SI: Below the Radar: Private Groups, Locked Platforms and Ephemeral Content

SM+S
social media + society

Social Media + Society
October-December 2020: 1–12

DOI: 10.1177/2056305120984459
journals.sagepub.com/home/sms
SAGE

Articulating Networked Citizenship on the Russian Internet: A Case for Competing Affordances

Tetyana Lokot

Abstract

The Russian government's crackdown on free speech online has seen social media users jailed and fined for publishing critical content. Digital rights activists have cautioned Russians to delete their accounts on platforms that cooperate with law enforcement, but also have advocated for the use of privacy and secure tools. How do these actions inform emergent articulations of networked citizenship in Russia? Using activity reports published online by the state Internet regulator and two digital activist groups, I conduct a narrative analysis of how both parties interpret networked citizenship. I find that the networked authoritarian Russian state embraces the ideal of the *dutiful networked citizen* online as visible, vulnerable, and controlled, exploiting the melding of public and private aspects of networked publics. Instead, Russian digital rights activists advocate for a *self-actualizing networked citizen* who exercises agency online by becoming less visible, often ephemeral, and therefore, more secure. This reinterpretation contests the traditional affordances of networked publics and questions conventional ideas of citizenship, agency, and digital rights in the context of non-democratic societies.

Keywords

digital rights, networked citizenship, Russia, affordances

Introduction

The digitally mediated reality offers a number of affordances to social media users for communication, self-expression, and exercising political agency through the use of social media platforms, messaging services, and other networked technologies. But these affordances are not always possibilities for action: often, they can limit the potential for empowering citizens, as governments seek to use digital media to reaffirm their control over the public sphere. These socially mediated affordances and limitations contribute to the diverging definitions of citizenship in increasingly digitized societies where contestation of power occurs in the entanglement of offline and online spaces. This article focuses on understanding how the work of Russian digital rights advocates contests the concept of digital or networked citizenship in Russia's conditions of networked authoritarianism (Maréchal, 2017).

The Russian government's ongoing crackdown on free speech online has seen social media users jailed and fined for publishing critical content (Mostovshchikov, 2015). Many RuNet users today see the classical affordances of networked publics—permanence, searchability (boyd, 2010), and visibility (Pearce et al., 2018)—as threats to their freedom and their livelihood. This narrowing of free space for critical debate has also led activists to seek out less visible and more ephemeral means of exercising their citizen agency. Digital rights activists are now promoting widespread use of secure tools, such as virtual private networks (VPNs), proxy servers, or encrypted messaging (Merzlikin, 2019). Increasingly, Russians are taking their political discourse to messaging platforms such as Telegram, Signal, and WhatsApp that offer encrypted chatting and disappearing messages (Akbari & Gabdulhakov, 2019). There is also a trend of activists moving to host their websites on servers based in other jurisdictions to make their work less susceptible to Russian state censorship and blocking (Ermoshina & Musiani, 2017). In view of all this, I argue that Russian digital activists seek to redefine the affordances of social media for active networked citizenship.

Dublin City University, Ireland

Corresponding Author:
Tetyana Lokot, School of Communications, Dublin City University, Glasnevin, Dublin 9, Ireland.
Email: tanya.lokot@dcu.ie

In this article, I provide background on the current state of Internet freedom and digital rights in Russia. I then discuss the emergent notion of networked citizenship, drawing on relevant literature about theories of citizenship as well as more recent scholarship on digital rights and digital citizenship. The affordances of networked publics and social media platforms for communication, civic participation, and discontent emerge as a useful lens for understanding how both the Russian state and Russian activists conceptualize the idea of a networked citizen.

I collate and examine text corpora of regular activity and monitoring reports by the Russian state media and Internet regulator, Roskomnadzor, and by key Russian digital rights groups, Roskomsvoboda and Internet Protection Society (OZI). Using the reports published on their official websites in 2015–2019, I conduct a comparative narrative analysis of how a state institution and grassroots activist groups interpret networked citizenship. I find that the networked authoritarian Russian state embraces the ideal of the *dutiful networked citizen* online as visible, vulnerable, and controlled, exploiting the melding of public and private aspects of networked publics and seeking to impose top-down control on the digital acts of its citizens. Instead, Russian digital rights activists advocate for a *self-actualizing networked citizen* who exercises their agency online by employing digital platforms and tools to become less visible, more ephemeral, and therefore, more private and secure. This reinterpretation contests boyd's (2010) traditional concept of affordances of networked publics and questions conventional ideas of citizenship, agency, and digital rights. I also suggest that the "below the radar" activities of digital activists, though harder to trace and to study, are all the more important for understanding how the affordances of social media can diverge from the traditional Western-centric models (Abidin, in press) when applied to authoritarian and hybrid regimes (Diamond, 2002; Robertson, 2010).

Conceptualizing Networked Citizenship

The key aim of this research project is to explore the growing connection between citizenship, human rights, and digital rights and to elaborate a clearer understanding of the competing definitions of networked citizenship by the Russian state and Russian digital rights activists. While this project explores the particular context of Russia, a networked authoritarian state, the findings are useful for understanding networked citizenship in other contexts as well.

The relationship between citizenship and rights is a complicated one. The traditional definition of citizenship presents it as a special personal status based on one's legal belonging to a sovereign nation-state. This concept of citizenship is closely connected to ideas of territory, belonging, and identity (Turner, 2009). As a formal status, citizenship comes with certain rights as derived from the laws or norms in a given country (Waters, 1989), but also certain obligations imposed by the same. However, the Universal Declaration of Human Rights (UN General Assembly, 1948) defines the liberties and freedoms of people around the world regardless of their citizenship status (or lack thereof), thus offering a broader definition of human rights across borders.

Another debate that has shaped the concept of citizenship is the differentiation between its passive and active forms (Turner, 1990). Dahlgren (2009) describes this division as a split between a universalist and state-centered idea of *received* citizenship and the differentiated idea of *achieved* citizenship that is based on individual agency. The main difference here is whether citizens are considered passive recipients of rights or actively engage and participate in civic and political life. Both forms of citizenship co-exist in modern interpretations of the concept, though the tensions between them are becoming more evident.

Hintz et al. (2018) argue that the most important shift in understanding active citizenship has come with a growing focus on how individuals in society enact their citizenship, focusing on practice rather than status. Within this paradigm, citizenship is best viewed not as a "formal, legal set of rights and obligations," but as a "mode of social agency" (Dahlgren, 2009, p. 57) or as an "expression of agency" (Lister, 2003, p. 38). This view of citizenship focuses on acts of citizenship and investigates the spaces of "doing citizenship" where members of society perform and enact their role as citizens. It also underscores the contested nature of citizenship, as citizens and nation-states struggle for control over the very ideas of agency, identity, and belonging.

The inherent contradiction between inalienable human rights and the rights of nation-state citizens has only sharpened in the digital age as Internet companies and platforms have become global actors and have modified the meanings of rights such as freedom of expression, the right to privacy, and the right to information. This expansion of the boundaries of human rights to encompass digital rights has triggered constant deliberations between various social actors over the scope of these rights and how they could be reflected in new conceptualizations of citizenship. The debates have ranged from discussions about whether Internet access should be a basic human right to the discourse around pervasive datafication and surveillance and their impact on citizen agency (Hintz et al., 2018).

As social and political life is increasingly mediated by digital technologies, citizenship acts also gain a networked dimension. Bennett (2008) notes that, especially in post-industrial democracies, economic, social, and technological change has transformed the traditional group-based society into a network society, one in which individuals become "responsible for the production and management of their own social and political identities" (p. 13). The networked character of society should also be viewed in the context of an increasingly informal political culture, where the boundaries between politics, cultural values, identity processes, and local self-reliance measures become more fluid

(Dahlgren, 2009). These overlaps also inform the understanding of citizenship as performative and expressive and underscore the role of expressions, discourses, and narratives surrounding the idea of citizenship.

Importantly, networked technologies not only afford new kinds of rights and responsibilities to citizens, but also reconfigure the enactment of citizenship itself. From digital protest and activism to digital storytelling and citizen journalism, everyday digital acts now constitute part of our role and identity in society, contributing to our understanding of networked citizenship. Scholars of digital citizenship have mostly been optimistic about the positive role of digital technologies as forces enabling democratic participation, but more measured approaches have also grappled with notions of access, literacy and inclusion. Lindgren summarizes digital citizenship as "the opportunities and resources" individuals have "to participate online in society and politics" (Lindgren, 2017, p. 147), whereas Isin and Ruppert (2015) focus on how specific "digital acts" combine to form people's position as active citizens in a society. These interpretations usefully align with the concept of technological affordances as possibilities for action or constraints on action that arise at the nexus of actors and technologies in a particular context.

I propose to apply the affordances lens to examine the notions of networked citizenship as interpreted and constructed by the Russian state and Russian digital rights activists. Such an analysis also accounts for a more critical understanding of networked citizenship, where the digitally mediated environment is not simply seen as empowering, but may also be used by the state or corporate powers to limit users' agency and capacity for self-actualization. Despite new potentialities for action, the performative enactment of digital citizenship does not negate the power of traditional authorities that convey citizenship upon state subjects (Hintz et al., 2018). This power can be conveyed through restrictions on citizen agency such as surveillance, censorship, filtering and blocking, and other "information controls" (Deibert et al., 2010). Still, these competing forces ultimately result in a new ontology of the citizen, as described by Siapera (2017)—one brought into being through digital acts and claims to new kinds of digital rights (Isin & Ruppert, 2015).

In their public discourse, both the state and the activists in Russia seek to impose their own frames and interpretations of what it means to be a networked citizen and thus construct different ideas of networked citizenship in the RuNet. In the next section, I offer relevant historic and modern context on Russian strategic narratives about state identity and citizenship. I also discuss key developments in Russian Internet governance that inform further analysis of the relationship between affordances of networked technologies and the frames constructed upon them by the state and digital rights activists to form broader narratives of networked citizenship.

Internet and Digital Rights in Russia

The contested nature of networked citizenship in Russia stems from the increasingly divergent ideas about the relationship between the state and its citizens, as well as the status of human rights and civil liberties in the country. It is also predicated upon the chasm in how the state and digital rights activists understand the role of the Internet and digital technologies in social and political life. These factors inform how the Russian authorities and the active citizens in Russia conceptualize the modern networked citizen.

In its struggles to rebuild its identity after the fall of the Soviet Union, Russia has attempted to construct new shared meanings of past, present, and future by crafting new strategic narratives (Miskimmon et al., 2014) about its history, its nationhood and its citizens. Since the decade of Putin's coming to power at the start of 2000s, the dominant self-identity of the Russian state's strategic narrative has been one of a great power and a strong, sovereign state (Szostek, 2017). That has been coupled with a fear of political and civil unrest as a result of Western interference (tied to the "colour revolutions" in neighboring states). This has led to what Snyder describes as a "politics of eternity," in which the national self-identity relies on a continuous cycle of Russia's perceived victimhood at the hands of Western states and a conviction that "government cannot aid society as a whole but can guard against threats" (Snyder, 2018, p. 8). In this narrative, citizens emerge as securitized subjects that should be manipulated into emotional states of elation or fear. Such manipulation is exercised by political actors through mainstream media channels, but also through digital media (Snyder, 2018). Importantly, active citizens who perform their citizenship through such means of engagement as activism, protest, and advocacy, are also seen as part of the existential threat to Russia's autonomy and security (Akbari & Gabdulhakov, 2019; Robertson, 2010).

Throughout Russian history, issues of state security have often taken precedence over individual freedoms and rights of citizens. This approach is also evident in Russia's modern-day national narrative. The conditional rhetoric of national security is quite pervasive: it is visible in domestic politics and the state's perception of opposition forces, foreign policy threats, defense of social norms, and "traditional" cultural values (Hutchings & Szostek, 2015; Makarychev & Yatsyk, 2014). This logic can also be traced in Russia's ongoing crackdown on Internet freedoms through a series of increasingly restrictive laws and regulations.

Centralized state control over citizens' communications was a foundation of Soviet governance and one of the main tools of influence upon Soviet dissident movements (Soldatov & Borogan, 2015), and today's Russia has readily embraced this legacy. This control was achieved through censorship of mainstream media, foreign publications, and literary works; restrictions on ownership and use of technology such as photocopiers (Hanson, 2008); and through

pervasive wiretapping and surveillance of citizen communications (Soldatov & Borogan, 2015).

Today, the Russian state continues to view control of information flows and restricting expressions of dissent as key to retaining its power (Epifanova, 2020). Moreover, control over technologically mediated communications has become part of the national governance and security agenda. Some scholars argue that the regime can best be described as "networked authoritarianism" (Greene, 2012; Maréchal, 2017), as the state aspires to control all spheres of mediated social life, while investing in high-tech networked infrastructure and developing connectivity. With mainstream media largely run or co-opted by the state, the Internet has until recently been a relatively free but increasingly contested space for dissent (Oates, 2013). But in the last decade, the Russian state has made legislative, regulatory, and economic efforts to wrestle control of the digital space away from dispersed private actors and to centralize Internet governance, content regulation and network infrastructure. Regulatory bodies such as Roskomnadzor, tasked by the state with oversight of the Internet, media, and telecommunications, have taken on a more prominent role (Turovsky, 2015). Laws such as the data localization bill, the anti-extremist legislation policing online speech (Luganskaya, 2017), and the more recent Internet sovereignty law, aimed at co-opting telecommunications infrastructure along with increased filtering of citizen communications (Lipman & Lokot, 2019), exemplify this push for control on the part of the state.

The Russian state has also propagated discursive norms in an attempt to normalize increased control and monitoring of citizens online. By framing the Internet as an inherently dangerous space and by presenting online content in general as "unreliable" (Ognyanova, 2015), Russian authorities seek to appeal to citizens' security concerns. The other narrative is a geopolitical one of "digital sovereignty," wherein the state promotes illiberal practices in Internet governance as part of a global cyber warfare narrative (Epifanova, 2020). Thus, the Russian state's idea of networked citizenship aligns closely with its networked authoritarian practices and revolves around key pillars of security, control, surveillance, and censorship.

Active Russian citizens find themselves having to contend with increasingly sophisticated state surveillance, in addition to state attempts to co-opt Internet and telecommunications infrastructure and pollute the digital public sphere. They respond to these challenges by using circumvention tools and encrypted communications, but also by promoting digital security and privacy more broadly (Lokot, 2018). Digital rights groups also engage in monitoring state repressions and censorship online, carrying out long-term data collection, and reporting on instances of blocking, filtering, citizen arrests, and prosecutions for online activity (Merzlikin, 2019).

Both the citizens and the state make use of the affordances of the Internet for sharing information and performing identities, though to very different ends. While it is important to understand how both the state and individual Internet users engage with and interpret the affordances of networked publics, I argue that it is also worth exploring the higher level narratives and meanings that emerge from this digitally mediated activity if we consider it as "doing citizenship." The articulation of networked citizenship as an active and achieved form of citizenship and the contestation of such discourse by the state as discussed earlier is helpful in drawing out competing ideas of what citizenship means in a digitally networked Russia today. It goes beyond previous research on fragmented practices of heterogeneous groups dealing with government surveillance or embracing state co-optation (Gabdulhakov, 2018; Lokot, 2018), and helps surface the key discursive frames in the alternative narratives of networked citizenship articulated by the state and digital rights groups working in Russia.

The analysis of public communications, described in more detail in the next section, suggests that the state and digital rights advocates frame networked citizenship in different ways, competing to create and promote a dominant strategic narrative. These frames, I find, map to some extent onto affordances of networked publics such as permanence, searchability (boyd, 2010) and visibility (Pearce et al., 2018), while also problematizing these affordances and revealing new ones.

Research Design and Methods

Although specific acts by the state and by activists speak to the competing conceptions of networked citizenship in Russia, it is equally important to examine how state and civic actors articulate these meanings in discursive terms in digitally mediated spaces and to what extent their narratives are contradictory. Exploring how the framing of specific aspects of networked citizenship fits into broader narratives is an approach that builds on the concept of strategic narratives used in international relations scholarship (Miskimmon et al., 2014). It allows to present frame contestation as a set of struggles over the meaning of certain events or acts within the contours of broader strategic narratives of states, institutions, or other groups. As they evolve and coalesce, strategic narratives can project influence or manage expectations in a national or international arena as they shape language and ideas, thereby also shaping interests, identities, or understanding of key issues (Livingston & Nassetta, 2018). Narratives "integrate interests and goals—they articulate end states and suggest how to get there" (Miskimmon et al., 2014, p. 5), so examining them helps understand how the central ideas and concepts of a state or a society are constructed and articulated. In addition, Hutchings and Szostek (2015) argue that strategic narratives do not only exert their influence in the foreign policy or international relations arena: they are also internalized by national political institutions, influence citizens at all levels of society, and inform policy decisions and civic activity.

With states, political and civic actors operating in a digitally mediated environment, Livingston and Nassetta (2018) argue that the narrative battle today also plays itself out on networked platforms. There, it tends to take the form of framing contests, either around specific events or around the discourse about norms and values ascribed to networked citizens. These framing contests and the strategic narratives they feed into are what I seek to capture in my analysis of the publicly available mediated communications of the state and the digital rights advocates on the Russian Internet.

The key sources of frames and narratives in this study are the following:

- *Roskomnadzor* (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 and monitoring of electronic media, mass communications, information technology, and telecommunications (Roskomnadzor, 2010). It operates as an independent agency under the auspices of the Ministry of Digital Development, Communications and Mass Media. Roskomnadzor oversees compliance with relevant Russian legislation and manages Russia's extensive banned websites registry—its main censorship tool (Turovsky, 2015).
- *Roskomsvoboda* (RKS) is 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, Roskomsvoboda 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. Its members regularly participate in national and international internet freedom events such as RightsCon and organize their own digital security conference, Crypto Install Fest (Roskomsvoboda, 2019c).
- *Internet Protection Society* (OZI) is a more recent player in the digital rights sphere in Russia, founded in 2015 by Leonid Volkov, an activist who also works with Russian opposition leader Alexey Navalny. Although not as prominent or public in their digital rights work as Roskomsvoboda, OZI has created several monitoring initiatives mentioned earlier (OZI, 2019a, 2019c) and has been involved in networked infrastructure projects, as well as engaging in more public activity. For instance, in March 2019, OZI became the first Russian NGO to join ICANN[1] as a member, as part of its Non-Commercial Users Constituency (OZI, 2019b).

I chose to examine publicly available Russian-language activity reports from the official websites of Russia's state Internet regulator Roskomnadzor and digital activist groups Roskomsvoboda and OZI (https://rkn.gov.ru/, https://roskomsvoboda.org/, and https://ozi-ru.org/) between the start of 2015 and the start of 2019. These reports (annual in the case of Roskomnadzor, monthly or more in the case of OZI and Roskomsvoboda) represent key issues and activity of each organization. They are created for public consumption, and are, therefore, an informative source of discourse and frames around digital rights, obligations, and Internet users that ultimately construct broader narratives of networked citizenship in Russia. For each organization, I also collected the text from their About or Mission sections to capture how they frame their goals and objectives in the context of their work.

To focus my analysis of the text corpora from each organization, I collated the content collected from each source into a plain text file. The resulting files contain 157,912 words (Roskomnadzor), 158,905 words (Roskomsvoboda), and 61,873 words (OZI), respectively.

I then used AntConc (Anthony, 2019), a freeware tool for conducting corpus linguistics and concordance analysis on large volumes of text, to examine the discursive context and frames around specific keywords related to digital rights, freedoms, and citizenship more generally. Other AntConc features such as Clusters, N-Grams, and Collocates also helped provide additional context for phrase and word use to reveal common frames used by each actor. The keywords that directed the analysis include "гражданин/граждане" ("citizen/citizens"), "гражданский" ("citizen," adj.), "пользователь/пользователи" ("user/users"), "право/права" ("right/rights"), "обязанность/обязанности" ("obligation or duty/obligations or duties"), "обязан/а/ы" ("obligated," in various declensions), and "свобода/свободы" (freedom/freedoms"), as well as "защита" ("defense/protection"), "безопасность" ("security"), and "безопасный/ая/ые" ("secure"). Where possible, stemming was used to capture all possible word endings and word forms in Russian.

The analysis revealed several recurring frames used by the state and by digital rights activists to articulate their own conceptions of networked citizenship in Russia. In the next section, I discuss these in more detail and show how these frames map onto affordances of networked publics to inform competing—and often conflicting—strategic narratives of networked citizenship.

Findings: Updating the Affordances of Networked Publics

The initial quantitative analysis indicates the relative prominence of relevant keywords in the public content corpus from each organization. Table 1 presents the keyword instances as a percentage of the total word count in each text corpus. While an imprecise measure of keyword prominence, this comparison offers some idea of how central

Table 1. Keyword Instances as Percentage of Total Word Count in Each Text Corpus.

Keyword (stemmed)	Roskomnadzor 157,912 words	Roskomsvoboda 158,905 words	OZI 61,873 words
"гражданин/граждане" ("citizen/citizens," n.), "гражданский" ("citizen," adj.)	0.34% (534)	0.23% (368)	0.13% (80)
"пользователь/пользователи" ("user/users")	0.07% (107)	0.49% (786)	0.31% (194)
"право/права" ("right/rights")	0.31% (495)	1.18% (1880)	0.48% (299)
"обязанность/обязанности" ("obligation or duty/obligations or duties"), "обязан/а/ы" ("obligated")	0.03% (44)	0.06% (96)	0.03% (18)
"свобода/свободы" ("freedom/freedoms")	0.03% (42)	0.27% (427)[a]	0.36% (220)
"защита" ("defense/protection")	0.23% (364)	0.38% (609)	0.09% (56)[b]
"безопасность" ("security"), "безопасный/ая/ые" ("secure")	0.05% (85)	0.08% (133)	0.08% (52)

[a]Excluding instances of "свобода" ("freedom") used as part of the organization name, Roskomsvoboda.
[b]Excluding instances of "защиты" ("protection") used as part of the organization name, Internet Protection Society.

Table 2. State and Activist Narratives of Networked Citizenship and Their Affordances.

State (RKN): Received citizenship	Activists (RKS/OZI): Achieved citizenship
Visibility—all citizen activities and communications in plain sight, state able to monitor data subjects	*Invisibility*—citizens are able to decide how visible they are and to whom, through encryption, anonymity, obfuscation
Searchability—state able to search for, filter and block undesirable activities/content, or prosecute citizens	*Privacy/secrecy*—citizens are in control of their communications, activities, and data, can keep them secret from the state
Permanence—access to citizen data and metadata at any time by state or law enforcement in name of security	*Ephemerality*—data and metadata can be deleted at user's will, citizen activities elusive, especially to state eyes
Vulnerability—citizens as data subjects controlled by the state, with state granting limited rights and freedoms in exchange for offering protection	*Agency*—citizens as active individuals exercising fundamental rights and freedoms in a self-regulated environment

these notions are to the recent public discourse of each organization.

Qualitative discursive analysis of the published reports reveals further discrepancies in the framing of specific attributes of networked citizenship. The state and digital rights advocates in Russia construct two contradictory narratives of networked citizenship, emerging from the discursive framing of rights, freedoms, and duties, as well as notions of defense and security. Table 2 offers a summary of how these frames map onto traditional affordances of networked publics—permanence, searchability (boyd, 2010), and visibility (Pearce et al., 2018).

It is evident that both the state and the activists are aware of these affordances and their limitations, yet, seek to harness them for their own cause. In the process, they also surface new affordances of networked publics (Abidin, in press), which contribute to the diverging constructions of networked citizenship in Russia. To some extent, these discrepancies align with Bennett's (2008) models of the dutiful citizen (favored by the state) and the self-actualizing citizen (championed by the activists), augmented by specific affordances of networked publics in Russia. The rest of this section examines these affordances as articulated by Roskomnadzor, Roskomsvoboda, and OZI, providing examples of relevant discourse from both the state and the activist corpora.

Visibility Versus Invisibility

The state regulator's public communications frame citizens in a predominantly instrumental context, referring to "citizen appeals" or "personal data" of citizens, instead of presenting them as active individuals exercising their rights. The focus is overwhelmingly on what is being done to the citizens and how the state works to protect them, rather than on their own actions. For instance, in its 2018 report (Roskomnadzor, 2019, p. 5), RKN announced that in that year, one of its main objectives was "providing the security of the rights of personal data subjects."

The state discourse around "users" is quite similar, with the keyword featuring mostly in a technological context and one of the most common clusters being "user identification." This was the case in the 2016 report (Roskomnadzor, 2019), where RKN boasted of organizing regional "raids to monitor mandatory identification of users availing of internet access through public collective access points, including Wi-Fi access points" (Roskomnadzor, 2019, p. 37).

These frames point to the preoccupation of the state with making sure their citizens are visible to relevant government and law enforcement bodies by monitoring citizen online activity, establishing blanket digital surveillance, and ensuring ad hoc access to user information, while seeking to shield it from external actors. Since 2012, Russia has passed laws

requiring popular bloggers to register with the state, mandating storage of Russian user data inside the country, as well as anti-extremism measures simplifying online surveillance and state access to user data (Luganskaya, 2017; Turovsky, 2015).

At the same time, the state's duty-related discourse mostly bypasses citizens and revolves around professional duties of civil servants working for RKN or legal obligations of telecommunications and Internet service providers. For instance, in its 2017 report (Roskomnadzor, 2019, p. 66), the state regulator advised that under a new law, search engines were now "obligated to remove information about banned webpages from search results." This opaqueness around individual obligations may serve as further evidence of the state's view of citizens as passive, vulnerable subjects devoid of agency, whose only duty is to conform to the state's expectations, participate in state-sanctioned activities (Bennett, 2008) and make themselves and their data visible and available to those in power.

In contrast, the framing of "duties" in activist text corpora is primarily related to the state imposing obligations on various actors in the information sphere, including users, Internet service providers, and social media platforms. This framing is clearly critical of the state's attempts to propagate its control mechanisms to other actors: both RKS and OZI discuss state requirements to deanonymize or register citizen identity; block, filter, delete, or limit content; and install surveillance equipment. These duties of ensuring visibility of citizens to the state are frequently seen as conflicting with the fundamental rights and agency of networked citizens. As OZI states in its mission manifesto (OZI, 2018),

> The internet is created to resolve any of its issues based on self-regulation and does not require any control on the part of state institutions.

In response to the state's insistence on pervasive visibility and regulatory control of citizens online, activist discourses instead promote self-regulation as key to Internet freedom. OZI argues that in Russia, this freedom has been impeded by draconian state legislation aimed at total control of online activity, such as the state's "plans to control Internet traffic and cross-border traffic exchanges" mentioned in the February 2016 report of OZI's Internet Freedom Index (OZI, 2019a).

The state is seen as actively undermining Internet freedom and at odds with the digital rights agenda, and activists adopt new kinds of activity, aimed at both educating the public about their rights and freedoms, and at combatting state attempts to wrestle those freedoms away from citizens and make them more vulnerable. These digital literacy efforts, such as promoting the use of encrypted tools to protect user communications from the watchful eye of the state and the use of anonymity-boosting measures such as proxy servers and VPNs, point to invisibility as a key affordance that activists see as foundational in exercising networked citizenship. One example of such advocacy is RKS's own VPN Love project (Roskomsvoboda, 2019c) that recommends trustworthy services. Importantly, activists argue that the power to decide how visible to be and to whom lies in the hands of Internet users, and should not rest solely with the state. For instance, in a July 2018 report, RKS critiqued the injustice of law enforcement accusing users of "extremist online speech" for "liveblogging court proceedings, reposting songs, film snippets or posting a careless comment" (Roskomsvoboda, 2019b).

Searchability and Permanence Versus Privacy/ Secrecy and Ephemerality

The ability to search for, filter, and block user data and communications is at the heart of the Russian state's approach to networked citizenship and how it is exercised by citizens. The discourse around digital rights in state communications is a fitting example of how the affordances of searchability and permanence of networked publics are operationalized by the state. Citizen rights are primarily framed by Roskomnadzor as rights of personal data subjects, and discussed in an instrumental context of the digital market and economy. In its 2017 report, RKN touted its key role in the emerging digital economy and noted that "in the context of new digital identities and biometric identification systems, the work of protecting personal data becomes especially sensitive and important" (Roskomnadzor, 2019, p. 10).

Roskomnadzor's discourse around security and safety further adds to the framing of networked citizenship as received or granted by the powerful state: its reports discuss digital security alongside personal data protection and safe online behavior. The focus is on a secure and safe environment, as well as law and order, which require user communications and activity to be permanently accessible by the state in perpetuity. Safety and security online are also discussed in the context of national security, with a focus on the Russian segment of the Internet as a sovereign space that requires state defense from global threats. In its 2018 annual report (Roskomnadzor, 2019, p. 2), RKN explicitly says,

> 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.

Such securitized discourse is in line with recent moves by the Russian state to use national security as a pretext to gain access to user communications and metadata (Luganskaya, 2017), preserving their permanence and making them searchable by state actors. These range from demanding encryption keys from messaging platforms and social networks to passing Internet sovereignty legislation to cement control over the RuNet's infrastructure, traffic, and citizen activity (Lipman & Lokot, 2019).

In comparison, the discussion of the right to privacy and secrecy is especially prominent in activist communications,

connecting citizen (civil) rights, human rights and digital rights and freedoms of Russians. Both RKS and OZI discuss "rights violations" and "defending rights," but often speak directly to the public about "your rights." In a June 2018 report, reacting to the new anti-extremist legislation adopted in Russia, Roskomsvoboda (2019b) activists addressed users and vowed to "help you to realise your right to anonymity and encryption under the conditions of total surveillance engineered by the state."

Importantly, the activist discourse explicitly refers to specific rights of networked citizens, such as privacy, anonymity, secrecy, free expression, free distribution of information, access to digital networks, and encryption. These are viewed as "fundamental rights" and are discussed alongside the criticism of the Russian state's violations of these rights. OZI, in particular, juxtaposes "state interests" and "individual rights": for instance, in an October 2017 update, OZI (2019a) cites expert reactions to the Russian state's ongoing crackdown on anonymity in messaging services and concludes that this is indicative of "a general state politics that aims to take away any right to privacy citizens may have by any means." This framing is reflected in the organization's activity, for example, their monthly index of Internet freedom (OZI, 2019a) and their project mapping Internet repressions in Russia (OZI, 2019c).

The rights-related discourse also features extensive discussion of the role of digital rights activists themselves in defending the rights of Russian networked citizens to privacy and confidentiality. Although they refer to "constitutional" rights and "legal" protections, they also place their advocacy and activism in a global context, referring to the practice of the European Court of Human Rights and the relevant international rights conventions which underpin their activity. Again, these frames are reflected in the activist work: in August 2016, RKS advertised a new partner project, the Digital Rights Centre, as "ready to help you solve any legal issues that internet users may face" (Roskomsvoboda, 2019b).

The security and safety discourse in activist corpora follows the tensions between individual user safety and the attempts of the state security apparatus to securitize networked spaces. They frame the notion of personal information security in terms of what citizens can do to protect themselves online, and how that notion is contested by the state as part of its national security discourse. Along with using encrypted messaging services, for instance, digital rights activists recommend that users delete their accounts on platforms that cooperate with law enforcement or purge their personal data from these accounts to avoid sanctions. In an August 2018 report, OZI (2019a) sounded the alarm, referring to several alleged cases of Russian social network VK "sharing personal and private data of its users with law enforcement bodies." These means of protection focus on making citizen activity less visible and more ephemeral, and therefore, more secure. This is a very Russia-focused discourse, tied closely to the digital rights frame, and here, user agency also emerges as a related affordance in empowering networked citizens to be safe and secure online, not through the actions of the state, but despite them.

Vulnerability Versus Agency

Freedom is framed as a national issue in Roskomnadzor's text corpus, bounded by the legal norms of the state rather than grounded in individual agency or any universal norms. It is often placed within the context of "constitutional rights and freedoms of citizens" in Russia. "Freedom of mass information" appears more often than mentions of freedom of speech or individual freedoms (17 instances vs. 5 instances in the text corpus, or 0.01% vs. 0.003%, respectively)—in line with Bennett's (2008) description of dutiful citizens as those informed about issues and government mostly through mass media. "Internet freedom" is only mentioned twice, and "digital freedom" only once. Cautions about "abusing freedom" are a recurrent theme, pointing to a desire on the part of the state to frame freedom, as with rights earlier, as a product of state control rather than of individual citizen agency. For instance, in its 2018 annual report, RKN stated that a large chunk of the organization's work that year dealt with preserving a balance in "providing citizens' rights to freedom of speech with simultaneous prevention of abusing the rights to freedom of information" (Roskomnadzor, 2019).

The state frames around defense and protection focus chiefly on personal data of subjects and not of citizens, further depriving them of agency. This instrumentalization 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 rights or freedoms of its citizens.

In contrast to the state discourse, citizenship in the discourse of digital rights activists is more closely connected to the rights and interests of individual citizens. Both Roskomsvoboda and OZI draw connections between citizen and human rights, as well as between networked citizenship and civil society. The networked aspect here is more pronounced, with phrases such as "citizens online" (Roskomsvoboda, 2019b) and "digital rights of citizens" (OZI, 2019a). Frequently collocated with "citizen" are mentions of state surveillance and control, criminal prosecution of citizen activities online, censorship of online content. OZI also allude to citizen literacy online, as well as to the broader idea of civil liberties. The activist discourse around "users" is quite similar, in that they frame Internet users as individuals with rights and agency, and not data subjects. The focus here is on "user access," "defending user rights," and combatting violations of these rights, which, in OZI's (2018) words, "distort the usual free environment of networked life so much that we risk losing the kind of internet we need."

Although there is broader discourse around "all internet users" and their rights, much of the content focuses on

specific cases of user rights violations, court cases, and appeals. In this sense, RKS and OZI discuss the activities of users on specific platforms, such as messaging platform Telegram which the Russian state has attempted to block since April 2018 after the messenger refused to share encryption keys with the state (Roskomsvoboda, 2019b), and refer to personal data and user identification in the context of these cases. A frequent phrase in both activist discourses (8 instances or 0.01% in the OZI corpus, and 15 instances or 0.01% in the RKS corpus) is "users can . . . " (OZI, 2019a; Roskomsvoboda, 2019b), underscoring their preoccupation with user agency.

The freedom discourse is central to activist communications, and is a key thread connecting other frames around networked citizenship together. Both RKS and OZI refer to digital freedoms as fundamental and key to preserving the agency of all networked citizens. The universality of these freedoms is again underscored by the mention of international declarations and treaties, including UN conventions. The following terms frequently appear in the text corpora of both organizations: "free internet" (113 instances or 0.18% in the OZI corpus, 58 instances or 0.04% in the RKS corpus), "rights and freedoms" (two instances or 0.003% in the OZI corpus, 33 instances or 0.02% in the RKS corpus) and "freedom of speech" (12 instances or 0.02% in the OZI corpus, 48 instances or 0.03% in the RKS corpus). Importantly, freedom is conceived as both "freedom to" and "freedom from." Citizens should be free to "search, express, disseminate and participate" online, as well as have the freedom to use any technology or platforms they prefer, RKS argued in a January 2015 report summarizing key user rights violations in 2014 (Roskomsvoboda, 2019b). In this regard, activists single out the key affordances and tools of networked publics to achieve such freedom, including privacy, anonymity, encryption, and circumvention. At the same time, they also frame freedom as freedom from intrusive state interventions and violations of user rights. In a January 2019 monthly report focusing on Russian Internet infrastructure and state attempts to take control, OZI (2019a) noted with some irony that "until 2012, the internet had successfully developed in Russia without state intervention and regulation."

As expected, the framing of defense or protection in activist discourse is directly connected to the rights and freedoms frames. Digital rights activists see their work as "defence of human rights" (Roskomsvoboda, 2019b), highlighting the centrality of rights and freedoms in their vision of what the networked sphere is meant to be. However, they see their mission as more than offering legal defense and technological solutions. Crucially, activists also promote individual agency by asking the users to "defend themselves" from surveillance and censorship and fight for their privacy. As RKS notes on their Projects page, "our aim is for every RuNet user to be able to defend their [digital] rights" (Roskomsvoboda, 2019a). This, they argue, can be achieved through sustained public deliberation and advocating for security literacy, to give the users more control over their visibility, searchability, and permanence online. These include organizing protest rallies; public documentation of state pressure on Internet users; and developing practical tips on protecting oneself from digital surveillance such as RKS's SAFE Project (Roskomsvoboda, 2019c).

Competing Narratives of Networked Citizenship

The state Internet regulator's strategic narrative of networked citizenship that emerges from the discourses analyzed in the previous section is that of received citizenship, granted by the state to its subjects in an act of benevolence. The networked authoritarian Russian state promotes the ideal of the *dutiful securitized citizen* (after Bennett, 2008) embedding it within the greater narrative of national security and digital sovereignty. This dutiful citizen is a state subject who is constantly visible to the authorities, vulnerable through the availability of their private communications and metadata. Dutiful networked citizens and their digital acts are heavily regulated and are subject to top-down control in the name of security. Bennett's model of citizenship as a matter of duty and obligation to the state is enhanced by the Russian regulator through the instrumentalization of Internet users as "data subjects" valuable not because of their individual agency but because of their permanently available data and metadata. The ideal dutiful networked citizen in the eyes of Roskomnadzor is not only law-abiding and willing to participate in government-sanctioned activity, but also willing to share their digital identity and information with the state without reservations, and willing to accept limitations on rights and freedoms in exchange for security. This narrative of networked citizenship demonstrates how intertwined the logics of data capitalism (Hintz et al., 2018) and securitization can become in hybrid regimes like Russia (Robertson, 2010), and how these regimes can capitalize on datafication to grow their power instead of seeing it as a threat.

Russian digital rights activists instead view networked citizenship as an achieved status independent of state or national jurisdiction. In the strategic narrative emerging from the discourses analyzed, they advocate for a *self-actualizing ephemeral citizen* (after Bennett, 2008) who exercises their agency online by taking control of their own visibility, searchability, and data permanence and circumventing state attempts to regulate or suppress their digital acts. This ideal of citizenship is self-actualizing as it is based on fundamental rights and freedoms available to all humans regardless of nationality and is enshrined in universal norms. It is also predicated on invisibility, privacy, and ephemerality as key affordances, as networked citizens exercise their agency in deciding which aspects of their online presence are made visible, how they can be discovered, and for how long. The privacy and ephemerality also afford users agency through the various tools they can use to be anonymous, to keep their communications private, to evade state surveillance, and to

access blocked or filtered websites. Being an active citizen—and having the agency and capability to do so—means being less (or selectively) visible to the state, harder to trace, and therefore, more private and secure. It also enables networked citizenship as performative enactment (Hintz et al., 2018), where citizens are empowered to engage in digital acts without particular deference or obligation to the state, and often as a direct challenge to state authority.

The idea of invisibility or ephemerality as empowering may seem counterintuitive. However, in the context of Russia's pervasive communications surveillance and growing securitization of everyday life, the "below the radar" activities of networked citizens, especially digital rights activists, demonstrate how the affordances of social media can be reinterpreted and reappropriated when applied to undemocratic or authoritarian environments.

Conclusion

Understanding emerging ideals and narratives of citizenship in a networked world is important, as the networked nature of everyday social and political life pushes scholars to re-evaluate what it means to be a citizen today. This study of competing strategic narratives of networked citizenship from the point of view of the Russian state and Russian digital rights activists shows how divergent such ideals can be in hybrid regimes (Diamond, 2002; Robertson, 2010). Both the state and the activists are aware of the affordances of networked publics for enacting citizenship, but they espouse wildly different interpretations of how those affordances can limit or empower citizens and states. My analysis of public communications of the Russian state internet regulator and prominent digital rights groups shows that digital rights activists in Russia advocate for self-actualizing networked citizenship based on individual agency and ephemerality. Such an ideal of citizenship is more in line with the internationalized digital rights narrative than the Russian state's narrative of a highly securitized and monitored citizen within a networked, but tightly regulated sovereign Russian state.

It is worth noting that both of these strategic narratives are highly aspirational and are ideal states that the Russian government and the activists aspire to. The current reality of networked citizenship in Russia is somewhere in between, shaped as much by Russians' ideas about the state and the networked Internet sphere as by what Greene (2019) calls "vernacular knowledge" of what citizenship means in modern Russia, embedded in localized micro-contexts of social and political life. Further research should explore how diverse Russian citizens conceptualize networked citizenship and how these ideas align with the strategic narratives in this study. Still, it is important to take stock of these framing contests and the narratives they generate. They offer competing meanings and scenarios for networked citizenship in the Russian context and, therefore, have implications for the future of Internet governance, digital rights, and personal identity in a networked Russia and a datafied world.

Acknowledgements

The author is very grateful to the Urbino AoIR Flashpoint Symposium committee for hosting the Symposium and to the issue editors for working to make this Special Issue happen and encouraging all of the authors to complete and perfect their contributions. The author also thanks the participants of the Symposium for their questions and feedback.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Tetyana Lokot https://orcid.org/0000-0002-2488-4045

Note

1. The Internet Corporation for Assigned Names and Numbers is a US-based multistakeholder group and nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet.

References

Abidin, C. (in press). From "networked publics" to "refracted publics": A companion framework for researching "below the radar" studies. *Social Media + Society*.

Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance & Society*, *17*(1/2), 223–231.

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

Bennett, W. L. (2008). Changing citizenship in the digital age. In W. L. Bennett (Ed.), *Civic life online: Learning how digital media can engage youth* (pp. 1–24). MIT Press.

boyd, d. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *A networked self* (pp. 47–66). Routledge.

Dahlgren, P. (2009). *Media and political engagement: Citizens, communication, and democracy*. Cambridge University Press.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. MIT Press.

Diamond, L. (2002). Elections without democracy: Thinking about hybrid regimes. *Journal of Democracy*, *13*(2), 21–35.

Epifanova, A. (2020). *Deciphering Russia's "Sovereign Internet Law": Tightening control and accelerating the Splinternet* (DGAP Analysis, 2). Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-66221-8

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.

Gabdulhakov, R. (2018). Citizen-led justice in post-communist Russia: From comrades' courts to dotcomrade vigilantism. *Surveillance & Society*, *16*(3), 314–331.

Greene, S. (2012). How much can Russia really change? The durability of networked authoritarianism. *PONARS Eurasia*. http://www.ponarseurasia.org/memo/how-much-can-russia-really-change-durability-networked-authoritarianism

Greene, S. A. (2019). Homo post-Sovieticus: Reconstructing citizenship in Russia. *Social Research: An International Quarterly*, *86*(1), 181–202.

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

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society*. Polity Press.

Hutchings, S., & Szostek, J. (2015). Dominant narratives in Russian political and media discourse during the Ukraine crisis. In A. Pikulicka-Wilczewska & R. Sakwa (Eds.), *Ukraine and Russia: People, politics, propaganda and perspectives* (pp. 173–185). E-International Relations Publishing.

Isin, E., & Ruppert, E. (2015). *Becoming digital citizens*. Rowman & Littlefield.

Lindgren, S. (2017). *Digital media and society*. SAGE.

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

Lister, R. (2003). *Citizenship: Feminist perspectives*. NYU Press.

Livingston, S., & Nassetta, J. (2018). Framing and strategic narratives: Synthesis and analytical framework. *SAIS Review of International Affairs*, *38*(2), 101–110.

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.

Luganskaya, D. (2017, April 23). Open Economy: как российские власти будут контролировать интернет. Три основных способа. [Open Economy: How the Russian authorities will control the Internet. Three main ways]. *Open Russia*. https://openrussia.org/notes/708721/

Makarychev, A., & Yatsyk, A. (2014). The four pillars of Russia's power narrative. *The International Spectator*, *49*(4), 62–75.

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1), 29–41.

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*. https://meduza.io/en/feature/2019/04/19/in-a-perfect-world-we-just-wouldn-t-exist

Miskimmon, A., O'Loughlin, B., & Roselle, L. (2014). *Strategic narratives: Communication power and the new world order*. Routledge.

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

Oates, S. (2013). *Revolution stalled: The political limits of the Internet in the post-Soviet sphere*. Oxford University Press.

Ognyanova, K. (2015). In Putin's Russia, information has you: Media control and Internet censorship in the Russian federation. In M. M. Mervio (Ed.), *Management and participation in the public sphere* (pp. 62–79). IGI Global.

OZI. (2018). *Манифест* [Manifesto]. https://ozi-ru.org/ob-obshhestve/manifest/

OZI. (2019a, June 1). *Индекс Свободы Интернета* [Internet Freedom Index]. https://ozi-ru.org/proekty/indeks-svobodi-interneta/

OZI. (2019b, March 25). *Общество Защиты Интернета – Член ICANN* [Internet Protection Society is a Member of ICANN]. https://ozi-ru.org/news/ozi/ozi-icann/

OZI. (2019c, June 1). *Карта Репрессий* [Map of repressions]. https://ozi-ru.org/proekty/internet-repressii/karta/

Pearce, K. E., Vitak, J., & Barta, K. (2018). Privacy at the Margins| Socially mediated visibility: Friendship and dissent in authoritarian Azerbaijan. *International Journal of Communication*, 12, Article 22.

Robertson, G. B. (2010). *The politics of protest in hybrid regimes: Managing dissent in post-communist Russia*. Cambridge University Press.

Roskomnadzor. (2010, November 25). *Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR)*. https://rkn.gov.ru/eng/

Roskomnadzor. (2019, April 15). *Public annual reports*. https://rkn.gov.ru/press/annual_reports/

Roskomsvoboda. (2019a, June 1). *О нас* [About us]. https://roskomsvoboda.org/about-us/

Roskomsvoboda. (2019b, June 1). *Аналитика* [Analysis and reports]. https://roskomsvoboda.org/cat/blog/

Roskomsvoboda. (2019c, June 1). *Проекты* [Projects]. https://roskomsvoboda.org/

Siapera, E. (2017). Reclaiming citizenship in the post-democratic condition. *Journal of Citizenship and Globalisation Studies*, *1*(1), 24–35.

Snyder, T. (2018). *The road to unfreedom: Russia, Europe, America*. Crown.

Soldatov, A., & Borogan, I. (2015). *The red web: The struggle between Russia's digital dictators and the new online revolutionaries*. Public Affairs.

Szostek, J. (2017). Defence and promotion of desired state identity in Russia's strategic narrative. *Geopolitics*, *22*(3), 571–593.

Turner, B. S. (1990). Outline of a theory of citizenship. *Sociology*, *24*(2), 189–217.

Turner, B. S. (2009). TH Marshall, social rights and English national identity: Thinking Citizenship Series. *Citizenship Studies*, *13*(1), 65–73.

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

UN General Assembly. (1948, December 10). *Universal Declaration of Human Rights, 217 A (III)*. https://www.refworld.org/docid/3ae6b3712c.html

Waters, M. (1989). Citizenship and the constitution of structured social inequality. *International Journal of Comparative Sociology*, *30*, 159–180.

Author Biography

Tetyana Lokot is an assistant professor in the School of Communications at 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.