share decryption keys because of the nature of its encryption protocol. On 13 April 2018 the Moscow Tagansko Court granted the blocking of the app in Russia. Roskomnadzor, the federal executive body entrusted with enforcing media and telecommunications regulations, encountered severe difficulties in effectuating the ban. To keep the messenger accessible in Russia, Telegram used domain fronting, among other techniques (see Burgess, 2018). Roskomnadzor blocked IP addresses associated with Telegram services, including some owned by Google and Amazon. The collateral damage caused by the campaign was significant as access to some 18 million IP addresses ‘with no evident relation to Telegram’ was blocked (Lokot, 2018b) and various online services were disrupted (Li et al., 2018). The efforts to block the messenger appear to have had the opposite effect since Telegram’s audience increased one-and-a-half fold and reached 4.4 million daily Russian users in February 2019 (Sobolev & Maliarenko, 2019).

As was mentioned above, the enforcement of internet legislation in Russia is selective. For example, while professional online networking website LinkedIn was blocked for not complying with the data localization requirement, other companies such as Facebook received only minor fines. The ban of Telegram therefore raised some eyebrows. As Pigman remarks, ‘Russian political elites initially presented Telegram as the face of the cyberthreat to public safety with such intensity that political commentators predicted the messaging app’s proscription was imminent almost a year before it occurred’ (Pigman, 2019, p. 27). The use of Telegram by terrorist groups has caused concern outside of Russia as well, in particular in connection to the series of ISIS-linked terrorist attacks in European cities after 2014 (Shehabat et al., 2017). The combination of the platform’s functionalities and its more lenient policies towards content have also made Telegram one of the places where ‘extreme’ users and internet celebrities who have been ‘deplatformed’ elsewhere for violating user rules (e.g., on Twitter) migrate to (Rogers, 2020, p. 217).

In the period between the initial stand-off between Roskomnadzor and Telegram in early 2017 over its registration as an ‘information distributor’ and the decision to block the messenger, alternative scenarios began circulating. Business media RBK, for example, cites a letter by an FSB employee, indicating that the real reason behind the blocking is Durov’s effort to launch a cryptocurrency (Kolomychenko, 2018). The plans for launching the Telegram Open Network (TON) blockchain and its native tokens was announced at the end of 2017, while the Initial Coin Offering gathered investments in February and March 2018. According to RBK, the blocking of Telegram would not necessarily prohibit the cryptocurrency launch in a technical sense – the blockchain operates independently – but the substantial financial costs incurred to keep Telegram accessible in Russia could place a severe burden on the company’s budget and thereby delay or prevent the launch (Kolomychenko, 2018).
Encrypted messaging is also popular among journalists and activists seeking to shield themselves from governmental surveillance. The functionalities offered by Telegram are useful for organizing protest actions, for example. The mass demonstrations that took place in the spring of 2017 in response to video investigations published by Aleksei Navalny’s Anti-Corruption Foundation, the first of this scale since 2013, led to a renewed effort to suppress political opposition. Some saw the decision to ban Telegram in direct connection to its role in facilitating political mobilization. In Iran, where the app has been used for similar purposes and has similarly refused to provide authorities with access to its users’ communications, Telegram was blocked around the same time (Akbari & Gabdulhakov, 2019).

Finally, Telegram offers a public channels function, which rapidly expanded into a booming news platform. While functioning in a way similar to a broadcasting device, both the owner of and subscribers to the channel can maintain their (public) anonymity (Lokot, 2018b). Special briefings on Telegram channels were added to media monitoring reports prepared for top government officials, including the Russian president, indicating their influence (Churakova et al., 2017).

After two years of unsuccessful attempts to effectuate the Telegram ban, the case took an unexpected turn. Following negotiations between Telegram and Russian authorities, the ban was revoked on 18 June 2020. While Roskomnadzor claimed the ban was lifted in response to Durov’s commitment to collaborate on fighting extremist and terrorist activities on its platform, it remains unclear whether and which concessions were agreed upon by the company (Reuters, 2020).

4. Methodology

In Russian political discourse, the decision to ban Telegram has thus been framed predominantly in terms of public safety – the need to protect the Russian population against the threat of Islamic terrorism – and, by extension, regime security since separatist movements in the North Caucasus form a threat to the integrity and stability of the Russian Federation. To examine the function of mass media in how the Russian government seeks to cultivate popular support for restricting online freedoms a qualitative frame analysis of TV coverage of the Telegram case was conducted.

Despite the expanding influence of online media, Russian state television continues to be the main source of information for 74 percent of Russians, while this is less pronounced among the younger generation (Volkov & Goncharov, 2020). As a result, federal TV channels continue to play an important role in shaping public opinion. Talk shows have played a key role in the Russian government’s political and ideological campaigns, in particular during Putin’s third presidential term, and ‘became the main format for exploring the campaign’s key themes’ (Tolz & Teper, 2018, p. 220). This strategy of discussing political questions on talk shows is particularly effective because, ‘while many people quickly discard factual details disseminated by television programs, they retain the “emotional tags” attached to conveyed pieces of information’ (Tolz & Teper, 2018, p. 220).

The media corpus selected for the study therefore was extended beyond news broadcasts to include all relevant items broadcast by the three most popular TV channels – Pervyi kanal, Rossiia and NTV – in the period May 2017–August 2018. This period
encompasses the first requests for Telegram to register as an ‘information distributor’ and provide decryption keys through to the blocking coming into effect. Broadcasts were collected from the websites and YouTube channels of the respective TV channels, using relevant keywords (including Telegram, written in Cyrillic and Latin script; messenger; Roskomnadzor; Durov). Checking for relevance and duplication, a total of 25 unique items were collected with a runtime of the relevant program item ranging between one minute and 25 min. Media attention peaked in parallel with regulatory enforcement and coverage was quite intense during these periods of political significance: 8 unique items were broadcast in the period 23–28 June 2017 as the initial standoff between Roskomnadzor and Telegram escalated, while 11 unique items were broadcast between 16–24 April 2018 when Roskomnadzor blocked the app. During the remainder of the sampling period, when political urgency was low, media coverage was also significantly less (6 items). In addition to news broadcasts (15), coverage included talk shows (5), thematic news series (3), investigative reporting (1) and the annual ‘Direct Line’ (Priamaia liniia) call-in talk show with the president. The protests against the blocking of Telegram were not covered by the federal channels examined.

While the method of data collection allows us to investigate media framing of events in the past, complementing the time and resource-consuming method of long-term comprehensive media monitoring, it has some limitations. First, not all instances that these items were broadcast were necessarily captured; in the case of news, the same item is likely to have been included in multiple news broadcasts throughout the same day. Second, it may be that not all relevant broadcasts were also published on the respective websites and/or YouTube channels. An assessment of online publication frequency and availability of archived materials suggests the implications of this limitation are acceptable. In the case of Pervyi kanal, for example, the online archive (at a minimum) comprises daily 6 PM news broadcasts for the past ten years, as well as all episodes of relevant talk shows, such as Vremia pokazhet. Similarly, the NTV website archives, for example, all broadcasts of Tsentralnoe televidenie (weekly) and ChP (on weekdays) as well as multiple daily broadcasts of news program Segodniiia, all going back to 2011. Via its YouTube channels, a very extensive archive of Rossiia programs is available, including all episodes of such talk shows as 60 minut po goriachim sledam and news broadcasts (among others, Vesti v 20:00) going back several years. Finally, there is the possibility that some relevant items were not identified as a result of the websites’ incomplete implementation of search functionality for video content (e.g., lack of captions). However, this would only concern those cases when none of the keywords was included in the item heading, thereby also significantly reducing the likelihood of their relevance.

Frame analysis is a well-established method for analysing the interpretative frames provided by media to their audiences for making sense of complex realities. It emerged out of an interest in how media coverage influences policy processes and public perceptions of policy. According to Robert Entman’s classic definition, ‘[to] frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation’ (Entman, 1993, p. 52). Through their framing choices, ‘media can affect how the public and policy makers view certain issues on the public and policy agendas’ (Crow & Lawlor, 2016).
Following Crow and Lawlor (2016), this study acknowledges the usefulness of complementing frame analysis with analysis of policy narratives. While the concepts of frames and narratives are closely related and share many core assumptions, ‘framing theory focuses on the broad categories, segments, or angles through which a story can be told, [whereas] narrative construction involves decisions by storytellers that determine the specific characters, plot, causal implications, and policy solutions presented’ (Crow & Lawlor, 2016). This narrativization – establishing a ‘setting, characters (heroes, villains, and victims), a plot, and the moral of the story’ – enables the personalization of the events described and thereby ‘helps create social meaning from events or actions’ (Crow & Lawlor, 2016).

The selection of frames departed from the three cyberthreats constructed by Russia’s political elites (Pigman, 2019). Research also indicates there is a high prevalence of conspiracy reasoning in Russian political and media discourses and mass culture (Wijermars, 2020a; Borenstein, 2019; Yablokov, 2015, 2018). A final frame emerging from the literature is the rhetorical strategy of overidentification with liberal norms, including rule of law, which has been demonstrated in Russian diplomacy (Kurowska & Reshetnikov, 2021). The validity of these frames was tested through a manual reading of a sample of the media corpus. Based on this assessment, the threats to regime security and public safety identified by Pigman were merged into a single ‘national security’ frame. The frames ‘societal norms,’ ‘rule of law’ and ‘conspiracy’ were maintained, while one additional frame – ‘technical complexity’ – was added in order to capture all perspectives found in the sample. Based on the literature discussed above, the frames can be characterized as follows:

**National security:** the national security frame stresses the danger posed by digital technologies and online communications to public safety and, by extension, regime security by facilitating the activities of terrorists and other extremist or subversive groups (Pigman, 2019). Relevant terms include security [bezopasnost’], terrorist [terrorist], (bomb) explosion [vzryv], drugs [narkotiki].

**Societal norms:** this frame emphasizes the need to protect societal norms and values (Pigman, 2019). By drawing upon morality and underlying notions concerning the proper role of the internet within society, the frame promotes increased control and proactive action to address potential harmful effects. Relevant terms include harmful [vrednyi], children [deti], vulnerable [uiazvimyi], health [zdorov’e], values [tsennosti].

**Rule of law:** this frame emphasizes legislation and compliance. With regards to Russian diplomacy, Kurowska and Reshetnikov (2021) argue that Russia’s contradictory, mocking or even blatantly false public statements are best understood through the concept of trickery, in which overidentification with liberal norms (sovereignty; the equality of states) takes center stage (for example, in Russia’s invocation of international legal norms to justify its military intervention in Georgia in 2008). The overidentification is effective in levelling out power relations and undermining these very norms, since ‘[c]alls for strict compliance put on public display the structural hegemony and quotidian hypocrisy of those liberal actors who profess but routinely breach liberal norms’ (Kurowska & Reshetnikov, 2021, p. 12). The use of this frame therefore simultaneously legitimates governmental action – stressing its adherence to the rule of law, even when this is not factually accurate – while undermining actors criticizing it on the basis of their supposed hypocrisy. Relevant terms include law [pravo], court [sud], decision [reshenie].
**Technical complexity:** this frame places emphasis on the way digital communications work. ‘Technolect’ framing may function to elucidate or obscure the functionalities of the technology in question, and thereby serve to either empower or dishearten the viewer in their capacity to understand, assess and respond to the threats associated with digital technologies. Relevant terms include technical [tekhnicheskii], complicated [slozhnyi], encryption keys [kliuchi shifrovanii], data [dannye].

**Conspiracy:** the final frame gives evidence of conspiracy thinking by claiming to expose double meanings, hidden motivations or conspiracies between foreign and domestic actors. While this frame may resonate with arguments associated with the national security frame, it sets itself apart by its argumentative style and how it draws upon well-established conspiracy tropes, such as allegations of ‘anti-Russian’ objectives (Yablokov, 2018). Relevant terms include allegedly [iakoby], in reality [na samom dele].

The occurrence of frames was detected through a manual coding of relevant terms and phrases. Taking media items as the unit of analysis, multiple frames could be assigned to a single item. In recognition of the audio-visual nature of the empirical materials analysed, visual elements were also coded. The coding furthermore included narrative elements – the presence or absence and identity of heroes, victims and villains.

### 5. Media framing of the Telegram ban

The analysis of the media corpus found that three of the five frames occurred most frequently. The ‘rule of law’ frame was identified in 18 of the 25 media items (72%), followed in frequency by the ‘national security’ (15) and ‘technical complexity’ (14) frames. The remaining two frames were used far less often: the ‘societal norms’ frame was identified five times, while ‘conspiracy’ framing was found in only four of the media items. These findings demonstrate that the media framing of the Telegram case is more diverse than suggested by how Russian political elites construct cyber threats. While the importance of national security framing is confirmed, concerns about digital technologies threatening societal norms and cohesion were not very pronounced in the media coverage of the Telegram ban. The high frequency of the ‘rule of law’ frame which, as will be discussed below, is characterized to a large extent by overidentification with these legal norms, demonstrates that Kurowska and Reshtnikov’s findings are valid beyond the confines of Russian diplomacy. Finally, compared to previous studies on Russian TV coverage of current affairs, conspiracy framing is quite infrequent. When the findings of the media frame analysis are compared to how the Telegram ban was framed in Russian political discourse, as was analysed above, it becomes clear that the media framing is both more diverse and more legal and technical in focus, in addition to replicating the national security framing employed by the Russian government.

Co-occurrence of frames was found in 16 media items (64% of the corpus), of which five items contained two frames, seven items contained three frames, and four items were found to have four frames (see Table 1). Items discussing their subject matter within the confines of a single frame tended to be short (mean value one minute), while mid-length items (mean value 5:20) were found to contain two or three frames, and four co-occurring frames were found in longer items (mean value 10:45). The following paragraphs characterize how these frames were realized in the coverage on Telegram and illustrates them with selected examples.
The application of the ‘rule of law’ frame focuses on legal obligations, procedures and compliance. The latest developments in the conflict between Telegram and Russian authorities are presented, often in complex procedural language. Creating the suggestion of neutral coverage, it is stressed Telegram needs to comply with the law; if the company fails to do so, Roskomnadzor is warranted to act. Statements by the agency’s head, Aleksandr Zharov, serve to emphasize its willingness to reach an agreement with Telegram, if only they would respond to its requests. This lack of responsiveness, in turn, is interpreted as a sign of the company’s disrespect for Russian law, which is often personalized by claiming that Durov believes himself to be exempt from abiding by its stipulations.

In a broadcast of Vesti nedeli (Pervyi kanal, 25 June 2017) we find an example of argumentation that emphasizes the motto that law is law. It exemplifies the rhetorical over-identification with international legal norms that ‘holds a mirror to hierarchies in international society and unearths controversies hidden in its core, thereby exposing double standards and heightening awareness of discrimination’ (Kurowska & Reshetnikov, 2021, p. 2). In this case, it is claimed double standards are applied when comparing Russian and American internet policy.3

Those who support Durov claim that, in the West, there are no requirements like those in Russia and that it is a violation of freedom. But they forget to mention that, over there, the secret services (and the American, most of all) surveil users secretly. Edward Snowden has told about this in detail ... The largest American tech companies cooperate with the secret services – this was also uncovered by Snowden. Russia takes a different route: the choice of alternative is not whether to surveil or not ... – no government will forego on this – but how. To surveil secretly, pretending that complete freedom exists, effectively misleading your citizens, or to carry out legal procedures, according to which the secret services will work. And we have already passed laws that have established these procedures.

The ‘rule of law’ frame functions to claim the rationality and proportionality of the decision and normalizes governmental surveillance. By referring to the National Security Agency’s (NSA) surveillance of American citizens the actions of the Russian government are presented as being more transparent and morally superior. The allegation of double
standards is a common feature in the media coverage examined. For example, in an episode of the talk show *Vremia pokazhet* (‘Time will tell’, *Pervyi kanal*, 18 April 2018) it is claimed that the US promotes internet freedom merely to gain full access to information abroad, while it seeks to defend its own ‘digital sovereignty’.

The ‘national security’ frame justifies the expansion of internet control by exposing how encrypted messengers, and Telegram in particular, facilitate the activities of terrorist and extremist groups and drug dealers. It often creates a (flawed) black-and-white opposition between the *individual* privacy provided by encryption and the *collective* safety of the general public. As a result, any defense of the value of online privacy is equated to sacrificing national interests and public safety. Recurring features associated with this frame are graphic imagery from terrorist attacks in Russia and Europe, footage of security services conducting arrests, screenshots of terrorist propaganda shared in Telegram groups and suspects’ testimonies (recorded under evident pressure) in which they spell out how they used Telegram to communicate. Multiple broadcasts point out that the European Union equally seeks to counter the transnational orchestration of terrorist acts enabled by the messenger.

The annual call-in show with the president provides another example. The 2018 show (*Priamaia liniia*, 7 July 2018) includes a group of Russian bloggers, who ask the President about the prospect of other popular platforms, such as YouTube, being blocked in the near future. Vladimir Putin connects the question back to Telegram and replies:

> We are not planning to close down anything. I understand the situation around Telegram well … I am worried … about the safety of people. When the representatives of, say, the security services tell me that the bombings in the St. Petersburg metro … they could not surveil the communications of the terrorists, they could not take preventive actions because it was encrypted … How should I respond to this? Questions of security come in first place. I myself worked in the secret service and know it is easiest to ban, it is much more difficult to find civilized solutions … I will push my colleagues to go in exactly this direction.

While Putin intimates the proportionality of the government’s response, he emphasizes that national security concerns must always prevail. Another speaking example was found in the *Vesti Nedeli* broadcast of 25 June 2017, introduced above. A news item dedicated to the St. Petersburg bombings earlier that year diverts extensive attention to the role of instant messaging services. The item features an anonymous FSB operative, shown from behind, who claims the existence of Telegram-activated terrorist ‘sleeper-cells’. While showing video footage of a large crowd of people queuing in the Moscow metro – most of them of Central Asian appearance (i.e., predominantly Muslim migrant workers) – the voice-over comments, that ‘some closed groups have a reach of up to 40,000 persons, which means that at any given moment – after receiving the agreed signal – they are ready to appear at a given location’. The strategy, it is stated, was used the year before by ISIS to organize an attack in Dagestan.

While terrorism is presented as the main danger, drug dealing, and on one occasion corruption, is also covered at length. For example, an item on news broadcast *Vesti* of 23 June 2017 (*Pervyi kanal*) dedicated to the possible blocking of Telegram shows footage of police raiding an apartment to arrest persons suspected of drug dealing. While large amounts of drugs can be seen in the frame, it is indicated sales were conducted through Telegram.
The third most frequent frame, ‘technical complexity,’ approaches the topic by showing how digital technologies work. A frequently occurring feature are visualizations, such as animations and stock images. In general, efforts to explain technology – in this case, encryption, transnational data flows, and so on – should be applauded. With regard to the corpus examined, however, the degree of complexity of the graphics stands out. This means that more often than not, the visualizations exacerbate confusion rather than clarify. For example, in an episode of an investigative show entitled ‘Census of terrorists’ (Perepis’ terroristov), rapidly moving numbers and blinking lights are used to illustrate the nature of digital communications (ChP. Rassledovanie, 19 May 2017, NTV). As the show’s subtitle, ‘Gigabites of terror: how did the virus of extremism strike online messenger services?’, indicates, the episode set out to elucidate how various instant messengers are used in spreading extremist thought and facilitate communication among terrorists. Among its visualizations is a globe, encircled by fast-moving dotted lines indicating communications across continents, embellished with lock signs to indicate their encrypted nature. The visual intensity of these graphics serves rather to confuse and overwhelm the viewer – if information is spreading at lighting speed, what can an ordinary person do about it? – and reinforce a sense of powerlessness. The fact that much of the imagery used is inaccurate – it is not related to or representative of the topic discussed – reinforces this discrepancy.

Interestingly, a news broadcast aired on 16 April 2018, shortly after Roskomnadzor initiated the blocking, advises its viewers on what to do if the app stops working. In addition to mentioning alternative apps, in line with government officials’ suggestion that users should switch to Russian-owned messenger TamTam, it is explained how the ban can be circumvented by using a VPN service (Vesti v 20:00, Rossiia 1).

How media discussed Roskomnadzor’s failure to effectuate the ban is diverse. While they initially declare it may take several hours for the ban to take effect but the first interruptions were already apparent (60 minut po goriachim sledam, Rossiia 1, 16 April 2018) by the next day the narrative had to be adjusted. Now, it was acknowledged the blocking was not yet fully effective and that the number of users was in fact increasing (Vesti.net, Rossiia 24, 17 April 2018). By the end of the week, the main Sunday news broadcast conceded that the blocking turned out to be difficult and may take several months (Vesti nedeli, Rossiia 1, 22 April 2018).

The ‘societal norms’ frame, which emphasizes the need to protect societal norms and values and promotes increased control to address potential harmful effects, was mostly identified in media items addressing Telegram in the context of a broader discussion of the dangers associated with digital technologies. In an episode of the thematic news series ‘The future is around the corner’ (Budushchee za uglom – Voskresnoe vremiia, Pervyi kanal, 22 April 2018) dedicated to the topic of ‘digital slavery,’ the internet freedom promoted by Durov and Mark Zuckerberg is claimed to be only a façade for manipulating users into a state of dependency. The addiction-like response users develop as a result of the release of dopamine – for example when someone likes their content – is particularly damaging for children, it is claimed. The argument is accompanied by a series of YouTube testimonials by young Russian children in evident emotional distress over their lack of followers.

Finally, the ‘conspiracy’ frame appeared infrequently and mostly focused on revealing the ‘true’ motivations behind Telegram’s actions. The conflict with Russian authorities
was not motivated by the company’s sincere concern with the privacy of its Russian users, it is argued, but is part of a PR effort to expand into global markets (Vesti nedeli, Rossiia 1, 22 April 2018). The global attention for Durov’s refusal to collaborate with the FSB, it is claimed in another news broadcast, will help to launch its cryptocurrency by underscoring the independence, reliability and security of his business endeavors (Vesti v 22:00, Rossiia24, 16 April 2018). Durov is often targeted directly, for example by intimating that the privacy protection offered by Telegram may not be real as it rests only on one’s belief in Durov’s integrity (Tsentrальное телевидение, NTV, 21 April 2018). Some of the media coverage diverts attention to the involvement of foreign governments and the domestic ‘enemies’ they supposedly support (so-called ‘foreign agents’). The episode of talk show Vremia pokazhet (‘Time will tell’, Pervyi kanal) of 18 April 2018, for example, introduces political scientist Natal’ia Shavshukova as a representative of the opposition-minded metropolitan ‘intelligentsia’ who use Telegram. In addition to a barrage of condescending and sexist remarks and not allowing her to speak, the hosts intimates Shavshukova maintains links to American ‘intelligentsia’.

While Russian talk shows tend to be carefully choreographed, some do not go as planned. A guest on ‘60 minutes’ (60 минут по горячим следам, Rossiia 1, 20 April 2018) suddenly deviates from the planned topic of Ukraine to discuss Telegram. Il’ia Shablinskii, a law professor at the Moscow Higher School of Economics, complains that the show discusses only Ukraine and Syria, while it should be discussing the blocking of Telegram. To silence his unplanned intervention, the two hosts draw upon the two most popular frames: while the first presenter emphasizes that court decisions need to be respected, the second stresses national security concerns.

Assessing the corpus as a whole, it can be noted that the designation of victims remains abstract – civilians, ordinary Russians – while the role of villain is more personalized – from the ‘eccentric,’ ‘anarchist’ figure of Pavel Durov to individual terrorism suspects. By protecting Russian citizens against the terrorist threat and enforcing Russian law, the FSB and Roskomnadzor take on the role of heroes, but even Russian state media has to concede that the latter failed to live up to its task.

6. Conclusion

This article has examined the legitimation of internet policy in Russia by analysing the political and mass media framing of the ban of Telegram. The alignment of media coverage with regulatory enforcement efforts confirms the role of state media in explaining and legitimating these actions, especially when citizens will experience their effects directly. State media framing of policy was more diverse than the official government line, yet served solely to support it. This created some awkward moments when implementing the ban proved problematic. While, as expected, national security framing was important in the media coverage, framing the ban in terms of ‘rule of law’ occurred most frequently. The predominance of (overidentification with) liberal norms was not previously demonstrated and warrants further research. How often the ban was presented as a complex technical matter and how infrequent conspiracy framing was found also deviates from what previous research suggests. This may, in part, be explained by the chosen case: encryption is far removed from the everyday reality of the average viewer, and with a court decision in hand there was less need to suggest hidden plots.
The fact that the ban had significant implications concerning civic rights was downplayed or simply ignored. By suggesting a black-and-white opposition between, first, national security and individual privacy and, second, between the metropolitan elite (who values privacy and access to information) and the general public, the ban of Telegram was presented as a necessary state intervention, brought about by Durov’s reluctance to respect Russian law, rather than as a restriction of citizens’ freedoms.

Further research is needed to confirm whether the case of Telegram is representative of internet policy framing in Russia, more generally, and to gain further insight into the dynamics of media coverage (when are policy issues addressed extensively, when are they intentionally ignored?). In addition, the audience reception of media coverage on internet policy and its effects on public opinion require further investigation.

Notes
1. The use of broader search terms, such as ‘social media’, did not return relevant items.
2. No data is publicly available on full broadcasting schedules on program item level.
3. All translations by the author.

Disclosure statement
No potential conflict of interest was reported by the author(s).

Funding
This work was supported by Nederlandse Organisatie voor Wetenschappelijk Onderzoek under [grant number 446-17-005]; Dutch Organization for Scientific Research.

Notes on contributors
Dr Mariëlle Wijermars is a Visiting Researcher at the Aleksanteri Institute of the University of Helsinki and Assistant Professor in Cyber-Security and Politics at Maastricht University. Previously, she was a Rubicon postdoctoral fellow at the University of Helsinki. She conducts research on internet governance with a focus on the impact of internet policy on human rights, and on the framing of cyberthreats and policy responses. She is co-editor of The Palgrave Handbook of Digital Russia Studies (Palgrave Macmillan, 2021) and Freedom of Expression in Russia’s New Mediasphere (Routledge, 2020) [email: marielle.wijermars@helsinki.fi].

ORCID
Mariëlle Wijermars http://orcid.org/0000-0001-7735-4403

References
Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. Surveillance & Society, 17(1/2), 223–231. https://doi.org/10.24908/ss.v17i1/2.12928
BBC Russian. (2019, March 10). V Moskve proshel miting protiv izoliatsii runeta. bbc.com/russian/news-47514303
Borenstein, E. (2019). *Plots against Russia: Conspiracy and fantasy after socialism*. Cornell University Press.

Burgess, M. (2018, April 28). This is why Russia’s attempts to block Telegram have failed. *WIRED*. https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google

Churakova, O., Mukhametshina, E., & Ser’gina, E. (2017, September 24). V Kremle i FSB zanialis’ monitoringom telegram-kanalov. *Vedomosti*. https://www.vedomosti.ru/politics/articles/2017/09/24/735092-kremle-fsb-telegram-kanalov

Claessen, E. (2020). Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: The case of Russia and the EU. *Journal of Cyber Policy*, 5(1), 140–157. https://doi.org/10.1080/23738871.2020.1728356

Crow, D. A., & Lawlor, A. (2016). Media in the policy process: Using framing and narratives to understand policy influences. *Review of Policy Research*, 33(5), 472–491. https://doi.org/10.1111/ropr.12187

Daucé, F., Loveluck, B., Ostromoukhova, B., & Zaytseva, A. (2019). From citizen investigators to cyber patrols: Volunteer internet regulation in Russia. *Laboratorium: Russian Review of Social Research*, 11(3), 46–70. https://doi.org/10.25285/mac.v5i1.816

Deibert, R., & Rohozinski, R. (2010). Control and subversion in Russian cyberspace. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access controlled: The shaping of power, rights, and rule in cyberspace* (pp. 15–34). MIT Press.

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

Entman, R. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

Ermoshina, K., & Musiani, F. (2017). Migrating servers, elusive users: Reconfigurations of the Russian internet in the post-Snowden era. *Media and Communication*, 5(1), 42–53. https://doi.org/10.17645/mac.v5i1.816

Gabdulhakov, R. (2020). (Con)trolling the web: Social media user arrests, state-supported vigilantism and citizen counter-forces in Russia. *Global Crime*, 21(3–4), 283–305. https://doi.org/10.1080/17440572.2020.1719836

Gelman, V. (2015). *Authoritarian Russia: Analyzing post-Soviet regime changes*. University of Pittsburgh Press.

Kolomychenko, M. (2018, April 20). FSB reshila blokirovat’ Telegram iz-za planov Durova sozdat’ kriptovaliutu. *RBK*. https://www.rbc.ru/technology_and_media/20/04/2018/5ad8c53a9a794723c3f3a270

Kurowska, X., & Reshetnikov, A. (2018). Neutrollization: Industrialized trolling as a pro-Kremlin strategy of desecuritization. *Security Dialogue*, 49(5), 345–363. https://doi.org/10.1177/096701681785102

Kurowska, X., & Reshetnikov, A. (2021). Trickstery: Pluralising stigma in international society. *European Journal of International Relations*, 27(1), 232–257.

Lehtisaari, K. (2020). Formation of media policy in Russia: The case of the Iarovaia law. In M. Wijermars, & K. Lehtisaari (Eds.), *Freedom of expression in Russia’s new mediasphere* (pp. 57–73). Routledge.

Levada Center. (2016, November 18). Doverie SMI i tsenzura. http://www.levada.ru/2016/11/18/doverie-smi-i-tsenzura/

Li, I., Nemchenko, I., & Balashova, A. (2018, April 23). Doguglilis’: kak servis postradal iz-za bor’by Roskomnadzora s Telegram. *RBK*. https://www.rbc.ru/technology_and_media/23/04/2018/5addee179a74976dc5d719f

Lokot, T. (2018a). Be safe or be seen? How Russian activists negotiate visibility and security in online resistance practices. *Surveillance & Society*, 16(3), 332–346. https://doi.org/10.24908/ss.v16i3.6967
Lokot, T. (2018b, November 26). Telegram: What’s in an app? Point & Counterpoint, PONARS Eurasia. http://www.ponarseurasia.org/point-counter/telegram-whats-app

Lokot, T. (2020). Data subjects vs. people’s data: Competing discourses of privacy and power in modern Russia. Media and Communication, 8(2), 314–322. https://doi.org/10.17645/mac.v8i2.2883

Lonkila, M., Shpakovskaya, L., & Torchinsky, P. (2020). The occupation of Runet? The tightening state regulation of the Russian-language section of the Internet. In M. Wijermars, & K. Lehtisaari (Eds.), Freedom of expression in Russia’s new mediasphere (pp. 17–38). Routledge.

Nisbet, E. C. (2015). Benchmarking public demand: Russia’s appetite for Internet control. Internet Policy Observatory. https://global.asc.upenn.edu/app/uploads/2015/02/Russia-Public-Opinion.pdf

Nisbet, E. C., Kamenchuk, O., & Dal, A. (2017). A psychological firewall? Risk perceptions and public support for online censorship in Russia. Social Science Quarterly, 98(3), 958–975. https://doi.org/10.1111/ssqu.12435

Nocetti, J. (2015). Russia’s ‘dictatorship-of-the-law’ approach to internet policy. Internet Policy Review, 4(4), 4. https://doi.org/10.14763/2015.4.380

Pigman, L. (2019). Russia’s vision of cyberspace: A danger to regime security, public safety, and societal norms and cohesion. Journal of Cyber Policy, 4(1), 22–34. https://doi.org/10.1080/23738871.2018.1546884

Reuter. (2020, June 18). Russia lifts ban on Telegram messaging app after failing to block it. https://www.reuters.com/article/us-russia-telegram-ban/russia-lifts-ban-on-telegram-messaging-app-after-failing-to-block-it-idUSKBN23P2FT

Rogers, R. (2020). Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. European Journal of Communication, 35(3), 213–229. https://doi.org/10.1177/0267323120922066

Shehabat, A., Mitew, T., & Alzoubi, Y. (2017) Encrypted Jihad: Investigating the role of Telegram app in lone wolf attacks in the West. Journal of Strategic Security, 10(3), 27–53. https://doi.org/10.5038/1944-0472.10.3.1604

Shen, F. (2017). Internet use, freedom supply, and demand for Internet freedom: A cross-national study of 20 countries. International Journal of Communication, 11, 2093–2114.

Sherstoboeva, E. (2020). Regulation of online freedom of expression in Russia in the context of the Council of Europe standards. In S. Davydov (Ed.), Internet in Russia: A study of the runet and its impact on social life (pp. 83–100). Springer.

Sivetc, L. (2020). The blacklisting mechanism: New-school regulation of online expression and its technological challenges. In M. Wijermars, & K. Lehtisaari (Eds.), Freedom of expression in Russia’s new mediasphere (pp. 39–56). Routledge.

Sobolev, S., & Maliarenko, E. (2019, April 13). Za god blokirovki Telegram ostal’sia v troike samykh poluliarnykh messendzerov. RBK. https://www.rbc.ru/technology_and_media/13/04/2019/5cb19f339a794741a319f84d

Soldatov, O. (2019). Half-hearted inception, miserable existence, and the untimely death of the bloggers’ register in Russia. Israel Law Review, 52(1), 61–75. https://doi.org/10.1017/S0021223718000250

State Duma. (2017, April 10). Zakonoproekt No. 145507-7 ‘O pravovom regulirovanii deiatel’nosti sotsial’nykh setei i o vnesenii izmenenii v otdel’nye zakonodat’el’nnye akty Rossisskoi Federatsii’. https://sozd.duma.gov.ru/bill/145507-7

Tolz, V., & Teper, Y. (2018). Broadcasting agitainment: A new media strategy of Putin’s third presidency. Post-Soviet Affairs, 34(4), 213–227. https://doi.org/10.1080/1060586X.2018.1459023

Van der Vet, F. (2020). Imprisoned for a ‘like’: The criminal prosecution of social media users under authoritarianism. In M. Wijermars, & K. Lehtisaari (Eds.), Freedom of expression in Russia’s new mediasphere (pp. 209–224). Routledge.

Veen, J., & Boeke, S. (2020). No backdoors: Investigating the Dutch standpoint on encryption. Policy & Internet, 12(4), 503–524. https://doi.org/10.1002/poi3.233
Volkov, D., & Goncharov, S. (2020). Rossiiskii medialandshaft – 2020. Levada Center. https://www.levada.ru/2020/04/28/rossijskij-medialandshaft-2020/

VTsIOM. (2017, April 10). Press-vypusk no. 3347. Zabanit’ sotseti?. https://wciom.ru/index.php?id=236&uid=116150

Wijermars, M. (2020a). Memory politics in contemporary Russia: Television, cinema and the state. Routledge.

Wijermars, M. (2020b). The stakes are high for Internet freedom in Russia in 2020. Baltic Rim Economies, (1), 41.

Wijermars, M. (2021). Russia’s law ‘On news aggregators’: Control the news feed, control the news? Journalism. doi:10.1177/1464884921990917

Wijermars, M., & Lehtisaari, K. (2020a). Introduction: Freedom of expression in Russia’s new mediasphere. In M. Wijermars & K. Lehtisaari (Eds.), Freedom of expression in Russia’s new mediasphere (pp. 1–14). Routledge.

Yablokov, I. (2015). Conspiracy theories as a Russian public diplomacy tool: The case of Russia Today (RT). Politics, 35(3–4), 301–315. https://doi.org/10.1111/1467-9256.12097

Yablokov, I. (2018). Fortress Russia: Conspiracy theories in post-Soviet Russia. Polity Press.