COGITATIO

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 2, Pages 314–322
DOI: 10.17645/mac.v8i2.2883

Article

Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia

Tetyana Lokot

School of Communications, Dublin City University, Dublin 9, Ireland; E-Mail: tanya.lokot@dcu.ie

Submitted: 9 February 2020 | Accepted: 5 May 2020 | Published: 23 June 2020

Abstract
The notion of individual privacy has always been a political one throughout Russia's Soviet and post-Soviet periods, but in the age of all-encompassing datafication and digitisation of identities, privacy has become an even more contested concept. This article considers how Russian state officials and Russian digital rights advocates construct the notion of privacy in their public online discourses. I argue that how these actors talk about privacy helps shape the norms and the politics around it in Russia. An in-depth analysis of activity reports published online by the state internet regulator and a grassroots digital rights group reveals competing privacy discourses underpinned by differential understandings of how anonymity, secrecy, confidentiality, and control of personal data determine the distribution of power and agency in Russian public and political life. These differential interpretations of privacy inform the contentious politics that emerge around how privacy is regulated and negotiated within the greater regulatory and normative framework of digital citizenship in Russia. Thus, the article offers critical insights into the contestation of citizenship and, consequently, the distribution of power in more and less democratic systems.

Keywords
data; digital rights; power; privacy; Russia

Issue
This article is part of the issue "The Politics of Privacy: Communication and Media Perspectives in Privacy Research" edited by Johanna E. Möller (Johannes Gutenberg University Mainz, Germany), Jakub Nowak (Maria Curie-Sklodowska University, Poland), Sigrid Kannengießer (University of Bremen, Germany) and Judith E. Möller (University of Amsterdam, The Netherlands).

1. Introduction

With digital technologies and networked internet platforms firmly embedded in the mainstream political and social life, and amid increasing datafication (Mayer-Schönberger & Cukier, 2013; Van Dijck, 2014) of all facets of society and identity, media and communications scholarship is increasingly concerned with how these forces are shaping the distribution of power and agency among the various actors involved in this ecosystem. This study focuses on the notion of privacy in the networked era and the emerging politics around it as closely related to issues of control, power, and agency. Examining the case of Russia, I argue that certain state and non-state actors engage in public discourse to articulate competing conceptions of privacy politics, and that these discursive articulations underpin different visions of how agency, power, and control should be distributed in a datafied society. Capturing these divergent ideas can offer valuable insights about how the state and citizens in Russia—and other networked authoritarian states—understand the meaning of privacy and its place in the emergent construction of digital citizenship.

Section 2 charts the development of the concept of privacy in media and communications scholarship, underscoring the highly contextual, relational, and political nature of privacy in technological systems and mediated environments. This section then discusses the understanding of privacy in the Russian context, and how the concept has evolved from the Soviet era to the modern times. The

study then presents arguments for examining the discursive representations of privacy as a way of understanding the competing politics of privacy in Russia today.

Section 3 briefly introduces the two sources of privacy discourse in this study: the Russian state regulator Roskomnadzor (RKN) and the digital rights group Roskomsvoboda (RKS). It then outlines the collection of publicly available activity and monitoring reports produced by both organisations and describes the approach used to analyse the privacy-related discourses that emerge from these public communications.

Section 4 presents an analysis of how both the state regulator and the digital rights group discursively construct privacy as contextual, relational, and political. The analysis suggests that the discursive representations of privacy by the state regulator and the digital rights activists are in competition with one another, and illustrates how this divergence informs the contentious politics of privacy in Russia.

Lastly, Section 5 presents concluding thoughts about the competing discursive articulations of privacy and the resulting politics of privacy in Russia, as reflected in the state's struggle for control over accessibility of private data and the grassroots resistance against restrictions of personal data flows. The section concludes with suggestions for future research by media and communication scholars into privacy politics and its discursive construction.

2. Articulating Privacy and Its Politics

This section first unpacks how the concept of privacy is discussed in media and communications scholarship. Next, it traces the evolution of the notion of privacy in Russian political and public life. Finally, it argues for the importance of attending to the discursive construction and representation of privacy by state and non-state actors as a vital force that shapes the politics of privacy in the Russian national context.

2.1. The Concept of Privacy in Media and Communications Scholarship

Pinning down the exact definition or nature of privacy as a concept is an ongoing struggle within media and communications scholarship (and, for that matter, in other disciplines as well). Nissenbaum (2010, p. 2) suggests it is less useful to grasp whether privacy is "a claim, a right, an interest, a value, a preference, or merely a state of existence" than to trace the concerns related to privacy with regard to technological systems and digitally-mediated practices related to flows of personal information. Rather than arguing for privacy to be understood as a purely descriptive, normative, or legal concept, it seems more productive to examine how certain descriptions of privacy, norms, or regulations around it engender anxiety, resistance, or struggle for control over accessibility and/or restrictions of personal data flows.

Following Nissenbaum's (2010) logic, Möller and Nowak (2018) suggest that privacy can be best understood as contextual, relational, and political. They argue that in line with Nissenbaum's (2010) idea of "contextual integrity," privacy is best conceptualised and reconceptualised with regard to specific contexts. Further, privacy is not only understood in relation to individuals, but is realised or threatened as a constant process of strategic determination (Trepte et al., 2017; Westin, 2015) with regard to how their personal information flows between them and other individuals and institutions in society (Möller & Nowak, 2018). In this regard, privacy can also be understood as relational because it relates to and is informed by a multitude of other issues, from surveillance and control to anonymity, confidentiality, and security. Finally, privacy can be understood as political or participatory (Möller & Nowak, 2018), as increasingly privacy-related decisions and activity impact other actors in any individual's networks, and have implications for political participation, individual safety of dissidents (when coupled with surveillance), and the overall climate of political freedom and expression—or lack thereof—in both democratic and non-democratic societies. I posit, therefore, that the contextual and relational articulations of the politics of privacy are intrinsically connected to broader issues of power, agency, and control in the framework of digital citizenship as it is understood and performed by various actors, including states, platforms, media, and citizens.

2.2. Privacy in Russia's Networked Authoritarian State

The notion of individual privacy has always been a political one throughout Russia's Soviet and post-Soviet periods, connected as it was to the culture of pervasive state surveillance (Lokot, 2018) and the struggle to control thoughts, opinions, and information flows in both public and private lives of citizens (Gorny, 2007). Reflecting on the Bolsheviks' view that anything private was deprived of social meaning and thus politically dangerous, Boym (1994, p. 73) concludes that in early Soviet Russia "personal life seems rather to fit a concept of publicly sanctioned guilt and of a heightened sense of duty." However, in the age of all-encompassing datafication and digitisation of identities, privacy has become an even more contested concept in Russia, given the citizens' embrace of digital technologies and the state's preoccupation with control over data and information flows as part of the national security and sovereignty project. This has led to the emergence of what Greene (2012, after MacKinnon, 2011) terms 'networked authoritarianism': a regime in which the state prioritises developing networked infrastructure and digital connectivity, while seeking to control all spheres of the datafied social life.

The term 'privacy' itself (*приватность* [privatnost] in Russian) is a term clearly borrowed from other languages (Levontina, Shmelev, & Zaliznyak, 2017) and a fairly recent addition to everyday Russian vocabulary,

though other partial representations of it such as confidentiality, secrecy, and 'private life,' predate it (Boym, 1994). But privacy in the modern sense, including the privacy of personally identifying information, individual communications, behaviour, and digital data traces, is only now entering the mainstream legal, political, and social discourse in Russia. In legislative terms, for instance, this has meant that the traditional repertoire of legal protections for confidentiality of private communications and 'private life' has been expanded to include personal data protection (e.g., Federal Law "On Personal Data" [Russian Federation, 2006])—but also that access to user data and metadata stored by online entities and social media platforms is viewed by the state and law enforcement as a matter of national security (Soldatov & Borogan, 2013), while citizens increasingly perceive state policies in the area of data localisation (Sargsyan, 2016) and internet sovereignty (Lipman & Lokot, 2019) as threats to individual privacy. It is therefore important to investigate the competing representations of this concept in the Russian discursive public sphere and to capture how these competing forces in the field of privacy might reflect the overarching power struggles in society and represent competing ideas of the political power of the state and its citizens, spanning from hegemony to democracy.

2.3. Discursive Constructions of Privacy

This article considers how the Russian state and Russian digital rights advocates construct competing notions of privacy in their public-oriented discourses. Subscribing to a post-structuralist, critical approach that sees discourses as never separate from reality, but possessing the power to co-create it (Fairclough, 2013), I argue that how these actors conceptualise and contextualise privacy in their communications with the public helps shape the politics around privacy in Russia. An in-depth analysis of the text corpora of regularly published activity and monitoring reports by the state internet regulator and one of Russia's most prominent grassroots digital rights groups points to competing privacy discourses, concerned with questions of how privacy is understood, what value it possesses, and how it is conveyed, controlled, or restricted. The discursively constructed politics of privacy, I argue, are underpinned by differential understandings of how anonymity, secrecy, confidentiality, and control of personal data determine the distribution of power and agency in Russian public life.

In addition to being an empirical study of the Russian context that contributes to Russia-focused literature on internet governance and free expression online, this article applies the analytical privacy framework developed by Möller and Nowak (2018) to discursive constructions of privacy. It thus aims to make a novel theoretical contribution to the media and communications scholarship on privacy by articulating the connections between how the politics of privacy is represented discursively and how its divergent representations shape internet regulation, freedom of expression online, and digital citizenship in Russia.

3. Research Design and Methods

Though specific legislative, political, and other practices on the part of the state and the digital rights activists may point to the competing notions of privacy in Russia, it is equally important to examine how state and civic actors articulate these ideas in discursive terms in digitally-mediated spaces. Therefore, I chose to examine publicly available activity reports produced by Russia's state internet regulator, RKN, and by RKS, one of Russia's most prominent digital rights groups, to understand how these communications are used to shape discursive representations of privacy.

RKN (also known as the Federal Service for Supervision of Communications, Information Technology and Mass Media) is the Russian federal executive body tasked with oversight, monitoring and censorship of electronic media, mass communications, information technology, and telecommunications (Turovsky, 2015). It operates as an independent agency under the auspices of the Ministry of Digital Development, Communications, and Mass Media. RKN oversees compliance with relevant Russian legislation and manages Russia's extensive banned websites registry.

The grassroots digital rights initiative whose privacy-related discourses I examine is RKS, one of the main digital rights advocacy groups in Russia. It was founded in 2012 by members of the Pirate Party in Russia (Merzlikin, 2019) to address the early crackdown on internet freedoms that has since escalated. Initially monitoring the Russian state internet blacklist, RKS has since expanded its remit to digital literacy work, online privacy and security workshops, advocacy campaigns for internet freedom and digital rights, and even offering legal assistance to Russian citizens prosecuted for internet activity.

I collected publicly available Russian-language activity reports from the official websites of the two organisations (https://rkn.gov.ru and https://roskomsvoboda.org), published between the start of 2015 and the start of 2019, a period of turbulent change in Russia's digital society and its governance. These reports (annual in the case of RKN, monthly in the case of RKS) represent key issues and activity performed or overseen by these actors in conjunction with their work. As these reports are regular, structured and explicitly aimed at disclosure for public consumption, they present a useful source of discourse about issues related to digital rights and privacy more specifically. For each organisation, I also collected the text from their 'About' or 'Mission' sections to capture how each organisation articulates its mission and objectives in the context of their work. Sampling their discourses in this way allows to capture fairly recent, but also regular and well-structured discourse relating to digital rights, communication, and information, and to locate any references to privacy therein. The discur-

sive representations of privacy stemming from the analysis of these text corpora can then be connected to specific activity, showing how the competing politics of privacy shape state regulations, policy interventions, and activist efforts.

I collated the texts collected from each source into two text corpora. The resulting corpora contain 157,912 words (RKN) and 158,905 words (RKS), respectively. The RKN corpus contains text from five annual reports (154,584 words) and text from the 'About' page of RKN's website (3,328 words). The RKS corpus contains text from 54 monthly reports (158,743 words) and text from the 'Our Mission' page of RKS's website (162 words). I then used AntConc (Anthony, 2019), a freeware tool for conducting corpus linguistics and concordance analysis on large volumes of text, and specifically its 'Concordance' tool. A concordance is a commonly used display format in corpus linguistics similar to a table that shows instances of a selection of words in their context. I focused on concordances of specific words commonly used in privacy discourses—in this case the lemmas 'privacy' (*приватность* [privatnost], noun), 'private' (*приватный* [privatnyy] or *частный* [chastnyy], adjective), and 'personal' (*персональный* [personalnyy] or *личный* [lichnyy], adjective)—to uncover the semantic context in which they are most commonly used by each actor. Lemmas were used in order to capture all possible word endings and word forms in Russian.

AntConc has been used previously in communications, media, and policy research outside of corpus linguistics (e.g., Baker & McEnery, 2015; Fairclough, 2016; Lokot & Diakopoulos, 2016). Likewise, privacy and surveillance studies have often relied on discourse analysis to capture how public debates around privacy norms develop (e.g., Cichy & Salge, 2015; Möllers & Hälterlein, 2013). While the use of corpora in discourse analysis is well-documented (e.g., Baker, 2006), in this study a corpus linguistics tool was used primarily in order to reveal how privacy is discursively constructed by each organisation and how these discourses around privacy diverge. The frequency of specific words in this context was of less importance than the discourses that emerged around the privacy-related keywords in the RKN and RKS corpora. Therefore, though raw and relative frequencies for key terms are provided throughout, the analysis in this study is mostly qualitative in nature and examines the semantic fields (Fairclough, 2016) associated with the occurrence of privacy-related keywords in each corpus via their clusters, collocates, and concordances. Relevant examples from the text corpora provided in the article have been translated into English by the author.

4. Findings: Competing Discursive Constructions of Privacy

The raw (F_O) and relative (normalised, F_N) frequencies of the privacy-related keywords (lemmas) in both text corpora are presented in Table 1.

4.1. RKN

A key observation from the RKN corpus is that the state regulator never once uses the more modern Russian term 'privacy' (*приватность*)—instead, the term of choice is the more commonly used 'private life' (*частная жизнь* [chastnaya zhyzn]; $F_O = 76$ per 157,912 words, $F_N = 4.812807133$), along with terms such as 'personal' or 'family' used to denote personal or private contexts. Another notable observation is the coupling of 'inviolability' (*неприкосновенность* [neprikosnovennost]) with the context of privacy and private information (collocation frequency with 'private' within five words to the left or right at $F_O = 16$ per 157,912 words, $F_N = 1.013222554$)—this is not surprising, as these terms are often co-located in Russian legal parlance in information- and privacy-related contexts. An example of such collocation can be found in RKN's 2017 annual report, where the state blocked website registry is described as: "A regulatory instrument unique to international law that allows to protect the rights of Russian citizens to inviolability of their private life, their personal and family secrecy" (RKN, 2018, author's translation).

The state regulator's public communications discuss privacy in a predominantly instrumental context, referring to the 'personal data' of individuals ($F_O = 599$ per 157,912 words, $F_N = 37.932519378$), but rarely discussing individuals as active agents exercising their rights or freedoms. The focus is overwhelmingly on what is being done to the individual/user, rather than on their own actions: i.e., their private life is protected (by the state), and their personal data is collected and stored (by the state or third parties).

In its 2015 annual report, RKN describes a state official from the President's Office speaking at an RKN committee meeting and stressing that: "The main priority for state oversight and protection of personal data should be…the provision of individual security without infringing on private life" (RKN, 2016, author's translation).

Table 1. Raw and relative keyword frequencies in the RKN and RKS text corpora.

Keyword	RKN F_O	RKN F_N *	RKS F_O	RKS F_N *
Privacy	0 per 157,912	0	29 per 158,905	1.824989774
Private	79 per 157,912	5.002786362	288 per 158,905	18.124036374
Personal	645 per 157,912	40.845534222	334 per 158,905	21.648154558

Note: * Relative frequency F_N per 10,000 words.

These instances point to the preoccupation of the state with monitoring citizen online activity, establishing blanket digital surveillance, and ensuring ad-hoc access to personal information flows, while seeking to shield it from external actors.

Individual rights to privacy are framed in RKN's discourse as rights of 'personal data subjects,' reinforcing the instrumental context of state-controlled subjects generating data. In the RKN corpus, discourse related to 'defence' and 'protection' tends to be clustered together with 'personal' data of subjects and not with discussion of their individual privacy. For instance, in its 2018 annual report, RKN elaborates on practical and preventative measures implemented that year and, among other activities, boasts that: "The greatest number of preventative training events was held in the area of personal data protection—12,579 activities in total" (RKN, 2019, author's translation).

In a similar activity summary in the 2017 annual report, RKN reports that: "Greater attention was given to events aimed at school pupils and students in order to cultivate a culture of care with regard to their personal data" (RKN, 2018, author's translation).

This discursive instrumentalisation of privacy extends from protecting copyright and intellectual property to personal data to defending the interests of the Russian state in cyberspace. In all of these cases, the object being protected is either information or the state, and not the privacy of individuals.

The privacy-adjacent discourse around security and safety in the text corpus further confirms this: The RKN corpus clusters 'digital security' alongside 'personal data protection' and 'safe online behaviour'. The focus is on a secure and safe environment and data, as well as law and order, rather than on the individual and their privacy choices. In the 2018 report, the state regulator explicitly states: "In the context of the global transformation of the information world order, we see [our] main goal as ensuring security and protection for society and citizens from relevant cyberthreats" (RKN, 2019, author's translation).

Thus, individual privacy and privacy of personal data flows is predominantly contextualised by RKN as a matter of national security and presented as a function of the sovereign state retaining control over information and data of its 'subjects' to protect them against external threats.

4.2. RKS

Unlike the state regulator, RKS readily uses both 'privacy' and 'private' (in both its traditional and modern forms) in its public discourse online (see Table 1 for frequencies). In the RKS corpus, these terms most commonly co-occur with 'rights' (collocation frequency with 'privacy/private' within five words to the left or right at $F_O = 42$ per 158,905 words, $F_N = 2.643088638$), life (collocation frequency with 'privacy/private' within five words to the left or right at $F_O = 42$ per 158,905 words, $F_N = 2.643088638$), 'information' (collocation frequency with 'privacy/private' within five words to the left or right at $F_O = 22$ per 158,905 words, $F_N = 1.384475001$), 'inviolability' (collocation frequency with 'privacy/private' within five words to the left or right at $F_O = 10$ per 158,905 words, $F_N = 0.629306819$), 'data' (collocation frequency with *privacy/private* within five words to the left or right at $F_O = 10$ per 158,905 words, $F_N = 0.629306819$), and 'personal' (collocation frequency with 'privacy/private' within five words to the left or right at $F_O = 8$ per 158,905 words, $F_N = 0.503445455$), as well as in the context of protecting privacy and anonymity of users.

In its mission statement (RKS, 2019, author's translation), the digital rights organisation describes its aims in the following way: "Roskomsvoboda organises broad public campaigns and supports civic initiatives in favour of freedom of information and inviolability of the personal data of users."

In contrast to the state discourse, privacy in the discourse of digital rights activists is more closely connected to the rights and interests of individual citizens. Throughout the RKS corpus, RKS often refers to 'your privacy' (two-word cluster $F_O = 13$ per 158,905 words, $F_N = 0.818098864$) or 'their privacy' (two-word cluster $F_O = 9$ per 158,905 words, $F_N = 0.566376137$), drawing direct connections between the individual and their work. For instance, in a January 2015 monthly report, the organisation notes their legal director, Sarkis Darbinyan, participated in a seminar on internet regulation in the Russian city of Voronezh: "Darbinyan presented a short summary of technologies that help users, website owners and journalists circumvent the blocking of Internet resources and preserve their privacy online by using new digital rights such as the right to anonymity and encryption" (RKS, 2015a, author's translation).

The privacy-related discourse of RKS is more concerned with agency in the sense that privacy is presented as something the individual or the user can achieve or preserve, as opposed to something that the individuals are granted by some external power. In this regard, RKS regularly references specific tools that individual users can avail of to exercise and protect their privacy, including virtual private networks (VPNs), the TOR browser (a tool that camouflages users' IP addresses), and various encrypted communication options. In its June 2015 monthly report, RKS references a recent intervention discussing the advantages of using the TOR browser in the context of growing restrictions imposed by the Russian government on the online sphere: "We saw a sharp uptick in TOR browser use, because the new reality pushes people to search for new solutions so they can access their favourite websites. In addition, TOR can ensure your privacy online" (RKS, 2015b, author's translation).

Importantly, the RKS discourse links privacy to specific rights of networked citizens, such as anonymity, secrecy, unhindered distribution of information, access to digital networks, and encryption. In a public lecture on

digital rights for students, trainee lawyers and civic activists in Moscow, held in September 2015 and mentioned in the monthly report for the same period, a representative for RKS underscored that:

> Protecting the rights and freedoms of a person in an online environment is just as important as in everyday life, and you should not forfeit your rights to privacy, security and freedom to obtain and disseminate information under any circumstances. (RKS, 2015c, author's translation)

In their reports, digital rights activists discuss examples of user activity on specific platforms, such as Telegram, and refer to personal data and user identification in the context of these cases. For instance, in December 2017 RKS reports on a new 'Battle for Telegram' campaign it launched in support of the Telegram messenger, which was facing pressure from the Russian government to share user information and encryption keys: "If we do not protect this internet service that cares about the privacy of our data today, Russian users may become an easy target for cybercriminals and illegal actions on the part of the state institutions" (RKS, 2017b, author's translation).

When discussing the need to protect individual privacy and personal data flows, RKS unambiguously points to the Russian state as the main threat against which privacy must be protected. In multiple instances, the activists critique new and upcoming internet regulations developed by the state, such as the 'anti-extremist' Yarovaya law (Luganskaya, 2017). As observed in the December 2016 monthly report summarising key developments in Russian internet regulation in 2016 (RKS, 2016b, author's translation), RKS experts see the Yarovaya law as "eradicating privacy by default" for Russian internet users. Thus, the notion of personal information security is presented in terms of what citizens can do to protect their privacy online, and how this individual agency is contested by the state as part of its national security discourse.

As an activist and advocacy organisation, RKS sees its mission as more than offering legal defence and technological solutions (such as their VPN Love project recommending verified VPN services). Crucially, activists also promote individual agency by asking the users to defend themselves from state surveillance and fight for their privacy. This is supported by RKS's own initiatives, such as the SAFE Project announced in January 2017 and aimed at educating the public about a range of anti-surveillance and privacy tools: "Roskomsvoboda is launching a new resource—Project SAFE—about self-defence tools for internet users to protect themselves from surveillance and intrusions into their personal data and correspondence" (RKS, 2017a, author's translation).

Privacy-related agency, the activists argue, can be achieved through increased public debate and digital literacy, and this aligns with their advocacy efforts aimed at giving the users more control over their information and online presence. These efforts include public documentation of state persecutions against internet users, disseminating detailed instructions on how to appeal internet-related charges, and developing practical tips on protecting oneself from digital surveillance. As RKS notes in its mission statement on its website: "Our aim is for every RuNet [Russian Internet] user to be able to defend their [digital] rights" (RKS, 2019, author's translation).

4.3. Privacy: Contextual, Relational, and Political

In both the state regulator's and the digital rights activists' public online discourses, privacy is constructed as contextual, relational, and political. However, these articulations diverge greatly in terms of the normative foundations on which they are constructed. The discursive divergence also extends to how privacy is reflected and enacted by both the state and activists in terms of policy, regulations, and sanctions, as well as in terms of grassroots action, digital literacy efforts, and digital rights initiatives.

As a state institution, RKN interprets privacy of individual data and information flows predominantly in the context of Russia's national security and digital sovereignty concerns. In this almost geopolitical view, individuals are viewed not as independent agents empowered to protect their own private lives, but as 'personal data subjects' of the state, whose data require state protection, regulation, and control. This contextual interpretation of privacy is reflected in the Russian regulatory landscape over the past decade: Legislative acts such as the Yarovaya law (Luganskaya, 2017) and the internet sovereignty law (Lipman & Lokot, 2019) approach internet governance, online safety, privacy, and personal information as matters of national security, while the power to regulate and protect resides in the hands of state institutions. Privacy, therefore, emerges as a relational concept wherein the institutions of the state, be they telecom regulators such as RKN or law enforcement bodies, are involved in mediating and enabling individual private life, while also remaining constantly in control of personal data flows and in possession of access to individual data and metadata of Russian citizens. As the state and its institutions see themselves as granting privacy to citizens, they also conclude that they have the power and the right to grant or withhold privacy. This is reflected in the multiple instances of arbitrary requests for user data from social media platforms (Gadde, 2019; Lokot, 2016), alleged violations of privacy against opposition activists (Seddon, 2016), and the selective application of legal norms to persecute users for online expression (Mostovshchikov, 2015). This ongoing struggle for control over the field of privacy (with foreign governments, platforms, and users themselves) renders privacy as a clearly political issue for the Russian networked authoritarian state. However, the politics here is that of a hegemonic state that seeks to preserve the status quo

and to retain its power over information and data flows at the cost of the individual agency of its citizens.

In contrast, digital rights activists at RKS view privacy in the context of digital rights and freedoms and discursively present it as a key individual right in the digital age. For RKS, privacy is a key expression of individual agency as it is something each person can achieve or protect if given the proper tools and knowledge. This is reflected in RKS's digital literacy initiatives such as Project SAFE (described in Section 4.2 above). The activists also construe of privacy as relational, but in a different sense: For them, the struggle is that of the individual user attempting to wrestle the privacy of their data and their personal security from the grasp of the state. This is why RKS and their allies launch and maintain grassroots campaigns in support of privacy-enabling platforms such as Telegram (Novaya Gazeta, 2017) or in defence of individuals persecuted by the state for using privacy and anonymity tools, such as Russian TOR relay node operator Dmitry Bogatov (Gilmour, 2017). Though privacy-enhancing technologies are seen as beneficial in terms of user agency in general, it is the state that is seen as the biggest threat in the conditions of Russia's networked authoritarianism. In this respect, RKS also intervenes in the development and implementation of internet and privacy regulations, submitting opinions on new initiatives it believes to threaten privacy such as facial recognition systems (Kornya, 2019) and contesting legal sanctions impinging on user privacy in court (RKS, 2020).

In the circumstances of diminishing space for free expression and genuine political participation, digital rights activists promote a political articulation of privacy as a crucial condition of individual freedom to exercise political agency and to renegotiate the balance of power—both power writ large and power over the private lives of individuals—with the dominant governing regime. The activist politics of privacy, therefore, is aimed at the transformation of the status quo and at bringing about change at the grassroots level.

5. Conclusion: Data Subjects vs. People's Data

This study examines the discursive representations of issues surrounding privacy by the Russian state internet regulator RKN and by digital activist group RKS, and uses this discursive analysis to highlight relevant concerns in the Russian public sphere with regard to technological systems and digitally-mediated practices related to flows of personal information. This study contributes to the existing scholarship on internet governance and digital rights and offers critical insights into how privacy politics informs the contestation of citizenship and, consequently, the distribution of power in different kinds of democratic systems, including hybrid regimes such as Russia. The study also makes a contribution to the scholarship on privacy politics in media and communications research by using corpus linguistics tools for privacy-related discourse analysis.

Though both the state telecom regulator and the activists construe privacy as contextual, relational, and political, their interpretations of privacy and their privacy politics diverge significantly. By examining the articulations of the concerns, norms and regulations around privacy by the state institutions and grassroots digital rights advocates, I show how the struggle for control over accessibility of private data and resistance against restrictions of personal data flows lead to two different concepts of the politics of privacy in Russia.

I find that the networked authoritarian Russian state 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. On the other hand, Russian digital rights activists advocate for privacy as a human right and argue that technologies such as encryption and VPNs should be widely adopted by citizens to preserve their agency and protect their data and identities from the state. These tensions between interpretations of privacy by the Russian state and Russian citizens inform how privacy is negotiated as part of the ongoing political dissent and the struggle over divergent political visions of Russian society.

The differential understandings of how anonymity, secrecy, confidentiality, and control of personal data determine the distribution of power and agency in Russian public and political life shape the resulting politics of privacy in Russia, as reflected in the state's struggle for control over accessibility of private data and the grassroots resistance against restrictions of personal data flows. These divergent politics are reflected in privacy-related policing and control on the part of the state, and in privacy-related advocacy, activism, and digital literacy initiatives of activist groups. Amid the precarity of online expression and the struggle for control over personal data flows, the ongoing contestation of privacy-related power has implications for what kind of political future Russian citizens might anticipate: one where they are 'data subjects' at the mercy of a hegemonic state or one where their privacy enables greater political agency and allows them to refashion society towards a more equal, democratic, and rights-based vision.

Beyond Russian borders, many former Soviet states that Russia counts within its sphere of influence are closely watching the developments in internet governance and digital identity policies developed and contested in Russia. Further research by media and communication scholars focusing on Central and Eastern Europe should therefore examine the possible repressive or democratising impact of the discursively contested articulations of privacy politics in Russia on its neighbour states. Related research could also examine the overlaps and divergences of emergent privacy politics within EU states and within Russia, in light of the recent adoption of the General Data Protection Regulation and greater attention to personal data protection and privacy concerns.

Acknowledgments

This article was made possible with support from the 2019–2020 Journal Publication Scheme of the Faculty of Humanities and Social Sciences, Dublin City University.

Conflict of Interests

The author declares no conflict of interests.

References

Anthony, L. AntConc (Version 3.5.8) [Computer software]. (2019). Tokyo: Waseda University. Retrieved from https://www.laurenceanthony.net/software

Baker, P. (2006). *Using corpora in discourse analysis*. London: Continuum.

Baker, P., & McEnery, T. (2015). Who benefits when discourse gets democratised? Analysing a Twitter corpus around the British Benefits Street debate. In P. Baker & T. McEnery (Eds.), *Corpora and discourse studies* (pp. 244–265). London: Palgrave Macmillan.

Boym, S. (1994). *Common places: Mythologies of everyday life in Russia*. Cambridge, MA: Harvard University Press.

Cichy, P., & Salge, T. (2015). The evolution of privacy norms: Mapping 35 years of technology-related privacy discourse, 1980–2014. In *Proceedings of the Thirty Sixth International Conference on Information Systems* (pp. 1–13), Fort Worth, TX: Association for Information Systems.

Fairclough, I. (2016). Evaluating policy as argument: The public debate over the first UK austerity budget. *Critical Discourse Studies*, *13*(1), 57–77.

Fairclough, N. (2013). Critical discourse analysis. In J. P. Gee & M. Handford (Eds.), *The Routledge handbook of discourse analysis* (pp. 9–20). Oxford: Routledge.

Gadde, V. (2019). Key data and insights from our 14th Twitter transparency report. *Twitter Blog.* Retrieved from https://blog.twitter.com/en_us/topics/company/2019/key-data-and-insights-from-our-14th-twitter-transparency-report.html

Gilmour, D. (2017, April 26). Russian Tor relay operator facing terrorism charges. *Daily Dot*. Retrieved from https://www.dailydot.com/debug/russian-tor-relay-operator-facing-terrorism-charges

Gorny, E. (2007). *The Russian internet: Between kitchen-table talks and the public sphere*. Boston, MA: Art Margins.

Greene, S. (2012). *How much can Russia really change? The durability of networked authoritarianism*. Washington, DC: PONARS Eurasia.

Kornya, A. (2019, October 6). Moskvichka prosit sud zapretit' raspoznavaniye lits gorodskoy sistemoy videonablyudeniya [Muscovite asks court to ban facial recognition by city CCTV system]. *Vedomosti*. Retrieved from https://www.vedomosti.ru/politics/articles/2019/10/06/812955-moskvichka-prosit-sud

Levontina, I., Shmelev, A., & Zaliznyak, A. (2017). *Konstanty i peremennye russkoy yazykovoy kartiny mira* [The constants and variables of Russian language world view]. Moscow: Litres.

Lipman, M., & Lokot, T. (2019). Disconnecting the Russian internet: Implications of the new "digital sovereignty" bill. *PONARS Eurasia.* Retrieved from http://www.ponarseurasia.org/point-counter/article/disconnecting-russian-internet-implications-new-digital-sovereignty-bill

Lokot, T. (2016, March 6). Twitter reports massive increase in Russian government's content removal requests. *Global Voices*. Retrieved from https://globalvoices.org/2016/03/06/twitter-reports-massive-increase-in-russian-governments-content-removal-requests

Lokot, T. (2018). Be safe or be seen? How Russian activists negotiate visibility and security in online resistance practices. *Surveillance & Society*, *16*(3), 332–346.

Lokot, T., & Diakopoulos, N. (2016). News bots: Automating news and information dissemination on Twitter. *Digital Journalism*, *4*(6), 682–699.

Luganskaya, D. (2017, April 23). Open economy: Kak rossiyskiye vlasti budut kontrolirovat' internet. Tri osnovnykh sposoba [Open economy: How the Russian authorities will control the internet. Three main ways]. *Open Russia*. Retrieved from https://openrussia.org/notes/708721

MacKinnon, R. (2011). Liberation technology: China's "networked authoritarianism." *Journal of Democracy*, *22*(2), 32–46.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Dublin: Houghton Mifflin Harcourt.

Merzlikin, P. (2019, April 18). 'In a perfect world, we just wouldn't exist' How Roskomsvoboda became the primary force standing between the Russian government and Internet censorship. *Meduza*. Retrieved from https://meduza.io/en/feature/2019/04/19/in-a-perfect-world-we-just-wouldn-t-exist

Möller, J. E., & Nowak, J. (2018). Surveillance and privacy as emerging issues in communication and media studies: An introduction. *Mediatization Studies*, *2*, 7–15.

Möllers, N., & Hälterlein, J. (2013). Privacy issues in public discourse: The case of "smart" CCTV in Germany. *Innovation: The European Journal of Social Science Research*, *26*(1/2), 57–70.

Mostovshchikov, E. (2015, February 9). 'There's no such thing as an accidental repost' How Russia punishes people for likes, retweets, and selfies. *Meduza*. Retrieved from https://meduza.io/en/feature/2015/02/09/there-s-no-such-thing-as-an-accidental-repost

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Novaya Gazeta. (2017, December 21). V Rossii zapustili kampaniyu dlya podachi kollektivnoy zhaloby "Telegram protiv FSB" ["Telegram vs. FSB" campaign launched in Russia for collective appeal]. *Novaya Gazeta*. Retrieved from https://novayagazeta.ru/news/2017/12/21/138115-v-rossii-zapustili-kampaniyu-dlya-podachi-kollektivnoy-zhaloby-telegram-protiv-fsb

Roskomnadzor. (2016). *Publichnyy doklad za 2015 god* [2015 annual public report]. Moscow: Roskomnadzor. Retrieved from https://rkn.gov.ru/docs/docP_1485.pdf

Roskomnadzor. (2018). *Publichnyy doklad za 2017 god* [2017 annual public report]. Moscow: Roskomnadzor. Retrieved from https://rkn.gov.ru/docs/doc_2326.pdf

Roskomnadzor. (2019). *Publichnyy doklad za 2018 god* [2018 annual public report]. Moscow: Roskomnadzor. Retrieved from https://rkn.gov.ru/docs/doc_2406.pdf

Roskomsvoboda. (2015a). Roskomsvoboda prinyala uchastiye v seminare po pravovomu regulirovaniyu I problemam rasprostraneniya informatsii v Seti [Roskomsvoboda participates in seminar on legal regulation and issues of information distribution online]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/10202

Roskomsvoboda. (2015b). Master-klass Roskomsvobody: Internet I zakon. Prava, obyazannosti I otvetstvennost v onlayne [Roskomsvoboda master-class: Internet and the law. Rights, obligations and responsibilities online]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/11869

Roskomsvoboda. (2015c). Roskomsvoboda provela seminar dlya yuristov-volontyorov I aktivnykh grazhdan: Prava pol'zovatelya v Internete [Roskomsvoboda holds seminar for volunteer lawyers and active citizens: User rights on the internet]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/12894

Roskomsvoboda. (2016b). Itogi gosregulirovaniya interneta v Rossii v 2016 godu [Summary of state internet regulation in Russia in 2016]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/24592

Roskomsvoboda. (2017a). Proyekt SAFE: Zashchiti sebya ot slezhki [SAFE Project: Protect yourself from surveillance]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/24961

Roskomsvoboda. (2017b). Roskomsvoboda zapustila obshchestvennuyu kampaniyu "Bitva za Telegram" [Roskomsvoboda launches public campaign "Battle for Telegram"]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/34243

Roskomsvoboda. (2019). Proekty [Projects]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/projects

Roskomsvoboda. (2020). TgVPN i РосКомСвобода obzhaluyut deystviya rossiyskikh gosorganov v ESPCH [TgVPN and Roskomsvoboda to appeal Russian state institutions' actions in ECHR]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/54384

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication*, *10*, 2221–2237.

Seddon, M. (2016, May 6). Activists say Russian telecoms group hacked Telegram accounts. *Financial Times*. Retrieved from https://www.ft.com/content/74d5ce00-12dd-11e6-839f-2922947098f0

Soldatov, A., & Borogan, I. (2013). Russia's surveillance state. *World Policy Journal*, *30*(3), 23–30.

Russian Federation. (2006). *Federalnyy zakon "O personal'nykh dannykh"* [Federal law "On personal data"] (N 152-FZ). Moscow: Russian Federation. Retrieved from https://www.consultant.ru/document/cons_doc_LAW_61801

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society*, *3*(1), 1–13.

Turovsky, D. (2015, August 13). This is how Russian Internet censorship works. *Meduza*. Retrieved from https://meduza.io/en/feature/2015/08/13/this-is-how-russian-internet-censorship-works

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

Westin, A. F. (2015). *Privacy and freedom*. New York, NY: IG Publishing.

About the Author

Tetyana Lokot is an Assistant Professor at the School of Communications, Dublin City University. She has been researching activism, protest, internet governance, and censorship on the Cyrillic web for over a decade. Tetyana's work has been published in *Information, Communication and Society*, *Surveillance and Society*, *International Journal of Communication*, and *Digital Journalism*, and presented at international academic conferences. She is currently working on a book about protest and digital media in Ukraine and Russia.