Surveillance & Society

Article

Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices

Tetyana Lokot

Dublin City University, Ireland
tanya.lokot@dcu.ie

Abstract

This paper examines how Russian opposition activists negotiate online visibility—their own and that of their messages and campaigns—and the security concerns brought on by the pervasive digital surveillance that the state resorts to in order to reinstate its control over the online discursive space. By examining the internet-based presence and activity of the members of Alexey Navalny's FBK (Anti-Corruption Foundation) and other opposition activists, the paper traces connections between everyday security practices that these activists engage in online and the resistance tactics and repertoires they enact in an environment where the free and open exchange of information on the Russian internet is becoming increasingly difficult. The analysis finds that Russian opposition activists place a high value on digital, media, and security literacy and that navigating the internet using security tools and protocols such as VPN, two-phase authentication, and encrypted messaging is increasingly seen as the default modus operandi for those participating in organised dissent in Russia to mitigate growing state surveillance. Furthermore, the analysis reveals that Russian activists have to balance the need for security with growing visibility—a key factor for entering the mainstream political and social discourse. The tension between being secure and being visible emerges as a key aspect of resistance practices in an environment of near-constant state surveillance, as activists concurrently manage their safety and visibility online to minimise the risks posed by government spying and maximise the effect of their dissent.

Introduction

The practices of state surveillance in Soviet Russia were ubiquitous and consistently remained one of the main tools of influence and pressure on the embattled dissident movements throughout Soviet history. Unlike the Western tradition wherein independent media were meant to serve as watchdogs and civil society groups historically had the role of keeping authorities accountable, the Soviet regime saw the unrestricted circulation of information as a threat to be tightly controlled (Gorny 2007). This control was achieved through censorship of mainstream media and literary works, as well as through pervasive surveillance of communications. Soldatov and Borogan (2015) note that only select elites were permitted access to objective news or to foreign publications by the Soviet state, whereas ownership and use of technology such as photocopiers were highly restricted in an attempt to prevent the distribution of "subversive" material and literature, known as *samizdat* (Hanson 2008). At the same time, wiretaps and physical surveillance of communications and activities of key anti-regime dissidents were also common (Soldatov and Borogan 2015).

Lokot, Tetyana. 2018. Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices. *Surveillance & Society* 16(3): 332-346.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

In modern Russia, the state's preoccupation with exerting control over technologically mediated communications has become part of the national governance and security agenda. Indeed, some scholars have argued that the regime has morphed from one of communism to one of networked authoritarianism (MacKinnon 2011; Greene 2012), as the state now aspires to control all spheres of mediated social life while placing a high value on developing networked infrastructure and connectivity. With mainstream media largely run or co-opted by the state, the internet remains a relatively free but increasingly contested space for alternative opinions and dissent (Oates 2013). Dissenting internet users find themselves having to contend with a state surveillance apparatus that is growing in its sophistication and making use of the affordances of the internet for sharing information and performing identities (Gunitsky 2015).

This study examines how Russian opposition activists negotiate online visibility—their own and that of their messages and campaigns—and the security concerns brought on by the pervasive digital surveillance that the state resorts to in order to reinstate its control over the online discursive space. Why are opposition activists suddenly publicly preoccupied with surveillance and security? And how are they dealing with these concerns while pursuing their activist agenda? Situating its inquiry at the nexus of technologies, practices, and publics, the paper draws on the concept of "media as practice" (Couldry 2004, 2012) that is increasingly being used to analyse protest politics as well (Mattoni 2016; Mattoni and Treré 2014). It considers how political activists can adapt and integrate the changing media practices in the hybrid media system, where the field of mainstream and alternative media and the field of politics interpenetrate (Chadwick 2013). In particular, Mattoni and Treré (2014) suggest using media practices as part of a conceptual framework to explain the interactions between the actors and their mediated environment in social movements at various stages of contention and at various levels of organisation. Among other things, this approach allows connection of the daily routine practices and short-term decisions of individual activists to the broader mechanisms of resistance at community, campaign, or movement levels. By examining the internet-based activities of Russian opposition activists, the paper aims to document the everyday security- and visibility-related practices that these activists engage in. It also seeks to explain how these practices inform the resistance mechanisms and tactical repertoires that the activist community comes to embrace in an environment where the free and open exchange of information on the Russian internet is becoming increasingly difficult.

The paper first describes the emergence of Russia's networked authoritarianism, explaining how the state relies on a system of "information controls" (Deibert et al. 2010) to manage the perceived threats to its authority posed by a free internet and a burgeoning civil society. It also reviews the state surveillance apparatus, its historical precursors, and its recent developments in light of an overall shrinking of the space for free expression and alternative political viewpoints in Russia. The paper then uses ethnographic observation of a range of public online practices by Russian opposition activists to draw conclusions about their strategies and tactics in negotiating state surveillance, managing their own digital (and physical) security, and maintaining visibility of their activism and resistance. The empirical research for the paper involves ethnographic observation of public opposition websites, Twitter feeds, YouTube channels, and Telegram channels in order to evaluate the tools and practices of opposition activists with regard to surveillance, security, privacy, and internet freedom. The observation is complemented by the analysis of relevant media coverage in Russia and beyond.

The study finds that Russian opposition activists place a high value on digital, media, and security literacy. Navigating the internet using security tools and protocols such as VPN, two-phase authentication, and encrypted messaging is increasingly seen as the default modus operandi for those participating in organised dissent in Russia to mitigate growing state surveillance and create relatively safe spaces for activist organising and coordination. Furthermore, the analysis reveals that Russian activists have to balance the need for security with growing visibility—a key factor for entering the mainstream political and social discourse. They negotiate this high-profile visibility through the use of non-Russian social media platforms, hosting their content and conversations on multiple servers, including those outside of

Russia (Ermoshina and Musiani 2017), and making broad use of the internet's affordances for real-time reporting and sharing. As a result, their heightened visibility and transparent security practices online underscore the contrast between internet freedom and the constraints imposed on it by Russian censors and law enforcement. These "strategic visibility" and "conspicuous security" practices also act as insurance against pervasive surveillance that endangers their livelihood and threatens to undermine their resistance work. The tension between being secure and being visible emerges as a key aspect of resistance practices in an environment of near-constant state surveillance, as activists concurrently manage their safety and visibility online to minimise the risks posed by government spying and maximise the effect of their dissent.

Theorising Russia's Networked Authoritarianism and State Surveillance

It is fair to say that the overall climate of fear around state surveillance in Russia is not a new phenomenon. In fact, scholars of the Soviet Union have observed that state surveillance of its citizens was an essential aspect of Soviet political culture (Holquist 1997) and was embedded in society as a cultural practice, per Monahan's definition of such as "an orientation to surveillance that views it as embedded within, brought about by, and generative of social practices" in a specific cultural context (Monahan 2011: 496). Levina (2017) argues that surveillance was not only imposed as a top-down measure, but grew to be normalised and internalised by Soviet citizens and transformed into a kind of performative self-surveillance. At the same time, we cannot discount the infrastructural work of the Soviet surveillance apparatus that worked in a "distinctly pervasive, interventionist, and active mode" (Weiner and Rahi-Tamm 2012: 5) and gave birth to numerous state institutions, policies, and initiatives, many of them secret or semi-official.

In its present form, the Russian state continues to place a high value on controlling information flows and managing or curtailing any expressions of dissent within the country's public social life. To this end, Russian authorities employ a system of "information controls"—a concept coined by Deibert et al. (2010) and circumscribing a vast range of "techniques, practices, regulations, or policies that strongly influence the availability of electronic information for social, political, ethical, or economic ends" (Citizen Lab 2015). Such a system of controls necessarily includes technical means such as "filtering, distributed denial of service attacks, electronic surveillance, malware, or other computer-based means of denying, shaping, and monitoring information," as well as less definite measures such as "laws, social understandings of 'inappropriate' content, media licensing, content removal, defamation policies, slander laws, secretive sharing of data between public and private bodies, or strategic lawsuit actions" (Citizen Lab 2015). This aligns closely with the surveillance studies perspective of the pervasive "culture of control" and David Lyon's proposed definition of surveillance as "focused, systematic, and routine attention […] for purposes of influence, management, protection, or direction" (Lyon 2007: 14).

In a similar attempt to systematise the state internet governance practices in Russia, Ermoshina and Musiani (2017) single out three main types of measures that they describe as "layers" of control. These include surveillance and "lawful interception" of telecommunications data from telephone and internet networks; restrictions on storing and importing user data within and beyond national borders; and finally, filtering and restricting access to particular websites on the basis of laws banning content such as child pornography, discussions of suicide, or extremist materials. Just like the information controls described above, these layers of measures are closely connected and operate in concert to grant the Russian state more power over the Russian-speaking segment of the internet, inching the country towards a "balkanised" internet (Ermoshina and Musiani 2017)—one where the user experience is increasingly fragmented and bound by local restrictions and national regulation.

The multi-layered system of internet controls where surveillance plays a central role rests on a foundation of state governance imposing its control on an infrastructure that is chiefly built, owned, and maintained by private companies, both Russian and international ones. In theory, internet service providers (ISPs), social network platforms, and search engines exercise a form of private governance over how online activity is regulated (MacKinnon 2012) through terms of service, privacy policies, and user agreements. But in practice, the Russian state frequently abuses its legal and regulatory power to shape and constrain these quasi-private online governance practices and seeks to conform them to its broader agenda of controlling the information flows and the digital technology undergirding them. As DeNardis notes, such a melding of state and private regulatory mechanisms enables "new forms of sometimes unaccountable and nontransparent power over information flows" (2014: 15), and in the case of authoritarian regimes, can lead to frequent abuses of such power as the state seeks to influence and coerce internet and telecommunications companies.

It is important to note that Russia's overall approach to internet surveillance and control is evolving in reaction to shifts in political and social climate. Deibert et al. (2010) identify three known generations of internet controls. The first generation resorts to straightforward blocking of websites (Russia's internet blacklist registry[1] is one example of this) to prevent access to content. The second one involves the creation of legal or technical frameworks to restrict access on a case-by-case basis (for example, through geo-focused internet shutdowns or temporary blocking of specific platforms or content). The third generation of controls combines the legal and technical tools with "effective counter-information campaigns which discredit or demoralize the opponent" (Deibert et al. 2010: 16): this includes Russia's widely covered "information warfare" efforts (Thornton 2015), including state-sponsored media propaganda and more sophisticated efforts such as the online troll factory allegedly run with Kremlin support from an office building in Saint Petersburg (Toler 2015; Chen 2015).

Though in the last decade Russia has mostly resorted to second- and third-generation controls and has avoided large-scale blocking, the Kremlin has consistently maintained its broad communications surveillance, extending its reach from telephone networks to internet infrastructure. Unlike the censorship component of recent state initiatives, which has raised considerable public debate, the details of state surveillance remain elusive, and significantly less information about them is publicly available. This aura of fearful mystery, coupled with systematic development of regulatory policies and technical solutions to curtail dissent in Russia while preserving some semblance of free expression, has led to what MacKinnon (2011) terms "networked authoritarianism"—a regime where the state is able to leverage cutting-edge techniques to police online speech and dissuade explicit resistance without resorting to crude mass blocking or filtering.

In terms of fostering a surveillance culture, the Russian government has propagated several different normative ideas in an attempt to normalise citizen monitoring. One has been the narrative of pushing security interests over the value of privacy for individuals: this has been achieved through framing the internet as an inherently dangerous and risky space (Ognyanova 2015) and through presenting online content overall (often seen as an alternative to state-run media) as "unreliable" and "biased" (Kratasjuk 2006; Ognyanova 2015). The other narrative, a more geopolitically flavoured one, is that of "online sovereignty," wherein the state advocates for illiberal practices in internet governance arenas (invoking the "fourth-generation" information controls [Deibert 2016]), legitimising them as part of a global cyber warfare discourse. These narratives combine to shape the public perception of surveillance as a necessary evil and a safety measure, colouring Russian citizens' perception of privacy, dissent, and free expression.

[1] The blacklist of banned websites, or the "Unified Register of Domain Names, Internet Website Page Locators, and Network Addresses that Allow to Identify Internet Websites Containing Information Prohibited for Distribution in the Russian Federation," is run by Roscomnadzor, Russia's state internet watchdog. The blacklist database is accessible via a search form on https://eais.rkn.gov.ru/, and Russian internet rights organisation RosKomSvoboda maintains a mirror database at https://reestr.rublacklist.net/.

The analysis of opposition activists' online strategies and activity in this study aims to understand how they manage these infrastructural, legal, and cultural challenges posed by the state surveillance effort and how they balance their own security and safety with the need to have a visible public presence in order to present to the public a viable alternative dissenting voice.

Data Collection and Research Design

This study is part of a larger exploration of the visibility and practices of activists and protesters in former Soviet states. Specifically, it applies an ethnographic approach to examine the practices and presence of Russian opposition activists in online spaces in the context of pervasive state surveillance. Netnography (Kozinets 2010) or virtual ethnography (Hine 2000) emerges as the most appropriate method to understand the networked media and discursive practices of a particular group (in this case, Russian opposition activists). It is a non-reactive approach (Salmonds 2015) that allows one to observe social media activity and the content it produces over delimited periods of time and to collect extant data without necessarily engaging with the subjects of observation. Observing how digital media platforms afford Russian opposition activists opportunities to address surveillance-related challenges or how they might limit their capabilities, both for security-related activity and for activist practices, informs the key objective of digital ethnography as it ultimately seeks to understand how people use technology in particular circumstances.

The researcher employing netnography may operate primarily in the networked space of connections and communication exchanges rather than a geographic location or a physical site, yet material infrastructures and political systems (especially poignant in the case of pervasive surveillance) enmesh with the digital structures of networks, personal connections, and affordances of technologies, informing our understanding of the modern augmented reality in which surveillance and control, as well as dissent and counteraction, interpenetrate the worlds of atoms and bits. The study would have benefited from being supplemented by surveys or interviews with members of the activist community as this would have allowed the researcher to glean insights into motivations and decisions made by the members of the community behind the scenes. However, this is beyond the scope of the present study, which employs virtual ethnographic methods to analyse manifest (public) traces of mediated activist practices and relies on what has been disclosed, created, or shared in online public spaces.

For the purposes of this study, unstructured ethnographic observation was conducted on a number of public social media accounts of the members of Alexey Navalny's FBK (Anti-Corruption Foundation), based on the list of FBK staff on their website.[2] The netnography sample also included the accounts of several other activists close to the organisation and working with FBK on digital security matters.[3] The decision to study the digital mediated practices of this particular group was informed by the central role that FBK and Navalny's supporters play in the Russian opposition movement (Laruelle 2014; Gel'man 2015) as they bridge political and civic concerns (White 2015). The study is especially interested in seeing how a non-technology-centric and a non-internet-freedom-centric activist community (such as FBK) engages with issues of surveillance, privacy, and security, and what this might mean for how pertinent these issues are for Russia's civil society overall.

Virtual ethnographic observation for this study involved public opposition websites (https://navalny.com/, the main website of Alexey Navalny, and https://fbk.info/, the website of the Anti-Corruption Foundation); public Twitter feeds and Telegram channels of FBK staff, activists, and consultants; and

[2] FBK's official website at https://fbk.info/about/.

[3] The complete list of accounts is not being made public to protect the identities of the activists, many of whom are at risk of state pressure or repressions for their work.

FBK- and Navalny-created online video programming on the public Navalny LIVE YouTube channel.[4] These platforms were observed in order to evaluate the tools and practices of opposition activists, as well as to analyse how these practices allowed the activists to engage with the issues of surveillance, security, privacy, and internet freedom. Where possible and necessary, quotes and observations from particular accounts have been anonymised. Social media observations were supplemented by a review of complementary media coverage of the opposition activists' work for comprehensive analysis and triangulation, and this coverage is cited throughout the study findings where necessary. The overall objective was to observe and document the mediated activist practices of the FBK community and to amalgamate from the observations several overarching trends and themes that could inform our understanding of how Russian political activists strategically approach dealing with issues of security and visibility in an environment of pervasive digital state surveillance.

Because of temporal limitations and the scope of the research project, the observation was constrained to the period between August 2016 and August 2017. Nonetheless, this time period included some milestones, such as several protest rallies and Navalny's embattled campaign in the run-up to the 2018 presidential elections.

The study's findings indicate that Russian opposition activists accept state surveillance as part of their everyday existence but also craft strategic practices to manage their visibility and security in light of pervasive state spying and pressure. The next section discusses these key findings in greater detail.

Security and Visibility Practices for Managing Surveillance

The primary mission of Alexey Navalny's non-profit FBK is to investigate, expose, and fight "corruption among high-ranking Russian government officials" (Anti-Corruption Foundation 2017a). In addition to the NGO's core staff of about thirty people, Alexey Navalny, who is himself a lawyer, also operates an election campaign headquarters network, with a central Moscow office and regional outposts. This network stemmed out of his initial bid to run for Moscow mayor in 2013 (Oliphant 2013) but has grown as he fought to gain access to the presidential electoral race set to finish in March 2018, despite his battles with Russian courts over fraud and embezzlement convictions that Navalny claims are politically motivated (*Moscow Times* 2017).

Throughout their investigative activity and campaign efforts, Navalny's team and the community that emerged around it have made extensive use of digital tools and social media and have proven themselves to be savvy in harnessing the power of internet-enabled communications. Unlike digital rights activists such as RosKomSvoboda, Society for Protection of the Internet, or the Pirate Party in Russia, FBK and its allies have never explicitly made it their mission to fight internet censorship or to raise awareness of the Kremlin's crackdown on free expression online. And yet, over the recent year and a half, the activities on FBK-affiliated online platforms have shifted to include practices dealing with physical and digital surveillance, online censorship and its circumvention, and hacking attacks on activists, as evident from the "Conspicuous Security Practices" section below.

Why are opposition activists suddenly publicly preoccupied with surveillance and security? And how are they dealing with these concerns while pursuing their activist agenda? The study finds that, while FBK activists come to accept state surveillance as routine and inevitable, they also devise security strategies to counter it, promote digital literacy, and employ conspicuous tactics to minimise the threat of government spying. Activists complement these security practices with strategic use of their public communications channels, transparent financial reporting, and counter-surveillance of state officials. These practices allow

[4] https://www.youtube.com/channel/UCgxTPTFbIbCWfTR9I2-5SeQ

for heightened but more controlled visibility that, coupled with their security practices, emerges as a mitigating mechanism in the face of pervasive state surveillance.

Surveillance as the Norm

In modern Russia, which inherited much of the Soviet state's institutional infrastructure and many of the cultural constructs from the Soviet period, we can observe a similar trend towards the normalisation of telecommunications, digital, and internet surveillance. Russia's state security bodies have made use of the narratives about safety, security, and the threats of terrorism and "foreign agents" propagated by the state propaganda machine (and the federal state-run media channels in particular), making security their top argument for pervasive surveillance of both public and private lives of Russian citizens. Such normalisation of surveillance has involved infrastructural, legal, and other measures.

The backbone of digital surveillance infrastructure in Russia, the System of Operative Investigative Measures (SORM), was introduced in 1995, mandating all telecom operators and internet service providers to install Federal Security Service (FSB)-provided hardware to monitor metadata and contents of private communications such as phone calls, email traffic, and web browsing activity (Privacy International 2013). Failing to provide Russian security services with access or to share data could lead to a revocation of an ISP's licence. Since 2012, SORM has also applied its traffic-monitoring capabilities to social networking websites (Soldatov and Borogan 2015), and while its filtering mechanism is said to be flawed, Russian digital rights activists today operate under the presumption that "any information shared on Russian social networks like VKontakte or Odnoklassniki is collected by the intelligence services" (Maréchal 2017: 33). As of 2014, the FSB has begun installing new SORM-3 (third-wave) equipment, allegedly with Deep Packet Inspection (DPI) capability and provisions for long-term data storage (Soldatov 2017). However, comparatively little official information on SORM and its capabilities is available, lending it the same clandestine aura as that of the Soviet wiretapping systems that were its precursors.

With regards to legal norms, Russian lawmakers and officials have adopted a number of legislative acts in recent years that contribute to the normalisation of state censorship and surveillance in digital spaces, both for organisations, such as media outlets and NGOs, and for private citizens. These include the infamous bloggers' law that required popular bloggers with over three thousand daily views to register with the state and disclose their personal information (Lokot 2014); the law creating a state-run list of "organisers of information distribution" and requiring social network websites, portals, and similar sites to register and share certain data with the state; measures limiting anonymous use of public Wi-Fi networks and banning sales of prepaid SIM-cards to customers without state IDs. Some of the most damaging surveillance-oriented legislation has been passed just in the past several years and includes the data localisation law that came into force in 2016 and requires internet companies to store Russian users' data on servers located within Russia. Though some companies (for example, Viber, Booking.com) have complied with the demands, others (such as Facebook and Twitter) have yet to move to do so and face potential fines or blocking: the professional social network LinkedIn has already been blocked in the country for failing to move Russian users' data to Russia (Lunden 2016). Another major recent surveillance tool—the so-called Yarovaya Law passed in the summer of 2016 and taking effect in 2018 (Luganskaya 2017)—is an "anti-extremism" package of amendments that includes anti-dissent measures such as increased sentences for the use of "extremist" language online, a push for internet companies to share encryption keys with the state and to decrypt user communications, and requirements to store user data (content) for six months and metadata for up to three years. Most recently, in July 2017, Russian lawmakers voted to ban anonymous use of messenger apps and services (*Meduza* 2017), further broadening the surveillance powers of Russian security services and law enforcement.

These legal and technical developments contribute to the routinisation of surveillance (Lyon 2007) in Russian society, and this has an impact on activists as well. A persistent theme in the online practices of

FBK activists and their allies in the past year is their acknowledgment of the growing number of surveillance-related threats and attacks on their community. The activists document these attacks and threats meticulously in public social media posts, offering details and speculating about the reasons for the surveillance, the possible perpetrators, and their connections to the state. Examples of surveillance include physical monitoring such as individuals following Navalny campaign activists and even premeditated physical attacks. Navalny's website documents such an attack on the partner of FBK lawyer Lyubov Sobolev, who was attacked by an unknown assailant near their home and drugged in November 2016 (Navalny 2016). Documented examples of combined physical and digital surveillance include plain-clothes law enforcement officers filming participants of protest rallies (on March 26, July 23, and August 26, 2017) with digital cameras and later detaining them based on video evidence, as well as confiscating computers and other data-storing equipment from FBK and campaign headquarters in Moscow and around Russia.

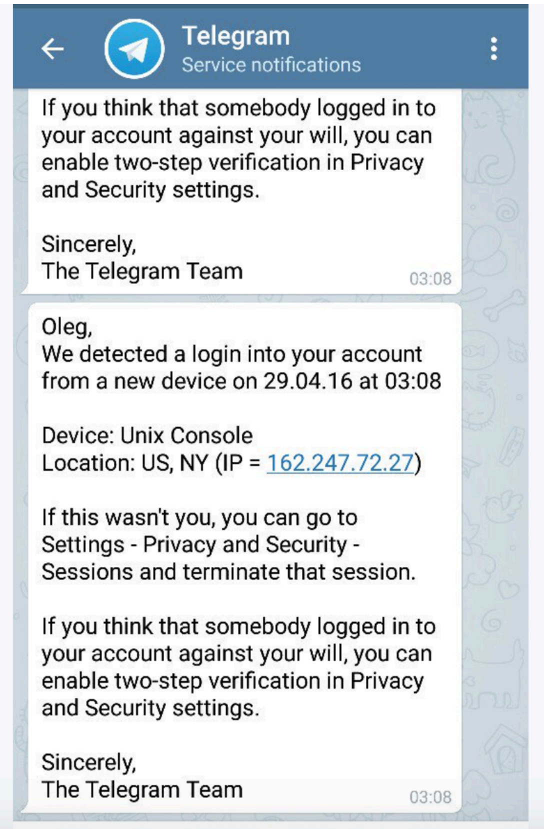
Activists also document multiple examples of networked surveillance, based around digital platforms and employing digital tools. These range from innocuous keyword-triggered Twitter bots (replying to tweets critiquing certain officials) to more serious instances such as the monitoring and closure of e-payment accounts that FBK and Navalny used to solicit donations and crowdfund investigations and the hacking of private email inboxes. Navalny's own email was hacked by "Hacker Hell" in 2012 (Navalny 2015), and content from the emails was subsequently used in court proceedings against Navalny, which he claims are fabricated. Other examples include the attempt to hijack the Telegram accounts of several high-profile activists in April 2016, including Georgiy Alburov, head of investigations at FBK, and civic activist Oleg Kozlovsky (see Figure 1). This particular case was investigated by the victims and their allies in great detail and their digging led them to conclude that the mobile provider MTS cooperated with Russian security services and attempted to remotely hack their accounts by tampering with Telegram's SMS login feature (Lokot 2016). The activists believed intruders wanted to gain access to their personal communications, including contact lists, and even announced they intended to take the provider to court.

Such extensive documentation of instances of state surveillance provides the activists with an opportunity to reflect on how secure their communications and information are and to raise awareness of security issues among their followers and supporters. The next section details how Russian activists become intentionally overt in their security practices.

Conspicuous Security Practices

The examples above combine into a stark canvas of an environment of normalised surveillance practices exercised by the Russian state against those it sees as threats to its hegemony. However, the FBK team and allied opposition activists do not simply document the instances of being watched, recorded, or hacked. While they admit state-perpetrated surveillance is broad and multi-pronged, they also adopt a more proactive position in addressing the attacks and threats by engaging in "conspicuous security" practices on their public online platforms. These practices are conspicuous because they emerge on platforms where previously discussion had centred only around issues of politics and state corruption. They are also conspicuous because activists explicitly and overtly acknowledge the fact of the surveillance and attempt to mitigate or minimise security risks posed by state spying, while also demonstrating in detail how this can be achieved.

First, they use each suitable surveillance case to stage a public deconstruction of what happened and how one can avoid the same happening to them (as in the case with the attempted Telegram hacks). They also promote digital literacy and security literacy in other ways, offering advice, guides, and explanations about key security tools such as the Tor browser, end-to-end encryption, and two-factor authentication. Leonid Volkov, Navalny's long-time ally and head of his election campaign, began hosting a regular online video segment on the Navalny LIVE YouTube channel called "The Cloud," where he specifically



If you think that somebody logged in to your account against your will, you can enable two-step verification in Privacy and Security settings.

Sincerely,
The Telegram Team 03:08

Oleg,
We detected a login into your account from a new device on 29.04.16 at 03:08

Device: Unix Console
Location: US, NY (IP = 162.247.72.27)

If this wasn't you, you can go to Settings - Privacy and Security - Sessions and terminate that session.

If you think that somebody logged in to your account against your will, you can enable two-step verification in Privacy and Security settings.

Sincerely,
The Telegram Team 03:08

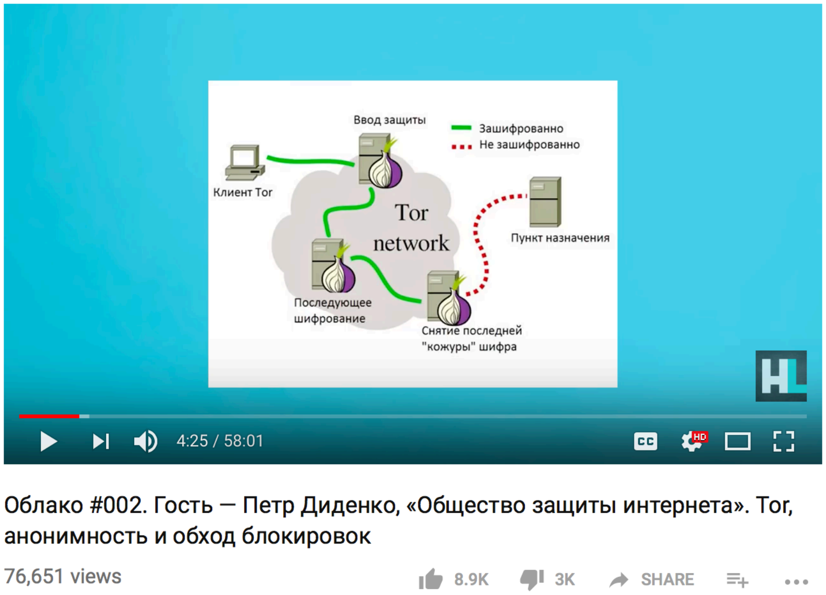
Figure 1. *Screenshot of a security message from Telegram warning of hacking attempt. Image courtesy of Oleg Kozlovsky on Twitter***.**

focuses on issues of online privacy, anonymity, and security, often bringing on expert guests such as security experts and digital rights advocates (see Figure 2). In Volkov's show segments, as well as on their Telegram channels, FBK staff and allies often offer advice on using specific anti-surveillance tools, such as VPNs and proxy services (Navalny LIVE 2017).

Other examples of conspicuous security practices employed by FBK activists include moving away from Russia-based online services and moving their content and activity to servers and platforms outside of Russia. After Navalny's official website was briefly blacklisted in Russia in 2015, and especially with the advent of the Russian data localisation law, opposition activists focused on moving all possible resources to hosting providers outside of Russia, as well as making use of social media platforms that have not conceded to storing Russian users' data inside the country. Activists have taken the time to explain their decisions and discussed the use of platforms such as YouTube, Twitter, Facebook, and Telegram in the context of Russia's environment of political repressions and the tightening space for online free expression.

Finally, FBK and other opposition activists practice conspicuous security by directly involving themselves in the development and creation of digital security and anti-surveillance tools and by supporting others who wish to lend their hand to improve the community's digital arsenal. This is in line with Lysenko and Desouza's observations about the co-evolutionary nature of state surveillance and counter-protest measures and activist ICT-enabled tactics to overcome counterrevolutionary and restrictive measures in the former Soviet Union states (Lysenko and Desouza 2014). Such projects include the Red Button, an app developed by a team led by Alex Litreev, an IT expert and FBK consultant, in April 2017 (Litreev

2017). The app allows protest and rally participants to react quickly in cases of police pressure and to let their friends and family know they have been detained. Another project is the Telegram-based VPN bot developed by Vladislav Zdolnikov, a long-time FBK contributor and IT-entrepreneur (TgVPN 2017). The bot, launched in May 2017, allows for quick delivery of VPN services via Telegram messenger and offers an easy way to begin using the anti-surveillance technology that also allows access to websites banned in Russia. Most recently, Navalny's campaign headquarters organised a hackathon (a collaborative coding and prototyping event) for activists and volunteers to develop digital solutions for the campaign and the activist community around it (Navalny 2017).



Облако #002. Гость — Петр Диденко, «Общество защиты интернета». Tor, анонимность и обход блокировок

76,651 views

Figure 2. *Screen grab from YouTube talk show "The Cloud," hosted by Leonid Volkov, explaining the basics of the Tor network. Episode 002 was devoted to online anonymity and circumventing website blocks.*

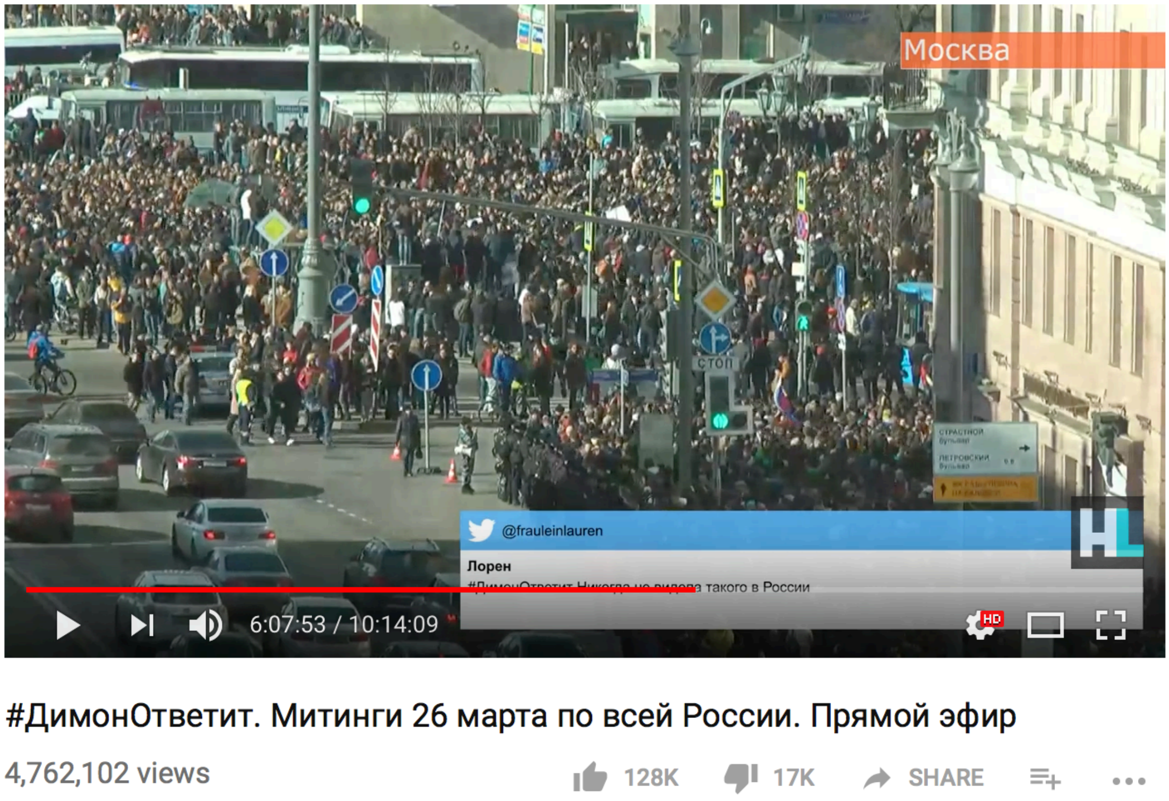
Public management of state surveillance through explicit acknowledgment, analysis, and mitigation of risks makes these security practices conspicuous given FBK's usual online activity as political and anti-corruption activists. But how do they negotiate security and risk awareness while also being highly visible?

Strategic Visibility Practices

The focus on raising awareness of surveillance and offering tactics to mitigate it and increase digital literacy through conspicuous security practices is further buttressed as a surveillance management tactic by strategic choices that FBK activists and their allies make about their public visibility in online spaces. This focus on "strategic visibility" is intentional, as the tensions between private and public lives and spaces of Russian dissidents and citizens go back in history. Siegelbaum notes that in totalitarian regimes (of which the Soviet Union is an example), the state exerts "an all-embracing despotic interference in all manifestations of life" and that the Soviet period was characterised by "a balanced system of total surveillance" (Siegelbaum 2006: 2), but he also cautions against false dichotomies in the public–private debate. Indeed, the public and private spheres in the lives of Soviet citizens were complex and often multiple, as exemplified by the co-existence of the official and informal publics (Zdravomyslova and Voronkov 2002) and the dissonance between centralised state surveillance and the doublethink and performative self-surveillance of the everyday Soviets (Levina 2017).

To some extent, the advent of the internet has granted ordinary citizens, and Russian dissidents in particular, a greater measure of control over their private sphere and their public image, but the state has been quick to move in on the free territory. As the activists find their private spheres under threat of constant surveillance as much as their public work, they choose to exercise the control they do have online over what to reveal and to what effect. Such strategic visibility work often seeks to forestall state-sanctioned leaks or accusations of unscrupulous activity thrown against the opposition members. In this way, by taking back some control and being visible on their own terms, the activists' visibility practices serve as a mechanism of resisting the state surveillance apparatus. The observation and analysis of public online activities of the FBK community and their allies allows one to outline four different kinds of practices that contribute to the community's strategic visibility mechanism:

1. Networked sharing: As a combined measure against both state censorship and state surveillance, FBK and other opposition activists actively use all available informal channels to remain visible and accessible. As they are basically barred from state-run federal media and exercise little control over state media narratives, they resort to alternative channels such as Telegram messenger and Facebook. They frequently post and share promos of their own investigative and activist content and on-the-ground activity, often produced in-house and then broadcast on YouTube or teased on Twitter. They also actively use memes and viral content, exploiting the networked logic of spreadable media (Jenkins, Ford, and Green 2013).
2. Real-time content delivery: This strategy relies on the use of modern technology to enable things such as live streams from protests, live casting of interviews or daily news briefs, YouTube-powered online real-time shows, and updates on court hearings provided as live text blogs. Using unedited content delivered to the viewers or readers in real-time mode increases trust (as there are no edits) and allows activists to bypass mainstream media frames or silence. Especially for offline events such as protests and court hearings, if anything does happen it is immediately documented and made public, negating the need for surveillance as the activists make the choice in advance to be seen. For instance, the large-scale anticorruption protests on March 26, 2017, had FBK delivering syndicated live streams from rallies around Russia, showing both the scale and the breadth of the rallies, as well as documenting arrests and police brutality (see Figure 3).
3. Radical transparency: As financial and operational surveillance of FBK work is widespread, the organisation and its community have made a conscious choice to be public and transparent about their funding, budgets, and other activity. They regularly publish financial reports (Anti-Corruption Foundation 2017b), explanations on how their campaigns were run, offering behind the scenes content, instructions on how to build and run campaigns or investigations, as well as photos and video reports from on-the-ground activity. Such radical transparency seeks to raise the level of trust among the community's supporters, but also to neutralise ongoing and potential surveillance efforts by the state and security services aimed at extracting information that could be used to discredit the activists.
4. Counter-surveillance: As part of their overall dissent strategy and activist tactics, FBK community members are actively engaged in counter-surveillance measures against state officials and security services. In their investigative anti-corruption work, they use public online records, social media data, and even volunteer-made drone videos to investigate Russian officials' financial dealings and real estate and money-laundering schemes. Activists also engage in reverse surveillance of law enforcement during protest rallies by posting regular updates to social media and providing photographic and video evidence of police presence, police surveillance efforts, and any altercations or arrests. They also educate citizens about their rights with regard to documenting police presence at such events.



@frauleinlauren

Лорен

#ДимонОтветит Никогда не видела такого в России

#ДимонОтветит. Митинги 26 марта по всей России. Прямой эфир

4,762,102 views

Figure 3. *Screen grab of YouTube live stream syndicated by FBK during the March 26, 2017, anti-corruption protests in Russia.*

In a climate of normalised state surveillance, Russian opposition activists seek to retain some measure of control on the remaining discursive spaces in the online sphere. To continue their political and anti-corruption work, they find they must now engage with issues of information security in public and conspicuous ways. But this strategic approach also extends to their own visibility online as a means of mitigating the risks of surveillance and retaining control over the outcomes of their actions and narratives. While some of the strategic visibility practices, such as counter-surveillance and networked sharing, are reactive, others, such as real-time broadcasting and radical operational transparency, seek to forestall state surveillance attempts and exercise power to shape the activist narrative on their own terms. By making both their security practices and their political work highly visible, Russian opposition activists offer their supporters new models of resistance to the state surveillance apparatus.

Conclusions

This study examined how Russian opposition activists, specifically members of Alexey Navalny’s FBK (Anti-Corruption Foundation) community, manage the persistent threats and risks posed by digitally enabled state surveillance in Russia’s conditions of networked authoritarianism. The study drew on the concept of media practices and its application to the study social movements to analyse the intersection of media technologies and actors in political contexts to consider how political activists adapt and integrate the changing media practices in the hybrid media system. By examining the internet-based activities of Russian opposition activists in light of the long history of state surveillance in Russia, the paper traced connections between activists’ everyday online security practices and the resistance tactics and strategies they enact in an increasingly hostile environment with shrinking space for free expression and dissent.

The paper used virtual ethnography (netnography) to conduct observation of public opposition websites, related Twitter feeds, YouTube channels, and Telegram channels to capture a range of public online mediated practices of Russian opposition activists and to draw conclusions about the challenges they face while negotiating state surveillance, managing their own digital and physical security, and maintaining the visibility of their resistance efforts. The study also theorises about how these individual mediated practices can inform the broader mechanisms of resistance used by the activist community. In this way, the study contributes to existing research on surveillance in post-Soviet states by considering the implications of individual and community activist online practices aimed at managing state surveillance. The observation was complemented by the analysis of relevant media coverage in Russia and beyond. Though (virtual) ethnography has its limitations, it was a viable non-reactive approach to collecting data on public online activity of individuals and communities that has been used in the study of activism. Future research in this area could be expanded to involve surveys or interviews with members of the activist community in order to gain a deeper understanding of the motivations and decisions made about their online activities and strategies.

The analysis found that in an environment where state surveillance is increasingly normalised, Russian opposition activists employ a number of practices to construct a mechanism of conspicuous security online. They promote digital, media, and security literacy and increasingly default to using security tools and protocols such as VPN, two-phase authentication, and encrypted messaging in their daily online work. Beyond digital literacy efforts, FBK activists employ conspicuous security practices by making public examples of known surveillance cases and attacks against them; by moving away from Russian social media platforms and services, and hosting their content and data on servers outside of Russia; and by directly participating in the development and creation of anti-surveillance and digital security tools. These literacy and security efforts underscore the ongoing battle for control over digital online platforms and their users between the state and its discontents. In Russia's regime of "networked authoritarianism," the state is becoming increasingly adept at using technology to police online speech and expressions of protest, while attempting to exert control over every sphere of mediated political and social life.

Furthermore, the analysis revealed that Russian activists have to balance the need for security with the struggle for control over visibility, an important factor for entering the mainstream political and social discourse. However, visibility is traditionally seen as a necessary condition of surveillance, so activists must mitigate its threats while reaping its benefits. They make use of their visibility in strategic ways by exploiting the internet's affordances for real-time reporting and networked message sharing; by engaging in radical transparency with regards to their funding and operational practices; and by employing a range of counter-surveillance measures against the state and security service apparatus. As a result, their practices online underscore the contrast between the possibilities offered by internet freedom and the constraints imposed on it by Russian internet censors and law enforcement.

These tactics, therefore, illuminate the stark differences between online activism in democratic or free states and online activism in a networked-authoritarian state such as Russia. In democracies, activists avail themselves of the visibility the internet and social media afford to mobilise support for their cause or to draw attention to their messages. But in Russia, this dynamic is more complex. While allowing FBK and their fellow activists to raise their political profile and engage in productive dissent to some extent, their "strategic visibility" and "conspicuous security" mechanisms also act as insurance against pervasive surveillance that endangers their livelihood and threatens to undermine their resistance work. This tension between being secure and being visible is a key characteristic of online resistance practices in an environment of near-constant state pressure and oversight, as Russian activists concurrently manage their safety and visibility online to minimise the risks posed by government surveillance and maximise the effect of their activism. Further interdisciplinary research in other non-democratic or authoritarian states might consider extending this inquiry into online visibility and public activist practices as a means of resistance to or management of state surveillance.

References

Anti-Corruption Foundation. 2017a. About Us. https://fbk.info/english/about/ [accessed August 2, 2017].

Anti-Corruption Foundation. 2017b. Отчеты. [Reports.]. https://fbk.info/about/reports/ [accessed August 2, 2017].

Chadwick, Andrew. 2013. *The Hybrid Media System: Politics and Power*. Oxford: Oxford University Press.

Chen, Adrian. 2015. The Agency. *New York Times,* June 2, 2015. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Citizen Lab. 2015. Citizen Lab Summer Institute. Last modified June 19, 2015. https://citizenlab.ca/summerinstitute/2015.html.

Couldry, Nick. 2004. Theorising Media as Practice. *Social Semiotics* 14 (2): 115–32.

Couldry, Nick. 2012. *Media, Society, World: Social Theory and Digital Media Practice*. Cambridge, UK: Polity.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Miklos Haraszti. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

Deibert, Ronald. 2016. Cyberspace under Siege. In *Authoritarianism Goes Global: The Challenge to Democracy*, edited by Larry Diamond, Marc F. Plattner, and Christopher Walker, 198–215. Baltimore, MD: Johns Hopkins University Press.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press.

Ermoshina, Ksenia, and Francesca Musiani. 2017. Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. *Media and Communication* 5 (1): 42–53.

Gel'man, Vladimir. 2015. Political Opposition in Russia: A Troubled Transformation. *Europe-Asia Studies* 67 (2): 177–91.

Gorny, Eugene. 2007. The Russian Internet: Between Kitchen-Table Talks and the Public Sphere. *Art Margins*. http://www.artmargins.com/index.php/2-articles/145-the-russian-internet-between-kitchen-table-talks-and-the-public-sphere.

Greene, Samuel. 2012. How Much Can Russia Really Change? The Durability of Networked Authoritarianism. *PONARS Policy Memo*. http://www.ponarseurasia.org/memo/how-much-can-russia-really-change-durability-networked-authoritarianism.

Gunitsky, Seva. 2015. Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. *Perspectives on Politics* 13 (1): 42–54.

Hanson, Elizabeth C. 2008. *The Information Revolution and World Politics*. Lanham, MD: Rowman & Littlefield.

Hine, Christine. 2000. *Virtual Ethnography*. Thousand Oaks, CA: Sage.

Holquist, Peter. 1997. Anti-Soviet Svodki from the Civil War: Surveillance as a Shared Feature of Russian Political Culture. *Russian Review* 56 (3): 445–50.

Jenkins, Henry, Sam Ford, and Joshua Green. 2013. *Spreadable Media: Creating Value and Meaning in a Networked Culture*. New York: New York University Press.

Kozinets, Robert V. 2010. *Netnography: Doing Ethnographic Research Online*. London, UK: Sage.

Kratasjuk, Ekaterina. 2006. Construction of "Reality" in Russian Mass Media News on Television and on the Internet. In *Control + Shift: Public and Private Usages of the Russian Internet*, edited by Natalja Konradova, Henrike Schmidt, and Katy Teubener, 34–50. Norderstedt, Germany: Books on Demand.

Laruelle, Marlene. 2014. Alexei Navalny and Challenges in Reconciling "Nationalism" and "Liberalism." *Post-Soviet Affairs* 30 (4): 276–97.

Levina, Marina. 2017. Under Lenin's Watchful Eye: Growing Up in the Former Soviet Union. *Surveillance & Society* 15 (3/4): 529–34.

Litreev, Alex. 2017. Мы запускаем Красную Кнопку. [We are Launching the Red Button.]. Telegram channel post, April 22, 2017. http://telegra.ph/My-zapuskaem-Krasnuyu-Knopku-04-22.

Lokot, Tetyana. 2014. Blogger Law Traps Russia's Activists in Limbo. *Moscow Times,* August 21, 2014. https://themoscowtimes.com/articles/blogger-law-traps-russias-activists-in-limbo-38606.

Lokot, Tetyana. 2016. Is Telegram Really Safe for Activists Under Threat? These Two Russians Aren't So Sure. *Global Voices*, May 2, 2016. https://globalvoices.org/2016/05/02/is-telegram-really-safe-for-activists-under-threat-these-two-russians-arent-so-sure/.

Luganskaya, Dariya. 2017. OpenEconomy: как российские власти будут контролировать интернет. Три основных способа. [OpenEconomy: How the Russian Authorities Will Control the Internet. Three Main Ways.] *OpenRussia*, April 23, 2017. https://openrussia.org/notes/708721/.

Lunden, Ingrid. 2016. LinkedIn Is Now Officially Blocked in Russia. *TechCrunch*, November 17, 2016. https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/.

Lyon, David. 2007. *Surveillance Studies: An Overview.* Cambridge, UK: Polity.

Lysenko, Volodymyr V., and Kevin C. Desouza. 2014. Charting the Coevolution of Cyberprotest and Counteraction: The Case of Former Soviet Union States from 1997 to 2011. *Convergence* 20 (2): 176–200.

MacKinnon, Rebecca. 2011. China's 'Networked Authoritarianism'. *Journal of Democracy* 22 (2): 32–46.

MacKinnon, Rebecca. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Maréchal, Nathalie. 2017. Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication* 5 (1): 29–41.

Mattoni, Alice. 2016. *Media Practices and Protest Politics: How Precarious Workers Mobilise*. New York: Routledge.

Mattoni, Alice, and Emiliano Treré. 2014. Media Practices, Mediation Processes, and Mediatization in the Study of Social Movements. *Communication Theory* 24 (3): 252–71.

Meduza. 2017. Russia's Senate Adopts New Legislation Cracking Down on Internet Anonymity. All That's Left Now Is Putin's Signature. *Meduza*, July 25, 2017. https://meduza.io/en/news/2017/07/25/russia-s-senate-adopts-new-legislation-cracking-down-on-internet-anonymity-all-that-s-left-now-is-putin-s-signature.

Monahan, Torin. 2011. Surveillance as Cultural Practice. *The Sociological Quarterly* 52 (4): 495–508.

Moscow Times. 2017. Council of Europe Says Navalny Should Be Allowed to Run for President. September 22, 2017. https://themoscowtimes.com/news/council-of-europe-demands-alexei-navalny-be-allowed-to-run-for-president-59016.

Navalny, Alexey. 2015. Страшный суд над 'хакером' 'Хэллом'ю 24 июня, Бонн. [Judgement Day for 'Hacker' 'Hell'. June 24, Bonn.]. Navalny.com, June 18, 2015. https://navalny.com/p/4305/.

Navalny, Alexey. 2016. Нападение на мужа юриста ФБК Любови Соболь. [Attack on the Husband of FBK Lawyer Lyubov Sobol.]. Navalny.com, November 28, 2016. https://navalny.com/p/5142/.

Navalny, Alexey. 2017. Сегодня и завтра у нас хакатон. [Today and Tomorrow We Are Running a Hackathon.]. *Navalny.com,* August 12, 2017. https://navalny.com/p/5495/.

Navalny LIVE. 2017. The Cloud #002. Navalny LIVE, May 30, 2017. https://youtu.be/gKdFEoaTqLs.

Oates, Sarah. 2013. *Revolution Stalled: The Political Limits of the Internet in the Post-Soviet Sphere*. New York: Oxford University Press.

Ognyanova, Katherine. 2015. In Putin's Russia, Information Has You: Media Control and Internet Censorship. In *Management and Participation in the Public Sphere*, edited by Mika Markus Merviö, 62–78. Hershey, PA: IGI Global.

Oliphant, Roland. 2013. Alexei Navalny Rattles Kremlin in Moscow Mayoral Race. *Telegraph* (UK), September 7, 2013. http://www.telegraph.co.uk/news/worldnews/europe/russia/10293384/Alexei-Navalny-rattles-Kremlin-in-Moscow-mayoral-race.html.

Privacy International. 2013. Lawful Interception: The Russian Approach. *Privacy International*, March 4, 2013. https://www.privacyinternational.org/node/314.

Salmonds, Janet. 2015. *Doing Qualitative Research Online*. Thousand Oaks, CA: Sage.

Siegelbaum, Lewis H. 2006. Introduction: Mapping Private Spheres in the Soviet Context. In *Borders of Socialism: Private Spheres of Soviet Russia*, edited by Lewis H. Siegelbaum, 1–21. New York: Palgrave Macmillan US.

Soldatov, Andrei, and Irina Borogan. 2015. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. New York: Public Affairs.

Soldatov, Andrei. 2017. What Wikileaks' SpyFiles Tell About Russia. Agentura.ru, September 23, 2017. http://www.agentura.ru/english/projects/Project_ID/wlspyfiles/.

TgVPN. 2017. VPN в Telegram. [VPN in Telegram.] *Medium.com*, May 31, 2017. https://medium.com/@TgVPN/vpn-%D1%81%D0%B5%D1%80%D0%B2%D0%B8%D1%81-%D0%B2-telegram-b63f1d02a6b0.

Thornton, Rod. 2015. The Changing Nature of Modern Warfare: Responding to Russian Information Warfare. *The RUSI Journal* 160 (4): 40-48.

Toler, Aric. 2015. Inside the Kremlin Troll Army Machine: Templates, Guidelines, and Paid Posts. *Global Voice*, March 14, 2015. https://globalvoices.org/2015/03/14/russia-kremlin-troll-army-examples/.

Weiner, Amir, and Aigi Rahi-Tamm. 2012. Getting to Know You: The Soviet Surveillance System, 1939–57. *Kritika: Explorations in Russian and Eurasian History* 13 (1): 5–45.

White, David. 2015. Political Opposition in Russia: The Challenges of Mobilisation and the Political–Civil Society Nexus. *East European Politics* 31 (3): 314–25.

Zdravomyslova, Elena, and Viktor Voronkov. 2002. The Informal Public in Soviet Society: Double Morality at Work. *Social Research: An International Quarterly* 69 (1): 49–69.