International Journal of Communication 18(2024), 2731-2752 1932–8036/20240005

Firewalls Have Ears: How Horizontal Privacy Regulation Influences Online Political Expression in Russia

AYSENUR DAL♦[1]
Bilkent University, Türkiye

In authoritarian settings, dealing with privacy threats involving vertical (i.e., institutional) and horizontal (i.e., social) intrusions is an essential element of the day-to-day negotiation of online activism risks. Accordingly, this study investigates the role that horizontal privacy regulation efforts play in citizens' decision-making about online political expressions (OPE) on controversial topics under digital repression. Using a web-based survey of Internet users (*N* = 992) conducted in 2018, the findings reveal that, while horizontal privacy regulation significantly predicts a weaker intention to engage in OPE about governmental corruption in Russia, this negative effect is amplified by how much one cares about others' judgments about their position on corruption.

Keywords: privacy regulation, horizontal privacy, online political expression, self-disclosure, Russia

Although the potential visibility of one's political self-disclosure on social media plays an important role in raising awareness about and seeking solutions for contentious issues, the low levels of expenditure on the time, energy, and effort required for online political expression (OPE) do not equate to low levels of negative consequences. The legal, political, and physical sanctions associated with citizens' OPE can become quite severe, especially under authoritarian governance, such that even the most effortless online activities (e.g., liking a post) may pose serious risks that stem from both vertical (e.g., government tracking) and horizontal (e.g., friends' surveillance) privacy violations (Poupin, 2021; Roberts, 2020). Within this context, behavioral responses, such as privacy regulation, about who (or what) may view or access the risky content one posts online become key in examining the social-psychological mechanisms underlying citizens' OPE under authoritarian governance.

Horizontal and vertical privacy violations are simultaneously and often subtly carried out by fellow social media users and institutions (e.g., the government and companies), respectively. The hard-to-discern

Aysenur Dal: aysenur.dal@bilkent.edu.tr
Date submitted: 2023-10-02

[1] I would like to express my sincere thanks to Erik C. Nisbet and Olga Kamenchuk for their support in the survey construction, translation, and data collection; Efe Tokdemir, Seçkin Köstem, and the anonymous reviewers for their insightful suggestions; and Selin Küçükoruç and Ece Dede for their research assistance. I also acknowledge the support of the Young Scientists Award Program of the Science Academy, Türkiye.

mismatch between intended and unintended (or unwanted) audiences resulting from context collapse on social media is known to push individuals to use strategies targeting the perceived risks associated with their online expression (Litt & Hargittai, 2016; Marwick & boyd, 2011; Mor, Kligler-Vilenchik, & Maoz, 2015). These strategies may be in the form of practicing self-disclosure based on what one thinks others know about oneself (Leonardi, 2014; Pearce, Vitak, & Barta, 2018) or engaging in specific privacy regulating behaviors to manage which information about oneself other individuals or institutions can access (Baruh, Secinti, & Cemalcilar, 2017; Quinn, Epstein, & Moon, 2019; Raynes-Goldie, 2010).

From a citizen-centric perspective, individuals who face risks associated with online political self-disclosure must rely on their own judgments about uncertainties about privacy violations. In this regard, prior findings demonstrate that individuals report greater concerns about horizontal privacy threats on social media compared to vertical ones (Afriat, Dvir-Gvirsman, Tsuriel, & Ivan, 2021; Jozani, Ayaburi, Ko, & Choo, 2020; Ranzini, Lutz, & Hoffman, 2023; Sujon, 2018). While the potential explanations for the greater apprehension experienced with horizontal privacy threats include lack of awareness about, difficulty in understanding processes regarding, and cynicism toward vertical processes, studies bringing such findings forward focus predominantly on democratic settings. Meanwhile, most studies about online privacy in authoritarian contexts, where state surveillance is already the norm, focus on vertical privacy processes and thus create a lacuna of research about ordinary citizens' experiences with regulating their horizontal privacy on social media.

Building on prior work on online political activism and public perception of self-disclosure and using a web-based survey of 992 Internet users conducted in Russia in 2018, this study investigates the role that horizontal privacy regulation efforts play in OPE regarding controversial topics in authoritarian settings. The findings reveal that while the frequency of horizontal privacy regulation significantly predicts a weaker intention to engage in OPE on a risky political topic (i.e., governmental corruption), this negative effect is amplified by how much one cares about others' judgments of their position on the topic of expression.

The contribution of this research is threefold. First, by considering the different dimensions of privacy in an authoritarian context, the current study offers a nuanced understanding of the role that horizontal dynamics play in suppressed Internet users' political self-disclosure experiences. Second, by introducing impression-relevant involvement as a moderator for understanding political self-disclosure, the findings expand our knowledge of the boundary conditions that privacy research should investigate with regard to OPE. Third, by focusing on an understudied political context, it advances comparative privacy research beyond the WEIRD (i.e., Western, educated, industrialized, rich, and democratic) settings (Henrich, Heine, & Norenzayan, 2010; Masur et al., 2021; Wu, Vitak, & Zimmer, 2020).

Theoretical Framework

OPE as a Self-Disclosure Behavior

Online political expression is a form of digitally networked political participation that allows for an autonomous and activism-centered citizenship that is closely connected to the idea of activating one's social networks (Theocharis, 2015). Current social media platforms allow individuals to interact with the

connections they selectively form with both narrow and broad audiences at a relatively low cost (Bayer, Trieu, & Ellison, 2020; boyd & Ellison, 2007). Accordingly, unlike other modes of political participation, such as voting or protesting (Margetts, John, Hale, & Yasseri, 2016; Vaccari et al., 2015), OPE enjoys low barriers of entry. Besides its potential to serve as a gateway to other forms of individual political engagement (Bode, 2017), OPE is particularly important because it facilitates making one's political preferences, aspirations, and dissatisfaction known to fellow citizens and authorities, which is a fundamental aspect of democratic citizenry in specific and political socialization in general.

In line with its intentional and goal-directed nature, OPE is a form of self-disclosure, that is, "a process of making the self known to others" (Jourard & Lasakow, 1958, p. 91; Taddicken, 2014; Theocharis, 2015). From a privacy-centered approach, it is also linked to the extent of individuals' control over others' exposure to, or dissemination of, such information, namely informational privacy (Baruh et al., 2017; Nissenbaum, 2010). Online self-disclosure serves several functions, including identity development, social validation, relationship building, and emotional release (Bazarova & Choi, 2014; Cheung, Lee, & Chan, 2015), parallel with the functions of OPE. However, it may also involve a loss of control when sensitive information is shared, or in the case of rejection or disapproval by the audience, loss of friends, or the potential to hurt someone (Kruse, Norris, & Flinchum, 2018; Quinn & Epstein, 2018), which may result in severe consequences in authoritarian contexts when performed as contentious OPE.

Regulating Privacy for OPE

Scholars build on different perspectives as to why, how, and under what conditions individuals' desire to protect their online privacy turns into deliberate acts of protection or regulation. According to one of these views, individuals continuously exercise privacy regulation, as it is their right to determine the particular rules around the release and ownership of their private information in online settings (e.g., Baruh et al., 2017), similar to their interpersonal experiences (Petronio, 2002). While some of these rules may necessitate acts that are preventive in nature (e.g., filtering recipients, using pseudonyms), others may be along the lines of correcting one's already violated privacy (e.g., removing one's name tag from photos uploaded by others; see Masur, 2018, for a review).

These strategies aim to safeguard individuals' online privacy from horizontal and vertical intrusions. Whereas the former concerns violations performed by other individual users or one's social contacts, the latter concerns institutional actors, such as governments and service providers, as violators (Bazarova & Masur, 2020). Prior works on Internet users' understanding of online privacy suggest that these dimensions overlap with lay conceptualizations of privacy (Quinn et al., 2019), with horizontal privacy concerns observed to be more salient and substantial for individuals (Afriat et al., 2021; Jozani et al., 2020; Lutz & Ranzini, 2017; Sujon, 2018).

The extent to which individuals take deliberate actions to regulate their horizontal and vertical privacy levels primarily stems from their desired level of privacy (Altman, 1975)—a key construct for self-disclosure. When individuals fail to achieve this level, they may either adjust the privacy context or adapt their level of self-disclosure to the level of privacy available to them (Dienlin, 2015). In privacy research, there is ample empirical evidence demonstrating that active privacy regulation increases online self-

disclosure (Chen, 2018; Chen & Chen, 2015; Mak, Koo, & Rojas, 2022). While the content of online self-disclosure may vary largely, a recent study focusing on OPE on Twitter, for instance, found that changing privacy settings to manage social media audiences was associated with being more likely to tweet (Parviz & Piercy, 2021).

Negotiating Privacy Risks in Authoritarian Settings

Online political expression can be risky for individuals in both democratic and authoritarian settings. Nonetheless, the latter poses a wider range and severity of challenges to citizens' daily experiences, especially in terms of vertical threats via an unpredictable and inconsistent mix of strategies that involve monitoring and punishing citizens' OPE (Earl, Maher, & Pan, 2022; Kendall-Taylor, Frantz, & Wright, 2020; Roberts, 2020; Sanovich, Stukal, & Tucker, 2018). Likewise, previous research has shown that suppressed individuals resort to tactics such as highlighting humor elements in their political remarks (Chunly, 2020), performing self-censorship (Koçer & Bozdağ, 2020), or engaging in anonymization or circumvention when it comes to risky political expression (Honari, 2018). Within this framework, repressive strategies do not altogether stop citizens from countering their governments in online spaces despite the perceived risks, which makes unpacking what goes into these suppressed individuals' decision-making processes particularly important (e.g., Dal, Nisbet, & Kamenchuk, 2023; Pearce et al., 2018).

Thus, from the perspective of individuals living under authoritarianism, it is useful to handle privacy regulations as part of a larger problem stemming from governments' efforts to communicate to their citizens that contentious OPE would be *more trouble than it is worth.* In other words, privacy concerns and threats about self-disclosing political views that contradict or challenge authoritarian incumbents should be considered components of how citizens negotiate the risks of digital repression.

On the one hand, while engaging in privacy regulation may be expected to make citizens feel more confident about and in control of their online privacy, in authoritarian settings, it may make digital repression even more salient for citizens and result in a weaker intention to engage in political self-disclosure online. On the other hand, if citizens experience hopelessness coupled with disillusionment regarding exercising their freedom of speech online, this could lead to a form of apathy or cynicism toward available regulation tactics, especially for vertical privacy intrusions (Hoffmann, Lutz, & Ranzini, 2016; van Ooijen, Segijn, & Opree, 2022).

In this work, I focus on the horizontal dimension of online privacy because of its relatively more tangible dynamics for social media users compared with the often subtle vertical privacy violations of digital repression. Suppressed citizens' concerns about and efforts to regulate the social visibility of their online political self-disclosure become directly associated with their negotiation of the risks of online activism, as OPE is a matter of a "delicate act of impression management" (Mor et al., 2015, p. 1). A qualitative study focusing on horizontal dynamics conducted in the authoritarian context of Azerbaijan revealed that socially mediated visibility on social media platforms paves the way for both the benefits and risks associated with contentious OPE (Pearce et al., 2018). While the visibility of one's dissent may eventually lead to raising awareness or ensuring support from like-minded people, it may also lead to uncivil reactions from others, relationship turbulence, or even dealing with police informers.

Thus, when it comes to the visibility of one's OPE via horizontal dynamics, one ends up dealing with a double-edged sword. First, vertical privacy violations may exploit citizens' social media connections (i.e., horizontal dynamics) through passive listening or monitoring. Citizens may unintendedly put their friends or families at political risk when they engage with their online content (e.g., liking, reposting, and commenting on), making them not only more visible to other users but also vulnerable to vertical intrusions. As a result, the networked and collective nature of online privacy may activate vertical privacy threats via horizontal dynamics. Second, besides the institutional efforts authoritarian governments put into monitoring dissenters, it is not uncommon to see leaders encouraging their base to inform against fellow citizens in the name of patriotism or civic duty (e.g., Dixon, 2023, para. 2; Troianovski et al., 2023, para. 3). Considering the sheer volume of online content produced on which governments can practice surveillance directly or indirectly via other citizens, snitching on others inevitably becomes a valuable act of cooperation with digital repression.

The Russian Context

Individuals' privacy as a concept has been contested in Russia in both the Soviet and post-Soviet eras in line with the long-established culture of state surveillance (Lokot, 2020). The word "privacy" does not have a literal Russian translation that follows the concept's Western roots and connotations. Likewise, the terminology used in the Russian Constitution consists of adjectives that stand for *personal*, *particular*, or *separate* life instead. Similarly, the lack of explicit regulation of a fundamental right for private information/data protection in the current legal system is in tune with the remnants of the Soviet era, including limited self-determination in information disclosure practices—a key aspect of privacy (Saponchik, 2022). According to an in-depth analysis of how privacy is interpreted by the Russian state's Internet regulator vs. one of the most prominent grassroots advocacy groups for digital rights, the state regards itself as the grantor of protection against external (i.e., foreign) threats targeting citizens who are "vulnerable data subjects with little agency" as opposed to individuals who can exercise privacy as a human right (Lokot, 2020, p. 320). Not surprisingly, this approach also results in state institutions regularly exercising power to withhold online privacy and eventually shaping OPE experiences for ordinary Internet users.

Within the last decade, the Russian government's gradual tightening of citizens' freedom of speech and the threat against privacy in online spaces have created a risk environment, especially for Internet users with political views that challenge the regime and its representatives (Nisbet, Kamenchuk, & Dal, 2017; van der Vet, 2019). As the most recent wave of digital repression, the Russian government's handling of citizens' digital communication regarding Russia's full-scale invasion of Ukraine resulted in Russia reaching the lowest point in Internet freedom rankings (Freedom House, 2023).

Along with heavily controlling the legacy media to ensure the dissemination of state propaganda, the Russian government has demonstrated to citizens that expressing opinions on such sensitive topics may lead to severe consequences that can be triggered by fellow citizens (Dixon, 2023; Izadi & Ellison, 2022; Troianovski et al., 2023). In Russia, posting online content that "exhibits blatant disrespect for the society, government, official government symbols, constitution or governmental bodies" can result in fines and jail time (Freedom House, 2023, para. 170). When applied to topics like governmental corruption, any post

mentioning allegations or posing mere questions that hold the government accountable for its actions may easily make citizens feel that they hang by a thread. Similarly, in March 2022, the criminal code was amended in such a way that spreading "knowingly false information" about the Russian armed forces and their actions could result in severe consequences, ranging from heavy fines to 15 years in prison. Here, what is particularly puzzling for ordinary citizens is that terms appearing in Internet laws (e.g., defamation of power, justifying extremism) make it difficult to assess legal boundaries when discussing contentious issues. Since these terms potentially make concerning laws look conducive to being used against citizens whenever the government deems necessary, the resulting risk atmosphere means a constant struggle with uncertainty and fear, not only for journalists and activists but also for ordinary citizens.

Despite these measures, however, the digital information environments in Russia still serve as alternatives to state-controlled media and host cycles of mobilization for different causes. Social media in Russia are tools for both state control and protest when it comes to ordinary citizens' online practices (Lonkila, 2016; Lonkila, Shpakovskaya, & Torchinsky, 2020). Nevertheless, this dual role of social media does not stop citizens from engaging in OPE on platforms that they deem subject to government surveillance. For example, although the largest social media platform VKontakte's ownership has close ties with the Kremlin (unlike its previous owner who had to flee the country due to political pressures), individual users continue to post critical content on the platform for contentious issues, as was the case during the anti-waste protests in 2018 (Poupin, 2021).

Hence, vertical privacy intrusions in Russia are by no means unexpected, although they can be subtle and more extensive than anticipated (Sanovich et al., 2018). In response to both platform-specific and grassroots efforts to resist vertical privacy threats, the Russian government has made it even more difficult to remain anonymous—banning VPNs, requesting the collection of users' private information from companies, or making it mandatory to preload smartphones with Russian software (Baker & Hamilton, 2021)—in online spaces under the pretext of security purposes. However, it remains an empirical question as to what extent one can have a nuanced understanding of citizens' OPE by simply focusing on the vertical dimension of privacy, given the possibility of horizontal privacy dynamics playing a more prominent role in immediate decision-making regarding individuals' online experience.

Current Study

When faced with digital repression in contexts such as Russia, citizens can experience the chilling effects of self-censorship or self-withdrawal from platforms (Huang, 2015; Parks & Mukherjee, 2017). Alternatively, they can be motivated to exhibit psychological reactance to limits to their freedom of expression, which may then push them to take deliberate actions to restore their freedom (Behrouzian, Nisbet, Dal, & Çarkoğlu, 2016; Roberts, 2020). To this end, privacy regulation efforts could either be reminders of why such chilling effects occur or tools for restoring one's freedoms in digital spaces.

The current study builds on the idea that when the prevalence of vertical privacy threats leads individuals to accept such practices as already happening in the background, further unpacking horizontal privacy dynamics about the citizens' OPE experience will be more informative. Horizontal violations regarding one's OPE could also be linked to negative outcomes that are institutional rather

than social (e.g., a social media connection acting as an informant for the police) in practice. However, in light of prior work on the dimensions of online privacy, the agency individuals technically have in regulating their horizontal privacy may still be perceived as being more about individual efforts within platforms' privacy features than about vertical limitations. Accordingly, the current study primarily addresses the following research question:

RQ1: How does horizontal privacy regulation play into suppressed individuals' intention to engage in OPE about a sensitive topic on social media?

Although empirical evidence from Western contexts mostly suggests that privacy-regulating behaviors primarily serve to make individuals feel more confident about self-disclosure, they may not be sufficient to allow suppressed individuals to feel safe enough to post on social media about topics that are sensitive and risky to challenge or even mention publicly. Namely, previous engagement in privacy regulation may serve two potential functions: (1) helping individuals feel more capable of using their agency and skills to bring their privacy closer to the desired levels, and (2) making privacy threats more salient as they remind individuals that there is an imminent threat they have to tackle. Therefore, the current study tested the following alternative hypotheses in the context of Russia:

H1a–b: Engaging in horizontal privacy regulation will be significantly associated with a (a) stronger (b) weaker intention to engage in OPE about a sensitive topic.

The current study also introduces impression-relevant involvement as a potential moderator of the hypothesized relationship between horizontal privacy regulation and OPE. Defined as "the public perception of the self" (Cho & Boster, 2005, p. 239), impression-relevant involvement concerns individuals' reservations about the extent to which their opinions would be socially acceptable (Johnson & Eagly, 1989). Those who score high on impression-relevant involvement tend to act in accordance with their imagined audiences (Lapinski, Zhuang, Koh, & Shi, 2017; Marshall, Reinhart, Feeley, Tutzauer, & Anker, 2008) and potentially engage in tactics of moderation in tone or content.

When dealing with threats to privacy, impression-relevant involvement may play a role in determining the strength of the link between taking precautions regarding what is visible to others on social media and the intention to disclose one's political self. When self-disclosure involves a sensitive topic in an authoritarian setting, how others perceive one's political self (e.g., supporting vs. opposing the government) may matter from a risk perspective. Similar to the role perceived vulnerability plays in subjective evaluations of threats (Witte, 1994), socially mediated visibility (Pearce et al., 2018) of one's OPE may amplify the likelihood or severity of negative outcomes that are primarily social in nature, such as being reported to authorities, being attacked, or getting flagged by fellow users. Overall, considering the potential importance of public perceptions in how horizontal privacy regulation functions in authoritarian contexts, the study hypothesizes the following relationship:

H2: Impression-relevant involvement moderates the relationship between horizontal privacy regulation behaviors and OPE about a sensitive topic.

Method

Data Collection

The data used in the analyses came from a self-administered web survey (translated by a former Russian journalist) of adults who resided in Russia. The survey instrument was approved by an American research university's Institutional Review Board. The recruitment of respondents was done via a Russian online commercial opt-in panel that Qualtrics had contracted, and the respondent eligibility required using at least one social media platform. The sample size (N = 992) was determined based on the statistical requirements of the experiment embedded in the survey. Furthermore, for quality purposes, the online survey employed a Captcha verification question to ensure the participation of real humans. Flatliners and those who failed to pass the attention checks embedded in the questions throughout the survey were also excluded from the analyses.

Survey fielding took place between April 16 and 21, 2018, which coincided with the aftermath of the 2018 elections in Russia, ensuring the relevance of the risks attached to OPE for ordinary citizens. As for privacy specifically, the blocking of Telegram for its failure to comply with the Russian government's requests for individual users' data and the mass protests that occurred in the following weeks made vertical privacy threats and their potential consequences salient.

Russia serves as an appropriate study context given the intensification of digital repression that accompanies the already strict control over legacy media and the resulting psychological challenges for ordinary citizens (Nisbet & Kamenchuk, 2021). From a horizontal privacy perspective, ordinary citizens in Russia not only suffer from the worsening vertical processes of digital repression (Freedom House, 2023) but also from incidents involving other ordinary people (e.g., co-workers, neighbors) informing against anti-war sentiments expressed through semi-public or public means, especially in the aftermath of the invasion, when thousands of citizens were arrested (Dixon, 2023). Moreover, considering the challenges survey researchers had to endure during the pandemic in general and the extreme circumstances associated with Russia's full-scale invasion of Ukraine in terms of working with Russian respondents in particular, the current study may reflect one of the last chances of taking a snapshot of Russian Internet users' political self-disclosure before the recent war-related aggravation of digital repression.

Measures

Main Variables

For the political opposition in Russia, governmental corruption stands out as one of the recurring themes for challenging the incumbent regime with several anti-corruption protests, both on the streets and in online spaces, having taken place also around the data collection (Lonkila, Shpakovskaya, & Torchinsky, 2021). Likewise, for study purposes, the intention to engage in OPE was measured by asking respondents how likely it was for them to engage in five different acts of political self-disclosure (α = .95) regarding corruption within the Russian government and political leaders on social media (1 = Extremely unlikely, 5 = Extremely likely).

These acts include (1) openly criticizing corruption among the Russian government or political leaders, (2) tweeting, posting, or otherwise promoting a political news story (for example, a newspaper article) about governmental corruption, and (3) retweeting, reposting, or otherwise promoting another user's post about governmental corruption. The responses to the five different acts concerned with OPE about governmental corruption were averaged, with higher scores indicative of a greater intention to engage in OPE (α = .94).

Respondents' horizontal privacy regulation was measured by asking how frequently they engaged in a list of six behaviors (1 = Never, 5 = Always) targeted at protecting their privacy from other users on social media (adapted from Young & Quan-Haase, 2013). These behaviors include (1) deleting messages posted to your profile to restrict others from viewing/reading the message, (2) restricting contacts on (most used app) to only limited access to your profile, and (3) changing my privacy settings from the default values.

The item wording for horizontal privacy regulation indicates what each respondent had previously reported in the survey as their most preferred social media platform (Odnoklassniki, VKontakte, Telegram, Facebook, Twitter) for political use. Similar to the outcome variable, the scores were averaged, with higher scores indicative of greater horizontal privacy regulation (α = .81), and the wording specified the most preferred special media platform for politics.

An impression-relevant involvement measure was constructed by averaging two 5-point items (1 = Strongly disagree, 5 = Strongly agree) adopted from Cho and Boster (2005). The items questioned the level of agreement with the following: (1) talking about my beliefs concerning corruption has little effect on what others think of me, and (2) talking about my position on government corruption strongly influences the impression that others have of me.

Control Variables

Vertical privacy management was measured by averaging the reported frequencies of engaging in four behaviors that targeted protecting privacy from institutional actors (1 = Never, 5 = Always, α = .76). Perceived response efficacy was measured by averaging five items (α = .92), assessing the extent to which respondents believed OPE was effective in policy changes, leaders' decisions, citizen awareness, and so on (1 = Very ineffective, 5 = Very effective). Political posting was measured by averaging the number of days a week for six different political expressive behaviors on social media (α = .95). For network heterogeneity, respondents reported the perceived portion of their friends with similar political opinions on their most preferred platform (1 = None, 5 = All of them). The most preferred social media platform was controlled by creating dummy variables for Odnoklassniki, VKontakte, Telegram, and Facebook, with Twitter serving as the reference category. Non-political posting is the average number of days a week respondents post on other topics, including movies, sports, and personal updates (α = .88). The full item wording for these variables is presented in the Appendix.

Additionally, socio-demographic variables consisted of age, sex (female coded 1), education, employment status (full-time employment coded 1), and regime opposition (favorability toward President

Vladimir Putin, Prime Minister Dmitry Medvedev, and United Russia, α = .86). Finally, because the survey involved an experimental manipulation that was beyond the current study's scope, the conditions to which respondents were randomly assigned were also statistically controlled in the analyses by using dummy variables. The full item wording for all variables can be found in the Appendix, and the descriptive statistics are summarized in Table 1.

Table 1. Descriptive Statistics.

Variables	N	Mean	SD	Min	Max
OPE Intention	992	2.84	1.14	1	5
Horizontal Privacy Regulation	992	1.95	0.80	1	5
Impression-Rel. Involvement	992	2.65	0.73	1	5
Vertical Privacy Regulation	992	1.66	0.72	1	5
Response Efficacy	984	2.63	1.22	1	5
Regime Opposition	989	3.83	1.66	1	7
Non-Pol. Posting	991	2.73	1.74	1	8
Political Posting	992	2.39	1.64	1	8
Network Heterogeneity	986	3.21	0.85	1	5
Odnoklassniki	992	0.19	0.39	0	1
VKontakte	992	0.50	0.50	0	1
Telegram	992	0.06	0.24	0	1
Facebook	992	0.17	0.37	0	1
Twitter	992	0.06	0.24	0	1
Age	967	39.65	11.24	18	79
Female	992	0.46	0.50	0	1
Education Level	991	0.80	0.40	1	11
Full-Time Employment	951	0.80	0.40	0	1

Results

In light of the hypotheses and research questions, two ordinary least square models were run, and the results of the multivariate regression and interaction analyses are shown in Table 2, with unstandardized coefficients and standard errors reported. Testing H1a–b, Model 4 investigated the direct effect of horizontal privacy regulation on intention to engage in OPE about governmental corruption, with the overall model explaining 28.8% of the observed variance. The regression results show that the frequency of engaging in horizontal privacy regulation is negatively associated with the intention to engage in said behavior (b = –.10, $p \leq .05$). Hence, of the two alternative hypotheses, H1b is supported.

As for the remaining covariates predicting greater intention to post about governmental corruption, believing that OPE has high response efficacy in politics (b = .12, $p \leq .001$), having a homogeneous network on the most preferred social media with regards to political opinions (b = .09, $p \leq .05$), engaging in frequent political posting in general (b = .27, $p \leq .001$), having high impression-

relevant involvement about posting about corruption (b = .10, $p \leq .05$), and being a male (b = −.14, $p \leq .05$) were all significant predictors. In addition, regime opposition was negatively associated with the intention to post about corruption (b = −.11, $p \leq .001$), which deserves further discussion regarding its implications for authoritarian contexts.

Next, to test H2, an interaction term was introduced to the initial model to see if impression-relevant involvement moderates the relationship between horizontal privacy regulation and intention to post (Model 5). Using Hayes's (2017) SPSS PROCESS macro, the model was bootstrapped 5,000 times, estimating the moderated effects of horizontal privacy regulation at one standard deviation below the mean, the mean, and one standard deviation above the mean of impression-relevant involvement. The analysis reveals that the model explains 29.2% of the observed variance, with the negative relationship between the horizontal privacy regulation and intention to post being significant only for those whose impression-relevant involvement is at the mean value (b = −.10, $p \leq .05$, 95% CI = [−.18, −.01]) or higher (b = −.20, $p \leq .01$, 95% CI = [−.32, −.08], for values one standard deviation above the mean). Thus, H2 is also supported.

Table 2. OLS Regressions Predicting Intention for OPE.

	Model 1	Model 2	Model 3	Model 4	Model 5
Horizontal Privacy Regul.	.01(.05)	-	.44(.15)**	−.11(.04)**	.16(.14)
Impression-Relevant Involv.	-	.24(.05)***	.59(.12)***	.10(.05)*	.32(.11)**
Horiz.Priv.X Imp.Rel.Involv.	-	-	−.17(.05)***	-	−.11(.05)*
Vertical Privacy Regul.	-	-	-	.06(.05)	.07(.05)
Response Efficacy	-	-	-	.12(.03)***	.12(.03)***
Regime Opposition	-	-	-	−.11(.02)***	−.11(.02)***
Non-Political Posting Freq.	-	-	-	.00(.03)	.00(.03)
Political Posting Freq.	-	-	-	.27(.03)***	.27(.03)***
Network Heterogeneity	-	-	-	.09(.04)*	.09(.04)*
Odnoklassniki	.18(.15)	.22(.15)	.24(.15)	.24(.14)	.26(.14)*
Vkontakte	.07(.14)	.06(.14)	.07(.14)	.20(.12)	.21(.12)
Telegram	.50(.19)*	.46(.19)*	.49(.19)*	.28(.12)	.29(.17)
Facebook	.34(.16)*	.33(.15)*	.34(.15)*	.27(.14)	.28(.14)*
Tv Use	-	-	-	.02(.02)	.02(.02)
Newspaper Use	-	-	-	.01(.01)	.01(.01)
Age	-	-	-	.00(.00)	.00(.00)
Female	-	-	-	−.15(.07)*	−.15(.07)*
Education	-	-	-	−.02(.02)	−.02(.02)
Full-Time Employment	-	-	-	.05(.08)	.04(.08)
Condition 1	−.07(.10)	−.06(.10)	−.06(.10)	−.08(.09)	−.08(.09)
Condition 2	−.06(.10)	−.09(.10)	−.07(.10)	−.11(.09)	−.11(.09)
Condition 3	.18(.10)	.16(.10)	.18(.10)	.17(.09)	.18(.09)
Constant	2.67(.16)***	2.06(.19)***	1.13(.36)**	1.67(.31)***	1.08 (.41)**

Unstandardized coefficients with robust standard errors in parentheses, *p < 0.05, **p < 0.01, ***p < 0.001.

For those who do worry about how others perceive them regarding their opinions about governmental corruption, the greater the horizontal privacy regulation gets, the weaker the intention to post about the sensitive topic at hand becomes. Moreover, when the interaction term is introduced, the significant covariates in the model (Model 5) consist of higher perceived response efficacy of OPE (b = .12, $p \leq .001$), network homogeneity (b = .09, $p \leq .05$), preferring Facebook (b = .28, $p \leq .05$) or Odnoklassniki (b = .27, $p \leq .05$) for OPE, being a male (b = −.14, p ≤ .05), and exhibiting low regime opposition (b = −.11, $p \leq .001$). Figure 1 illustrates the interaction slopes at different levels of impression-relevant involvement.

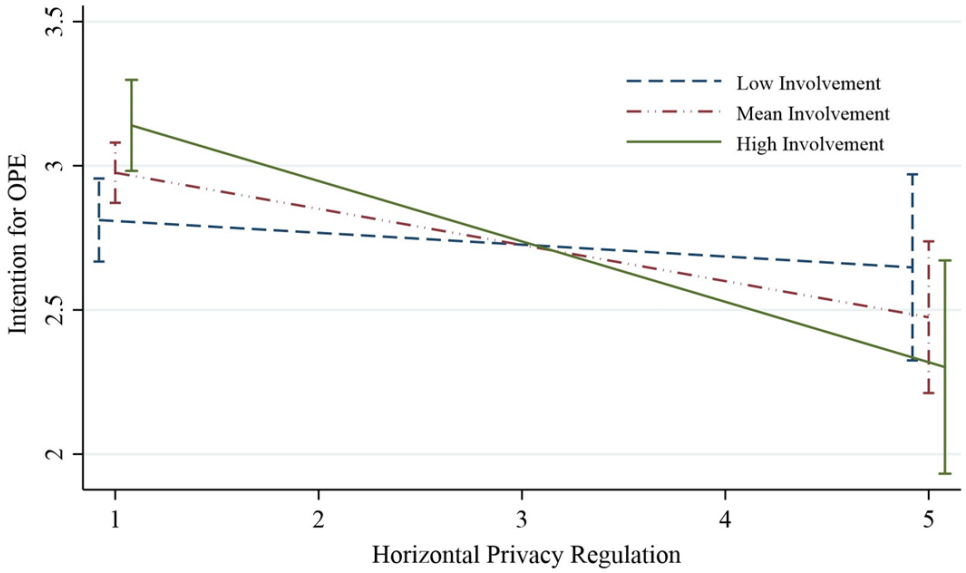

Figure 1. Effect of horizontal privacy regulation on intention for OPE conditional on impression-relevant involvement (95% CIs).

This study has several limitations. First, because the survey was fielded in a sociopolitical environment suffering from severe authoritarian practices, those who perceived the greatest levels of risk in online political activities may have been underrepresented in the sample. The second limitation concerns the dependent variable. Because OPE is only measured at the intentional level, the actual behavior may differ in light of the available risk signals and the resulting perceptions at the moment of hitting the "post" button. Likewise, individuals may engage in more (or less) intense privacy regulations based on the specific topic of expression. To address this limitation, future studies can incorporate experiments in which the features of privacy contexts are manipulated and participants are asked to make actual posts within study designs that may feel closer to real life.

Discussion

Even in the strictest authoritarian contexts, repression does not occur uniformly across time and space. It is not uncommon for officials in authoritarian regimes to deliver speeches that immediately make

it much riskier to defend a specific political stance. Alternatively, a single incident in which a seemingly innocuous online action is heavily punished can activate fear among citizens. Having to live with such precariousness places horizontal privacy regulations in an important position for those who are willing to engage in OPE. Hence, when studying digital repression at the micro-level, one should examine the social dynamics of the online networks of suppressed individuals, which simultaneously host both regime collaborators and those who aspire to have a more democratic treatment.

Living under authoritarian governance requires citizens to constantly negotiate the risks and uncertainties regarding the consequences of what they disclose publicly, semi-publicly, and privately. This negotiation often involves engaging in preventive or corrective actions in restricted online spaces where not only the rules but also the active players of the game are open to change unbeknownst to ordinary citizens. The current study investigates the link between citizens' horizontal privacy regulation attempts and the extent to which such actions play into the strength of their intentions to self-disclose opinions about governmental corruption in Russia, and explores a boundary condition relating to the perceived social costs of others knowing about their position about governmental corruption. The findings reveal that the more frequently individuals engage in horizontal privacy regulation, the weaker their intention to post about corruption on social media becomes. The analyses also show that this negative relationship is significant only for those with mean or higher levels of impression-relevant involvement.

These findings illustrate a chilling effect for those who deliberately try to regulate what they disclose to other users on social media regarding governmental corruption. Rather than inspiring confidence, privacy protection behaviors are associated with taking a step further, which is reluctance to engage in OPE on social media. Moreover, the extent to which individuals care about others' perceptions of their political selves amplifies the chilling effect, resulting in even weaker intentions. The study findings confirm prior research that suggests a greater concern for horizontal versus vertical privacy threats, although they focus on dissimilar sociopolitical contexts (Lutz & Ranzini, 2017; Stutzman, Gross, & Acquisti, 2013; Sujon, 2018).

Two of the significant predictors of a greater intention for OPE regarding governmental corruption deserve further attention. First, the analyses reveal that government supporters exhibit a greater intention, which may initially sound counterintuitive given that the anti-corruption protests primarily targeted Putin and his circle. However, it is important to note that authoritarian governments may benefit from the discussion of a sensitive topic as long as it fits into their own narratives. Likewise, Putin himself publicly showed support for a systematic struggle against corruption ("Putin: Corruption Must be Fought Against," 2017). He also suggested that the opposition's underlying goal was to engage in self-advertising by turning its anti-corruption stance into a political instrument before the elections. When such a message comes from authoritarian leadership, it can serve as an encouragement cue for government supporters to voice their support on a large scale, which would help balance the opposition's online presence about the same topic. Similarly, a longitudinal study previously done in the context of Türkiye reveals a moderating influence of government support between negative feelings about OPE and engaging in it (Dal & Nisbet, 2022). This example, too, shows that while feeling negatively about OPE may suppress the opposition, it may further mobilize pro-government individuals to visibly side with their government.

Second, the platform individuals use for OPE can be quite important for not only the potential differences between perceived effectiveness, ease of use, availability, and so on of privacy-regulating features but also how much control the Russian government exerts on the platform. For example, the change of leadership and the resulting increase in government oversight of VKontakte (Poupin, 2021) could help explain why using Facebook or Telegram comes forward as significant predictors in some of the statistical models. Likewise, it would be interesting to see if these results would hold after the intensification of government restrictions on Telegram, Facebook, and the circumvention technologies used to access these platforms in the aftermath of the survey (Freedom House, 2023).

One of the key questions this study raises is the underlying reasons for the failure of horizontal privacy regulation efforts. In light of the non-significance observed for those who score low in impression-relevant involvement, concepts like fear of social isolation (Chan, 2018) or desire to avoid conflicts and political disagreement (Vraga, Thorson, Kligler-Vilenchik, & Gee, 2015) may be in effect so much so that those who are concerned with the potential social sanctions refrain from taking the risks of online self-disclosure. As another reason, the perceived effectiveness of digital repression may trigger a ceiling effect in that individuals consider horizontal privacy regulation a futile step toward combating their authoritarian government (Roberts, 2020).

These potential explanations may also inform future investigations on concepts such as privacy helplessness (Cho, 2022) or privacy cynicism (Hoffmann et al., 2016) in contexts with similarly intensifying vertical privacy violations. As previously demonstrated, even under overt authoritarianism, as is the case in Russia, the increased salience of risk signals (e.g., going to prison) associated with a particular issue plays a role in individuals' immediate judgment and decision-making regarding online activism (Dal et al., 2023). Likewise, the availability of risks regarding privacy violations could highlight nuances in how the chilling effect this study suggests manifests in individuals. This makes more detailed examinations of the interactions between horizontal and vertical privacy dimensions important for further unpacking the experience in the face of digital repression.

Finally, there may also be dynamics particular to the issue of corruption in Russia that remain beyond the scope of this study. The observed effects may differ in direction or strength for more (or less) sensitive topics. For instance, the relationships suggested by the findings may be stronger for topics such as Russia's full-scale invasion of Ukraine. During such crises, governments may impose specific directions regarding what is allowed and what is forbidden for media professionals and ordinary citizens. They may ensure that risk signals are largely received by publicizing severe punishments for concerning actions in the media and across social networks. Moreover, it may be easier for governments to exploit nationalistic motivations in such times and, eventually, complicate daring to defame one's homeland in the eyes of fellow citizens. In such cases, concepts like impression-relevant involvement may become even more important in understanding citizens' experiences.

Concluding Remarks

Living in authoritarian regimes as citizens who are critical of the government means not only dealing with vertical threats but also with those who support the regime's actions and repressive tactics. That said,

ears that are potentially listening to what citizens have to say in online spaces surrounded by technical and psychological firewalls may result in both solidarity and severe punishment. In such environments, horizontal privacy threats, thus, serve as complementary to those that emerge from the enduring digital repression tactics of governments. Accordingly, this study portrays the citizen experience in dealing with the potential threats coming from one's social media contacts, with further consideration of how one feels about online political self-disclosure about a sensitive topic. While the Russian case, as the privacy context of interest, is used for testing the individual-level mechanism in this study, the findings are presented as potentially applicable to other authoritarian contexts as well.

References

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2021). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. *The Information Society, 37*(2), 115–127. doi:10.1080/01972243.2020.1870596

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole Publishing Company.

Baker, S., & Hamilton, I. A. (2021, April 1). Russia now requires all smartphones and devices in the country to have Russian software preinstalled. *Business Insider*. Retrieved from https://www.businessinsider.com/russia-requires-phones-devices-have-russian-software-pre-installed-2021-4

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53. doi:10.1111/jcom.12276

Bayer, J. B., Triệu, P., & Ellison, N. B. (2020). Social media elements, ecologies, and effects. *Annual Review of Psychology, 71*(1), 471–497. doi:10.1146/annurev-psych-010419-050944

Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication, 64*(4), 635–657. doi:10.1111/jcom.12106

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology, 36*, 118–123. doi:10.1016/j.copsyc.2020.05.004

Behrouzian, G., Nisbet, E. C., Dal, A., & Çarkoğlu, A. (2016). Resisting censorship: How citizens navigate closed media environments. *International Journal of Communication, 10*, 4345–4367.

Bode, L. (2017). Gateway political behaviors: The frequency and consequences of low-cost political engagement on social media. *Social Media + Society, 3*(4), 1–10. doi:10.1177/2056305117743349

boyd, d., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210–230. doi:10.1111/j.1083-6101.2007.00393.x

Chan, M. (2018). Reluctance to talk about politics in face-to-face and Facebook settings: Examining the impact of fear of isolation, willingness to self-censor, and peer network characteristics. *Mass Communication and Society, 21*(1), 1–23. doi:10.1080/15205436.2017.1358819

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist, 62*(10), 1392–1412. doi:10.1177/0002764218792691

Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 13–19. doi:10.1089/cyber.2014.0456

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Information Research, 25*(2), 279–300. doi:10.1108/intr-09-2013-0192

Cho, H. (2022). Privacy helplessness on social media: Its constituents, antecedents and consequences. *Internet Research, 32*(1), 150–171. doi:10.1108/INTR-05-2020-0269

Cho, H., & Boster, F. J. (2005). Development and validation of value-, outcome-, and impression-relevant involvement scales. *Communication Research, 32*(2), 235–264. doi:10.1177/0093650204273764

Chunly, S. (2020). Social media and counterpublic spheres in an authoritarian state: Exploring online political discussions among Cambodian Facebook users. *Discourse, Context & Media, 34*, 1–9. doi:10.1016/j.dcm.2020.100382

Dal, A., & Nisbet, E. C. (2022). To share or not to share? How emotional judgments drive online political expression in high-risk contexts. *Communication Research, 49*(3), 353–375. doi:10.1177/0093650220950570

Dal, A., Nisbet, E. C., & Kamenchuk, O. (2023). Signaling silence: Affective and cognitive responses to risks of online activism about corruption in an authoritarian context. *New Media & Society, 25*(3), 646–664. doi:10.1177/14614448221135861

Dienlin, T. (2015). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J.-M. Mönig (Eds.), *Medien und privatheit* [Media and privacy] (pp. 105–122). Passau, Germany: Karl Stutz.

Dixon, R. (2023, May 30). Russians snitch on Russians who oppose war with Soviet-style denunciations. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/2023/05/27/russia-denunciations-arrests-informants-war/

Earl, J., Maher, T. V., & Pan, J. (2022). The digital repression of social movements, protest, and activism: A synthetic review. *Science Advances, 8*(10), 1–15. doi:10.1126/sciadv.abl8198

Freedom House. (2023). *Freedom on the Net*. Retrieved from https://freedomhouse.org/country/russia/freedom-net/2023

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY: Guilford Press.

Henrich, J., Heine, S. J., & Norenzayan, A. (2010). Most people are not weird. *Nature, 466*(7302), 29. doi:10.1038/466029a

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), 1–18. doi:10.5817/cp2016-4-7

Honari, A. (2018). "We will either find a way, or make one": How Iranian Green Movement online activists perceive and respond to repression. *Social Media + Society, 4*(3), 1–11. doi:10.1177/2056305118803886

Huang, H. (2015). Propaganda as signaling. *Comparative Politics, 47*, 419–444. doi:10.5129/001041515816103220

Izadi, E., & Ellison, S. (2022, March 4). Russia's independent media, long under siege, teeters under new Putin crackdown. *Washington Post*. Retrieved from https://www.washingtonpost.com/media/2022/03/04/putin-media-law-russia-news/

Johnson, B. T., & Eagly, A. H. (1989). Effects of involvement on persuasion: A meta-analysis. *Psychological Bulletin, 106*(2), 290–314. doi:10.1037/0033-2909.106.2.290

Jourard, S. M., & Lasakow, P. (1958). Some factors in self-disclosure. *The Journal of Abnormal and Social Psychology, 56*(1), 91–98. doi:10.1037/h0043357

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computer Human Behavior, 107*, 1–15. doi:10.1016/j.chb.2020.106260

Kendall-Taylor, A., Frantz, E., & Wright, J. (2020). The digital dictators: How technology strengthens autocracy. *Foreign Affairs, 99*, 103–115.

Koçer, S., & Bozdağ, Ç. (2020). News-sharing repertoires on social media in the context of networked authoritarianism: The case of Turkey*. International Journal of Communication, 14*, 5292–5310.

Kruse, L. M., Norris, D. R., & Flinchum, J. R. (2018). Social media as a public sphere? Politics on social media. *The Sociological Quarterly, 59*(1), 62–84. doi:10.1080/00380253.2017.1383143

Lapinski, M. K., Zhuang, J., Koh, H., & Shi, J. (2017). Descriptive norms and involvement in health and environmental behaviors. *Communication Research, 44*(3), 367–387. doi:10.1177/0093650215605153

Leonardi, P. M. (2014). Social media, knowledge sharing, and innovation: Toward a theory of communication visibility. *Information Systems Research, 25*(4), 796–816. doi:10.1287/isre.2014.0536

Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. *Social Media + Society, 2*(1), 1–12. doi:10.1177/2056305116633482

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

Lonkila, M. (2016). "Social network sites and political governance in Russia." In V. Gel'man (Ed.), *Authoritarian modernization in Russia: Ideas, institutions, and policies* (pp. 113–127). Abingdon, UK: Routledge.

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

Lonkila, M., Shpakovskaya, L., & Torchinsky, P. (2021). Digital activism in Russia: The evolution and forms of online participation in an authoritarian state. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds.), *The Palgrave handbook of digital Russia studies* (pp. 135–153). Cham, Switzerland: Palgrave Macmillan.

Lutz, C., & Ranzini, G. (2017). Where dating meets data: Investigating social and institutional privacy concerns on Tinder. *Social Media + Society, 3*(1), 1–12. doi:10.1177/2056305117697735

Mak, M. K., Koo, A. Z. X., & Rojas, H. (2022). Social media engagement against fear of restrictions and surveillance: The mediating role of privacy management. *New Media & Society*. Advance Online Publication. doi:10.1177/14614448221077240

Margetts, H., John, P., Hale, S., & Yasseri, T. (2016). *Political turbulence: How social media shape collective action*. Princeton, NJ: Princeton University Press.

Marshall, H. M., Reinhart, A. M., Feeley, T. H., Tutzauer, F., & Anker, A. (2008). Comparing college students' value-, outcome-, and impression-relevant involvement in health-related issues. *Health Communication, 23*(2), 171–183. doi:10.1080/10410230801968252

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13*(1), 114–133. doi:10.1177/1461444810365313

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Wiesbaden, Germany: Springer.

Masur, P. K., Epstein, D., Quinn, K., Wilhelm, C., Baruh, L., & Lutz, C. (2021, December 9). *A comparative privacy research framework*. Retrieved from https://osf.io/preprints/socarxiv/fjqhs/

Mor, Y., Kligler-Vilenchik, N., & Maoz, I. (2015). Political expression on Facebook in a context of conflict: Dilemmas and coping strategies of Jewish-Israeli youth. *Social Media + Society, 1*(2), 1–10. doi:10.1177/2056305115606750

Nisbet, E. C., & Kamenchuk, O. (2021). Russian news media, digital media, informational learned helplessness, and belief in COVID-19 misinformation. *International Journal of Public Opinion Research, 33*(3), 571–590. doi:10.1093/ijpor/edab011

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

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

Parks, L., & Mukherjee, R. (2017). From platform jumping to self-censorship: Internet freedom, social media, and circumvention practices in Zambia. *Communication and Critical/Cultural Studies, 14*(3), 221–237. doi:10.1080/14791420.2017.1290262

Parviz, E., & Piercy, C. W. (2021). What will they think if I post this? Risks and returns for political expression across platforms. *Social Media + Society, 7*(4), 1–12. doi:10.1177/20563051211055439

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*, 1310–1331.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: SUNY Press.

Poupin, P. (2021). Social media and state repression: The case of VKontakte and the anti-garbage protest in Shies, in Far Northern Russia. *First Monday, 26*(3). doi:10.5210/fm.v26i5.11711

Putin: Corruption must be fought against, but using this issue to score points is wrong. (2017, March 30). *TASS*. Retrieved from https://tass.com/politics/938496

Quinn, K., & Epstein, D. (2018). #MyPrivacy: How users think about social media privacy. In *SMSociety '18: Proceedings of the 9th International Conference on Social Media and Society* (pp. 360–364). Copenhagen, Denmark: Association for Computing Machinery. doi:10.1145/3217804.3217945

Quinn, K., Epstein, D., & Moon, B. (2019). We care about different things: Non-elite conceptualizations of social media privacy. *Social Media + Society, 5*(3), 1–14. doi:10.1177/2056305119866008

Ranzini, G., Lutz, C., & Hoffmann, C. P. (2023). Resignation in the face of agency constraints. In S. Trepte & P. Masur (Eds.), *The Routledge handbook of privacy and social media* (pp. 134–143). Abingdon, UK: Routledge.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). Retrieved from https://firstmonday.org/ojs/index.php/fm/article/download/2775/2432

Roberts, M. E. (2020). Resilience to online censorship. *Annual Review of Political Science, 23*, 401–419. doi:10.1146/annurev-polisci-050718-032837

Sanovich, S., Stukal, D., & Tucker, J. A. (2018). Turning the virtual tables: Government strategies for addressing online opposition with an application to Russia. *Comparative Politics, 50*(3), 435–482. doi:10.5129/001041518822704890

Saponchik, R. (2022). *Digital citadel – Country report on Russia*. University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-12. Retrieved from https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality, 4*(2), 7–41. doi:10.29012/jpc.v4i2.620

Sujon, Z. (2018). The triumph of social privacy: Understanding the privacy logics of sharing behaviors across social media. *International Journal of Communication, 12*, 3751–3771.

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248–273. doi:10.1111/jcc4.12052

Theocharis, Y. (2015). The conceptualization of digitally networked participation. *Social Media + Society, 1*(2), 1–14. doi:10.1177/2056305115610140

Troianovski, A., Parshina-kottas, Y., Matsnev, O., Lobzina, A., Hopkins, V., & Krolik, A. (2023, December 29). How the Russian government silences wartime dissent. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2023/12/29/world/europe/russia-ukraine-war-censorship.html

Vaccari, C., Valeriani, A., Barberá, P., Bonneau, R., Jost, J. T., Nagler, J., & Tucker, J. A. (2015). Political expression and action on social media: Exploring the relationship between lower-and higher-threshold political activities among Twitter users in Italy. *Journal of Computer-Mediated Communication, 20*(2), 221–239. doi:10.1111/jcc4.12108

Van der Vet, F. (2019). Imprisoned for a "like": The criminal prosecution of social media users under authoritarianism. In M. Wijermars & K. Lehtisaari (Eds.), *Freedom of expression in Russia's new mediasphere* (pp. 209–224). Abingdon, UK: Routledge.

Van Ooijen, I., Segijn, C. M., & Opree, S. J. (2022). Privacy cynicism and its role in privacy decision-making. *Communication Research, 51*(2), 146–177. doi:10.1177/00936502211060984

Vraga, E. K., Thorson, K., Kligler-Vilenchik, N., & Gee, E. (2015). How individual sensitivities to disagreement shape youth political expression on Facebook. *Computers in Human Behavior, 45*, 281–289. doi:10.1016/j.chb.2014.12.025

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs, 61*(2), 113–134. doi:10.1080/03637759409376328

Wu, P. F., Vitak, J., & Zimmer, M. T. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology, 71*(4), 485–490. doi:10.1002/asi.24232

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479–500. doi:10.1080/1369118X.2013.777757