



# **‘In Google we trust’? The Internet giant as a subject of contention and appropriation for the Russian state and civil society**

Olga Bronnikova, Anna Zaytseva

## **► To cite this version:**

Olga Bronnikova, Anna Zaytseva. ‘In Google we trust’? The Internet giant as a subject of contention and appropriation for the Russian state and civil society. First Monday, 2021, 10.5210/fm.v26i5.11709 . halshs-04397690

**HAL Id: halshs-04397690**

**<https://shs.hal.science/halshs-04397690>**

Submitted on 17 Jan 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# ‘In Google we trust’? The Internet giant as a subject of contention and appropriation for the Russian state and civil society

by Olga Bronnikova and Anna Zaytseva

## Abstract

This article explores an apparent paradox related to the use of Google services in Russia: several NGOs based in the country consider the Internet giant as a protector of civil liberties. The highly polarized Russian political context, in which local technological companies are increasingly controlled by the State, explains the widespread uses of Google services in daily practices of NGOs. We show how their risk model is focused on the threat emanating from the State, seen as more important than risks emanating from global private companies. In this context, “big tech” solutions are preferred to open source software as they are valued for their usability. Internet giants, such as Google, are understood by civil society actors as powerful allies in this internal confrontation, as their dominant economic role is seen as a guarantee that they will not yield to pressure from authorities. Finally, we will see how, in parallel, self-regulatory virtues of the competitive global IT market, and the strength of global public opinion, are supposed to “naturally” force these companies to comply with ethical standards in data use.

## Contents

### [Introduction](#)

### [I. Google in the daily practices of human rights defenders](#)

### [II. Benefit of the doubt: Internet freedom defenders advocating with Google](#)

### [Conclusion](#)

## Introduction

Google’s blockage [in Russia] will block 30 percent of Russian sites, including Kremlin.ru (the site of the presidential administration). This will deal a severe blow to the economy in unexpected places. Everything is likely to break down: the public health system or the management of gas pipelines, it's unpredictable. [1]

This alarm, raised by an IT expert on the eve of the entry into force in Russia of the so-called “sovereign Internet” law in 2019 [2], are based on a real experience of blackout for the Russian Internet, linked to the

Telegram case [3]. It underscores both the close dependency of national economies and communication networks on “Internet giants” — Google, Facebook, Amazon — and the infrastructural complexity and interconnectedness of the global IT ecosystem. This complexity is likely to challenge any top-down intervention by state regulators and may pose a threat to the equilibrium of the global information ecosystem.

Internet giants are at the heart of a paradox. On the one hand, they are becoming “important checkpoints (...), making *de facto* policy decisions in the whole range of cases where they collect, collate, aggregate, select and present data to users (...), thus exercising governance over freedom of expression, cultural diversity and reputation” (Musiani, 2018, our translation; see also DeNardis, 2014). On the other hand, they are recognized as sites of economic and political power, various interests are coopting these infrastructures, investing them with roles and functions different from their primary meaning, to control and monitor populations, access data on them, fight against crime and piracy, etc. (DeNardis, 2012). These new relationships are ambivalent, as they involve both various forms of co-optation of Internet giants by national and supra-national actors, and a form of rivalry and struggle between them for the power to determine and direct information flows over territories.

The ambivalent and disproportionate role of these actors generates worried discourses about “algorithmic harms” (Tufekci, 2015) and about a society governed by opaque algorithms beyond human control (Pasquale, 2015; Burrell, 2016). Both researchers (*e.g.*, Brousseau, *et al.*, 2012) and civil society actors have come to plead for greater transparency and accountability of Internet giants (Jewler, 2015; Reporters Without Borders, 2019), and even for regulation of their activities (especially with regard to data use and anti-trust legislation) by the state, public bodies and civil society (Srnicek, 2017; Lessig, 2006).

Google entered the Russian market in 2005, at a time when the Russian digital ecosystem was already well developed (Limonier, 2017) with companies such as Yandex, MailRu Group and VKontakte (first an independent social networking service, then bought by MailRu Group). From the end of the 2000s and especially in the 2010s, the popularity of Google’s services began to grow [4], with YouTube becoming one of the most consulted social networks in Russia [5], invested by bloggers, political activists and independent journalists. Domestic as well as American platforms were widely used for political mobilization against electoral frauds in the winter of 2011–2012 [6]. The authorities read these mobilizations as an interference by the West in the internal affairs of the country, with the aim of carrying out a coup d’état. Analogies can be made with the “colour revolutions” in post-Soviet countries, and the “Arab Springs”, known for the importance of social networks as mobilization organizers, and for the support of the Western “Internet Freedom diplomacy” [7]. Comparable to other illiberal regimes (Finkel and Brudny, 2012), the anxiety of Russian leaders *vis-à-vis* the disruptive “power of networks” (Nocetti, 2015) and Western interference led them to adopt a series of restrictive laws [8], and to tighten the rules for nongovernmental organizations and external aid.

After 2012, the national Internet champions are the first to bear the consequences of this state takeover. After a series of measures to establish the filtering of RuNet (blacklist of materials banned from circulation in Russia since 2012), in 2017, the law concerning “organizers of the dissemination of information” required search engines and platforms to provide access to the contents of user exchanges and locate user data on the Russian territory [9]. Surprisingly, Google, like many other foreign companies, has not been included in this list, thus obtaining advantages over their local competitors: although still leaders in terms of number of users, Yandex and MailRu are suspected of close collaboration with the Russian law enforcement agencies [10]. Among the activists not loyal to the government [11] (in particular NGOs, under severe constraints regarding their daily activities after the adoption in 2012 of the law “On non-profit organizations” [12]), doubts loom large as to the usability of their services for safe communication. The pressure on civic activists continues to increase with the adoption of other laws along the same lines, such as the “Law on Undesirable Organizations” (2015) [13], or the “Law on Foreign Agents Individuals” (2020) [14]. In the context of what has come to be described as “information warfare”, with increased surveillance and repression practices, activists are turning even more to foreign platforms, seen as safe havens able to protect them from the ubiquitous Eye of the Leviathan.

Unlike under other illiberal regimes (China, Iran), Google and other global platforms remain legally accessible in Russia and are widely used, including by political leaders (often communicating via Twitter) and pro-government media (very active on YouTube). This ubiquitous and official presence makes them legitimate actors in negotiations on digital freedoms between the authorities and actors of civil society in Russia. However, they are also subject to some of the most recent measures aimed at controlling the Internet. A tension has unfolded in 2017 in the field of Google's infrastructure intermediaries, *i.e.*, the Russian ISPs and telecom operators hosting Google Global Cache servers. Information has indeed circulated in the media about the possible ban of GGC in Russia due to the lack of certification [15]. Tensions continue with negotiations on the filtering of online content. While Russian search engines have been applying it since 2018, Google is starting to do so in 2019 and only partially. Finally, Russian authorities' major efforts are concentrated on the implementation of the law about the storage of Russian citizens' data in Russia [16] within a larger series of measures known as "Sovereign Internet Law". In all these struggles, the main means of pressure for the Russian regulator are fines, which are more and more important. As Google has a legal personality registered in Russia (SARL Google, with an office in Moscow), in case of non-payment of fines, the state can block the company's accounts [17]. Finally, according to the law adopted in December 2020 — and following accusations made to YouTube of blocking some pro-government channels (Tsargrad-TV, RT) or removing them from the "trends" of their videos — access to platforms such as YouTube, Twitter and Facebook can be blocked or slowed down, at the request of the General Prosecutor's Office, for acts of censorship against Russian media publications [18]. A new tool of state pressure is thus emerging, that of slowing down access [19].

How does this polarized context, governed by a quasi-Schmittian binary scheme opposing "friends" and "enemies" of the Russian state (Schmitt, 2007), contribute to shaping representations about Google among Internet freedom activists and human rights NGOs, as well as their practices of using its services? In the first part of the article, we will present the ubiquity and the role of different Google services (G Suite in particular, GoogleDocs, YouTube etc.) in the regular practices and activities of different civil society actors (human and digital rights NGOs and activists, digital security trainers), as well as their justifications to explain these uses. In the second part, we will analyze the foundations for the trust placed in Google by the Internet freedom and digital rights defenders, based on measurable empirical evidence (indices, statistics). We will then analyze their "imaginaries" (Flichy, 2004; Asmolov and Kolozaridi, 2017) about the Big Tech market and its mechanisms and their strategies of advocating with it.

Focusing initially on the practices of digital security trainers, human rights NGOs [20] and independent journalists in Russia and Belarus, we have later extended our research to other actors, such as activists from local associations defending digital freedoms (Internet Protection Society — OZI, Digital rights center and Roskomsvoboda in Moscow, Human Constanta in Minsk [21]) and international organizations (Front Line Defenders, Access Now); local actors promoting civic technologies (Greenhouse of social technologies); representatives of the telecom community, and foreign experts on digital freedoms in Russia (authors of reports for Reporters Without Borders from its office in Berlin). In addition, we followed the Telegram channels of associations and individuals in the Internet freedom defenders space; analyzed their media discourses and interactions (forums, blogs); participated in public events with these activists [22], observed online from other events in Russia (Privacy Day in Moscow, 2020, 2021) and abroad (RightsCon, Tunis, 2019) in which these actors have participated; and observed a training of trainers [23] in online digital security in May 2020, set up by The Greenhouse of social technologies.



## I. Google in the daily practices of human rights defenders

Some national contexts — Russia is one of them — are peculiar *vis-à-vis* the international critical discourses, as Internet giants are considered by some civil society actors as protectors of freedom against growing state surveillance. At first glance, it appears that these actors are reproducing the discourse of

human rights defenders (HRD) that Google has fostered since its early days [24]. After the Snowden revelations in 2013, Google reaffirmed its support for civil society, especially in countries with illiberal regimes. Nowadays, “legalization” and “litigation” have become one of Google’s strategies to resist government requests, thereby restoring user confidence (Tréguer, 2018): Google’s dedicated teams study national laws and must examine the extent to which these requests actually comply with it in each case. In addition, if a law is ambiguous, “Google may interpret it in a narrow manner to avoid or restrict/focus the government request” [25].

So, Google is used by multiple human rights organizations and activists in Russia in their everyday work for the usability, security and efficiency of its various services. In addition, developing a long-standing strategy of presence in international HRD events, Google occupies an important place in the digital ecosystem of civil society organizations around the world. In this section, we will describe how HRD NGOs in Russia, helped by trainers and other experts on digital security, choose their communication tools and protect sensitive data from multiple digital threats they face and give some explanations about their ubiquitous positive consensus about Google. While some trainers suggest replacing Google’s services with FLOSS solutions, the latter are still perceived as not very accessible to non-specialists. Google’s success with NGOs is also due to the mediation work done by Russian social entrepreneurs, such as Greenhouse of social technologies (which will be further described later in the article).

### ***1.1. Digital security trainers’ recommendations***

To understand their trade-offs, it is useful to recall here the dangers that HRD NGOs face in Russia. Our interlocutors, while not always being deeply concerned about Google’s involvement in “surveillance capitalism”, pointed out the same phenomenon for Russian technology companies: *“In Russia, there are two logics of surveillance capitalism. On the one hand, companies that want to collect the maximum of behavioral data. On the other hand, there are some traditions and logics of citizen surveillance that allow the authorities to perceive this data as their property. The number of actors who can use it is really unlimited.”* [26] Thus, security trainers understand and convey to their audiences the risks associated with the registration of technology companies in the Russian jurisdiction.

In contrast, Google is considered rather reliable for activists from Russia and, more broadly, from authoritarian regimes in the post-Soviet space. First of all, this trust is based on the regular monitoring of Google’s Transparency Reports. As noted by a Belarusian trainer working for Russia and several Commonwealth of Independent States (CIS) countries, *“while for countries (...) participants in the ‘five eyes’ intelligence alliance, 80 to 90% of requests for information from the authorities are met, for Russia these figures represent only a few percent and for Belarus 0%”* [27]. When we asked our interlocutors to react to the fact that in 2019, the proportion of requests from the Russian authorities satisfied by Google increased to 38 percent (compared to 18 percent in 2017) [28], they always referred to their concrete knowledge of the HRD field in Russia: *“We still do not know of any real cases in our sector. Google has not given out any such data to the authorities about activists or human rights defenders”* [29].

In addition to Google data, our contacts rely on their own databases and measurement tools. According to M.K., coordinator of the “Map of repression on the Internet” (OZI project), this Map lists only a few cases related to Internet giants, whereas 95 percent of the cases concern posts and information delivered by VKontakte [30]. As to digital security trainers, they draw on their own internal “incident database”, shared via a mailing list including their counterparts in other post-Soviet states. Very few incidents involving Google’s services in these countries have been relayed through this database [31].

The uses of Google’s services by the activists are varied. Several NGO representatives use them for their internal exchanges. Thus, G Suite, adapted to the needs of an organization in particular, is prized for its usability, efficiency and high level of security. The IT managers of the NGOs in our interviews were constantly comparing Google’s services with their open-source equivalents. Besides legal and practical issues, there is relatively little use of alternative services to Google (Free/libre/open-source software, FLOSS) because “the right to anonymity is not considered to be valuable in Russia” [32]. The most



important question for NGOs digital security seems to be about the data: where it is stored, who has access to it, how it is transmitted. According to our interlocutors, the three categories of sensitive information handled by NGOs are: financial information concerning the transactions of NGOs with their partners and donors abroad [33]; data on NGO users; documents that can be considered “illegal” [34]. For example, an NGO working on racism hosts many writings qualified as “extremist”. They have already been incriminated, under the law “On countering extremist activity” (2002), which provides for prosecution for the storage of extremist information with the aim of disseminating it [35]. In this case, disk encryption tools (such as VeraCrypt) are used on the advice of trainers, but also storage on cloud facilities of various Net giants (including Google Drive) or on free file hosting services (such as NextCloud).

More broadly, although all our interlocutors recognize the danger of unsecure communications, many of them relativize its importance for Russia. For them, the main sources of danger are unsecured technical equipment (computers, servers, telephones, hard disks etc.) that can be seized during searches, or the publication by users of information and personal data in unreliable social networks such as VKontakte: *“I do not see any kind of huge surveillance. When a person is really being searched, well, his laptop was opened and they had access to social networks. Or, the person was well beaten there, and he gave out passwords from his accounts in social networks to the police”* [36].

During training sessions and digital security meetings, the trainers seek to target the particular needs and threats of these audiences in order to propose security protocols adapted to their practices. In developing this methodology, they have had to confront actual problematic cases, particularly experienced by NGOs outside major cities: *“The biggest reality check happens when you look at computers used by provincial NGO representatives”* [37]: they often use Russian services (VKontakte, Mail.ru, Yandex mail) under Russian jurisdiction, do not protect servers and computers with passwords and use digital resources in a chaotic way (e.g., former colleagues can still access the resources of these NGOs) [38]. In the early 2010s, several Russian NGOs were reluctant to use the tools proposed by digital security trainers sent by international organizations. The latter promoted the use of Linux Ubuntu, but *“it was a failure”* because Linux has “a very crooked, uncomfortable interface” [39].

The trainers gradually learned how to work with these audiences while *translating* into the Russian context international security methods and standards, strongly influenced by the liberal and libertarian cultures of the political Internet (Electronic Frontier Foundation, EFF) or the FLOSS movement [40]. In view of the experiences reported by training participants, security incidents shared among the trainers [41] and the specificities of the Russian NGO digital ecosystem, the trainers must constantly seek a compromise between “comfort” and “security”: *“It is not safe where it is very, very comfortable. And where it is very safe, it is not very comfortable. But finding an adequate balance for me and my clients is half the battle, so that they can understand, within their threat model, what can happen and to what consequences it can lead”* [42].

In this compromise, Google’s services play a key role. But they are often “complemented” by FLOSS solutions. As one of the trainers told us, *“I have never been a Google apologist. For example, I explain to my audiences about e-mail: switching from mail.ru to Google is a big step; but if you want more security for your e-mail, think about Tutanota. Gmail is not a benchmark for secure mail. It’s better to encrypt your files before you upload them to Google Drive. However, today Google is not just a service or software product that we have chosen by parameters among a range of similar products. Google is de facto extremely popular and well-known to the vast majority of users”* [43]. The use of Gmail has only increased with the shift to mobile Internet and the popularity of Android devices.

Even if the switch from mail.ru to Gmail is considered a big step, Google’s services do not cover all the security needs of our interlocutors, which may moreover contradict those of efficiency and comfort. Thus, the Google-dependency of various NGOs (e.g., use of G Suite for all tasks) becomes problematic to protect sensitive information. Several of our interlocutors have confessed that they have become accustomed to storing confidential information in GoogleDocs because Google has a good reputation for its investment in security [44]. However, incidents related to the indexing of documents by the Yandex search engine have

shown that this use of GoogleDocs is not secure [45]. Nevertheless, some of our interviewees consider that this case is not Google's responsibility, but is due to a lack of security skills on the part of the users.

If Google pretends to be exhaustive when providing technical solutions to social problems [46], security trainers circumvent this claim by proposing a diversity of tools to use. While for collaborative work and daily e-mail exchanges, they do not advise against the use of Google services, to protect sensitive communications they recommend open software, such as Veracrypt to store information, encryption tools such as Mailvelope to integrate into Gmail, encrypted messengers such as Signal, KeePassXC to secure and store passwords, in addition to the two steps authentication offered by Google services [47]. However, the use of FLOSS tools can also entail a political risk. Indeed, NGOs do not want to take the risk of organizing their entire IT architecture around software that in the imagination of Russian political decision-makers may be associated with illicit practices, as shown by the precedent with the open encrypted e-mail Protonmail [48] (which RKN has been trying to block since 2020) or the discussions around Tor, demonized by the Russian media and authorities as *"a tool for drug dealers and terrorists"* [49].

Another challenge inherent in the implementation of digital security standards within NGOs is due to the specific characteristics of their organization, which is often not very hierarchical, unlike the business world: *"Our accountant doesn't want to know anything about digital security. I've managed to convince her to switch to Gmail from Mail.ru. She did, but she hardly ever checks it"* [50]. A number of NGOs have opted for vertical solutions such as the G Suite, which allow them to "put some order" in the NGO structure [51]. The desire to verticalize the organization within NGOs is not new. It accompanies the turn to professionalization taken by NGOs (Le Naélou, 2004; DiMaggio and Powell, 1983) and their assimilation of a project-based organizational structure (Boltanski and Chiapello, 1999). In this evolution, Google plays an important role: *"FLOSS is suitable only for horizontal structures where everyone acts by consensus, everyone's roles are clear and no one has negative intentions. But if there is a group where the roles are vaguely defined, there is some conflict, G Suite clearly builds a management hierarchy"* [52]. Indeed, several of our interlocutors pointed out the danger of "physical infiltration" by malicious people that NGOs and independent media are facing. Services such as G Suite allow differentiated access to data for different NGO employees. In addition, many NGOs cannot afford to hire an IT manager to take care of digital architecture. In this case, the use of FLOSS solutions seems too difficult [53]. This situation of dependence on Google demonstrates that Russian NGOs have little choice, due to chronic lack of resources and faced with various threats from the Russian authorities. According to one of our interlocutors, the only alternative to G Suite is Office 365 [54]. But after Microsoft moved its servers to Russia to comply with the Russian law on personal data, its reliability was also questioned by digital security specialists [55].

From these debates, we see two logics emerging, both contradictory and complementary: to strengthen security (protecting communications and data), trainers continue to suggest FLOSS tools, while to organize the best management in organizations, social entrepreneurs (as Greenhouse of social technologies) recommend Google solutions.

## **1.2. Social entrepreneurs as Google's mediators in the non-profit sector**

In this section we will discuss the role played by social entrepreneurs in bringing together the *a priori* very different worlds of Google and human rights NGOs. Indeed, while having a reputation for being practical and efficient, Google's services, such as G Suite, are quite expensive for NGOs that lack financial resources. For several years, Google has been developing proprietary software donation programs for NGOs around the world [56]. Thus, the company has partnered with TechSoup, an initiative of several major American tech companies, such as Adobe, Amazon, Google, Microsoft, CloudFlare, which consists of granting logistical assistance devices (for Google, Gmail, GoogleDocs, cloud storage, Google "AdWords", YouTube Premium etc.) [57]. In Russia, this initiative is backed by an NGO, Greenhouse of Social Technologies, which positions itself in the world of social entrepreneurship and becomes "the mediator, the translator (...) who brings together two universes with distinct logics and horizons" (Akrich, *et al.*, 1988): Russian NGOs and global technology companies [58]. The aim of the joint program between TechSoup and the Greenhouse, called Teplodigital, is to teach activists to use ICTs according to the needs

of their organizations, and to create new tools where there are no technical solutions yet (Ermoshina, 2018) through the partnership with Internet giants. It should be noted that since the adoption of the law on “foreign agents”, the global technological companies have become one of the sources of funding for the activities of the Greenhouse via a number of programs focused on technological transfer and innovation.

NGOs get free or discounted access to proprietary solutions, including those from Google. The application of an NGO requesting a grant from Google must first be “validated” by the Greenhouse, which selects NGOs based on their status and the nature of their activities. A series of courses on YouTube are offered to NGOs to train them in the use of various Google services (such as AdWords), which is limited in time. Teplodigital members can also access G Suite basic (a simplified version of G Suite Business). For our interlocutors, Google’s interest in this program is to expand its presence in Russia by creating a Google “ecosystem” within NGOs due to their role as multipliers of social influence [59]. According to our interviewees, a many NGOs in Russia have interacted with this program somehow. In fact, several of them told us that their entire “ecosystem” is backed by Google (G Suite) [60] while others, such as one of the digital freedom NGOs, have obtained broadcast lists on YouTube [61].

The example of Teplodigital program and the Greenhouse reveals that the particularly tense context in which NGOs function in Russia, operating in quasi-“cold war” conditions favorable to the official hunt for foreign influences, paradoxically proves beneficial to the deployment of partnerships with foreign Internet giants. More broadly, it shows the efficiency of the worldwide efforts made by the company to consolidate the hold of its “soft power” beyond conventional means of lobbying, such as a long-term work with the non-profit sector, in particular, with NGOs defending Internet freedom and digital rights, “influential in civil society and devoted to myriad missions, including shaping technology and privacy policy” (Jewler, 2015). Presenting itself internationally as a defender of free speech and a sponsor of human rights organisations and of international Human Rights events, Google is thus criticized to fund “those who might otherwise raise alarms about its practices” (Jewler, 2015).

This part of the article demonstrated the omnipresence of Google services in the daily practices of Russian NGOs, to which they seem to bring an efficient and inexpensive managerial solution. We have also analyzed digital security trainers’ nuanced accounts about these practices; far from any dogmatism, they speak about concrete threats encountered by trained HRDs and the balance between security and usability. However, it is not easy to connect these different actors; this mediation role is played by social entrepreneurs such as Greenhouse of Social Technologies. We will now take a particular interest in the milieu of Internet freedom defenders in Russia and its relation to Google.

---

## **II. Benefit of the doubt: Internet freedom defenders advocating with Google**

Understanding visions about Google in the milieu of Internet freedom defenders seems important. The latter are shaped, on the one hand, by local political issues ruled by the growing confrontation between the pro-government camp and a liberal opposition to which they contribute. On the other hand, they articulate these issues with representations about Internet freedom and the role of different stakeholders, conveyed at the level of global NGOs and specialized forums they attend.

This section is mainly based on interviews and exchanges we conducted with activists from two Internet freedom and digital rights associations. The first, Roskomsvoboda [62], was founded in 2012 following the adoption of the law establishing the Unified Register of Prohibited Sites in Russia (the “black list”), which is managed by the newly created Internet surveillance state agency, Roskomnadzor (further — RKN). Originally a project of the Pirate Party of Russia, Roskomsvoboda’s primary goal is to oppose the blocking of Internet resources, to popularize ways to circumvent these blockages, and to defend the rights of blocked resource owners in court. Its missions also include public advocating of freedom of information and of personal data protection, monitoring of the legislation and of law enforcement practices in the area of



Internet regulation in Russia, with a recurring comparison with those of other countries.

The second association, linked in many ways to the first [63], is the Internet Protection Society (OZI) [64]. It was created in 2016 as a response to the series of restrictive laws regulating RuNet, particularly the “data localization” law. Several of its co-founders are activists of Aleksey Navalny’s Anti-Corruption Foundation. OZI attaches particular importance to an empirical and quantifiable measurement of digital freedoms, developing specific tools for this purpose. Thus, it has created the Internet Freedom Index, as a means to evaluate levels of online freedom [65], and the Map of Repressions, listing and geo-locating the criminal or administrative trials and sanctions resulting from online publications by Russian users [66].

Thus, we will look at Internet freedom defenders’ strategies and justifications for using Google, which concern not only its levels of usability, but also the company’s role in public life and for civil liberties in Russia. We will analyze their accounts about the game of “arm wrestling” between Google and the Russian state, and Google’s interests and strategies in this confrontation, which shape in turn the steps taken by these activists to influence the company’s behavior towards the Russian regulator. We will also pay attention to possible criticisms of Google in this milieu, their forms and pragmatic contexts. From there, we will try to flesh out a set of core elements of their imaginary about Google and, more broadly, their “Internet imaginaries” (Flichy, 2004).

### ***2.1. Google as a bulwark against state surveillance and censorship***

*“It could be funny, but using Gmail and Facebook messenger is still safe for me, as my state is my main enemy. The socially active users are now switching from Russian platforms, to Gmail and Facebook, because the former are giving out information about all the users in real time. The FSB does not even need to do official paper requests. For Facebook and Google, the FSB and the police need to do the request, to provide court sentence papers”*. These words by a FBK activist and the co-founder of OZI during the Privacy Camp in Brussels in 2020 [67], are at odds with the anti-monopolistic sensibilities of many European human rights and political activists (Pétin and Tréguer, 2018; Auray, *et al.*, 2014; Schneier, 2012; Stallman, 2015). Legalism, litigation strategies and Internet giants’ apparent respect of formal procedures when they process the requests for information, seem to protect Russian users against the arbitrariness of his own state, of which they have a habit and reasons to be wary. Relying on major Internet companies’ services, while being aware of non-transparent commercial uses of data, is not understood as a disadvantage because the primary threat model for these users leads to the prioritization of other risks, first and foremost surveillance, prosecution and various sanctions (up to imprisonment) on the part of the Russian state.

In addition to this observation of Google’s “harmlessness” with respect to their threat model, our respondents also refer to its active role in the fight against repressive laws in Russia. Its very selective compliance with Russian legislation is deemed to promote the free expression of civil society, especially when it comes to the referencing of protest sites and opposition media (such as Grani.ru, Smart Voting Site of Navalny or Khodorkovsky Media) by Google’s search engine, while they are officially included in RKN’s blacklist, or the hosting of mirrors of sites banned by RKN in application of the so-called “Lugovoy law” from 2014 onwards [68]. From 2016 Grani.ru has a permanent mirror [69] on the Google Cloud Platform [70], that the government cannot block because technically, they would then be obliged to block Google as a whole [71].

From 2019 onwards, complex negotiations between RKN and Google cast doubt on the start of the company’s collaboration with the Russian regulator, especially when cleaning up search results on Google Search is concerned. According to the words of anonymous sources of both RKN and Google, unlike Russian search engines, Google would not be directly “plugged” into the blacklist but would receive daily updates of blocked sites, which would allow it to select sites to be filtered (about 70 percent of the sites on the blacklist [72]). As for the official data from Google Transparency Report [73], for the same period only 40.4 percent of requests were satisfied in the category “Removed-legal” [74]. The deliberately imprecise information, that both opposing sides refuse to comment publicly, leads to divergent interpretations, varying from worries to a benefit of doubt. Thus, some experts [75] see these ambiguities as RKN’s tactic

of false pretense, to make people believe in the effectiveness of its pressure on the company, and which the latter does not deny, also for tactical reasons. These experts want to verify, empirically, Google's alleged compliance with the law: *"Try it yourself (...) Neither I nor the experts of Roskomsvoboda managed to find a site banned by RKN, which would not be issued on Google search, except for those that were previously excluded due to copyright claims"* [76]. Leonid Volkov (OZI's co-founder and Head of Navalny's regional headquarters network) goes further into the explanation. Despite the refusal of Google, Twitter and Facebook to comply with the law on personal data, the authorities did not dare to block them because *"RKN are not fools: they are well aware of the risk of shutting down YouTube"*; this blockage could only be a political decision taken at the highest level, of which the authorities do not have the courage anyway [77].

According to IT experts, a technical guarantee of non-blocking of YouTube by the authorities can be drawn from the fact that Google's complex and distributed infrastructure makes it impossible to fully apply the law on blacklisting and blocking to YouTube videos, because it would require the political courage to block all YouTube. Thus, even if some videos are the subject of insistent requests from RKN, the latter does not have real implementation tools and the company does not seem to give in to pressure. Indeed, none of the experts mentioned cases of politically motivated blocking of videos of Russian oppositionists on YouTube. According to one of them, if it was the case, it would be really alarming. Nevertheless, the few cases he knows where YouTube blocked a video of Navalny's channel are not the scandalous anti-corruption investigative films, but much more ordinary videos, such as Navalny's broadcast from Putin's press conference. The latter was blocked at the request of one of the state channels through the copyright ID-Content defense mechanism, because there was a TV presenter whose voice and face belong to the channel [78].

By betting on Google's resistance, in addition to criticizing the government's cowardice, our interlocutors often use the argument of its blatant technical incompetence in the face of the infrastructural complexity of Internet giants, which would condemn to failure all its attempts at censorship. This argument came to light in September 2017 during the aforementioned Google Global Cache servers' case [79]. The legal status of these GGCs came to be contested by the Russian regulator. RKN sent letters to operators in several Russian regions notifying them of the lack of certification of GGC servers, which would be punishable by a fine (applied to operators). Digital freedom defenders reacted by criticizing RKN's technical illiteracy, as it proved to be unable to distinguish between a "means of communication", to which the above-mentioned law applies, and a "communication service" (a system for managing the quality of communication services), a label which more closely applies to the status of the GGC [80] and for which certification is optional, according to the law [81]. The activists concluded that this new attack on Google by the FSB was aimed at slowing down YouTube (whose download speed has been significantly boosted by the GGC) on the eve of the 2018 presidential elections [82].

Despite empirical evidence of Google's resistance, worries persist that it may start implementing government requests more than it currently does. Indeed, these activists have no direct access to the company's representatives. Moreover, as a result of political pressure on Google-Russia LLC's managers [83], none of its employees make public statements; thus, controversies between Google and RKN take place, since 2013, behind closed doors and without any official comment from the company's side [84]. This opaque and preoccupying context does not challenge the benefit of the doubt granted to the company by Russian activists, based on their empirical observation that Google's services are safe for them, and the hope that the company is powerful enough to stand up to any repression attempts by the Russian authorities. Nevertheless, in the face of doubts, empirical evidence alone is not enough: it is also supported by activists' explanations of Google's rational reasons for continuing to resist, which they provide as an intellectual guarantee of its reliability. This reasoning also helps them to elaborate communication strategies to convince Google to continue not to comply.

## ***2.2. A libertarian free market utopia meets geopolitical factors***

To better assess the particularity of Internet freedom defenders' imaginaries about Google's motivations, it is useful to refer to research addressing the political economy inherent to the Internet freedom agenda. A

historically constituted symbiotic relationship between the American government and Silicon Valley companies brought Internet giants such as Google to the forefront of a new American cyber-diplomacy, inaugurated by the Internet freedom doctrine, first put forward by Hillary Clinton in 2010. This doctrine is “promoting a particular conception of networked communication that depends on American companies, supports Western norms, and promotes Western products” [85]. Beyond American interests within what came to be qualified as a “cyber war”, this doctrine established the “freedom-to-connect” as a new kind of human right specific to the digital era, which the United States aim to protect around the world in order to increase openness, facilitate informational and commercial exchanges. In this sense, Google’s “work abroad, including helping to expand connectivity in parts of the developing world and lobbying against censorship in authoritarian countries, closely coincides with the State Department’s freedom-to-connect agenda” [86].

The statements of our respondents regarding Google’s strategy are removed from these complex geopolitical considerations. They simply exclude any reference to state power; the mention of the undermining work carried out by the U.S. State Department and intelligence services towards civil society in post-Soviet countries is commonplace in official discourse in Russia, aimed at denigrating any local protest activity as remote-controlled. Thus, these bodies can only appear in their speeches in an ironic register, in the form of mockery of Russian state propaganda. When referring to Google’s conduct in a more serious tone, they all seem to converge towards the observation that if the company resists, it is not out of disinterested vocation as a defender of digital freedoms, but out of simple commercial interest: *“Why does Google support Russian civil society? Because the corporation wants to see Russia as a market where it can make a lot of money”* [87]. Conversely, the risk associated with possible compliance with Russian legislation is considered too high: the company would damage its reputation and lose profits on the Russian market, which would displease shareholders and lead to lower share prices: *“In general, the world of IT solutions is very much tied to the institution of reputation. Not that they are so kind and share the struggle against Putin. It’s a matter of money, and it’s unprofitable for them to give access to intelligence services. They are going to lose a lot of clients, including corporate ones.”* [88]

Thus, the protection of users against states considered to be disrespectful of human rights is viewed as a major component of reputation directly affecting global competitiveness [89]. This argument is part of the imaginary of the Internet as a network economy, referring to its “political genealogy” as combining “the libertarian spirit of the hippies with the entrepreneurial spirit of the yuppies” and developing with the privatization of the Internet in the 1990s on the West Coast [90]. Within our respondents’ “Internet imaginaries”, this American political genealogy seems to mingle harmoniously with a general post-Soviet mistrust *vis-à-vis* the state and governmental institutions, and with a relatively higher level of trust in business and private enterprise (Sapsford and Abbott, 2006). The Internet is therefore imagined as a sort of dematerialized “perfect” market, without intermediaries, where exchanges take place directly between interested parties and consumer confidence is rooted in the transparent flow of information and in “reputation systems” based on feedback from the consumer’s own experience [91]. Thus, “Google’s strength is (...) the ‘wisdom of the crowds’, which refers to certain (aggregate) theories of democracy” [92].

However, these visions of Google as a democracy defender that would be “naturally” democratic by its very genesis were severely shaken by the Snowden revelations in 2013. The following years were marked by companies’ multiple efforts to restore trust, demonstrate commitment to users’ protection and digital rights, and resist government pressure, including the adoption of end-to-end encryption techniques and the introduction of more detailed transparency reports showing the exact nature of governmental requests for users’ information (Tréguer, 2018). The period was also marked by a closer dialogue between these companies and NGOs defending digital freedoms (such as the EFF), “pushing them to adopt resistance strategies” and “to improve the protection of their users” [93]. It is noteworthy that both Russian NGOs considered here, Roskomsvoboda and OZI, have emerged and/or developed around the same period of increased influence of the field of HRDs and hacktivists among the Net giants.

Thus, the founding gesture for what later became the OZI was the dissemination, in 2015, of the petition to Google, Twitter, and Facebook, calling on them not to locate Russian user data on Russian territory: *“Don’t*

*move personal data to Russia! The Russian government is putting pressure onto Internet companies to move the personal data of their users to Russia. We don't agree this is 'in our own interests'” [94].*

Thereafter, the OZI makes multiple communication efforts to demonstrate to Google that requests from Russian authorities may be illegal and arbitrary, and complying with them would be harmful to reputation, and therefore ultimately to the proper conduct of business. Thus, after a temporary ban, on 8 September 2018 (the eve of municipal elections in several Russian cities), on paid advertising for the Navalny's FBK's meetings and the rotation of its videos on YouTube, following Google's receipt of a complaint from the Central Electoral Commission (CEC), Leonid Volkov notes with emotion this “unprecedented historical fact”: *“The Commission considers that our videos should be blocked under the ‘day of silence’. But Google has blocked our ads even for regions that are not holding elections and where rallies were allowed. (...) This makes Google's behavior particularly stupid. (...) We understand how it works. Every large corporation has its own legal compliance team, who says to the management: ‘Let's just comply with all the requirements of the authorities of each country (...) This approach works only for countries where there is the rule of law. (...) Now it is important for the international press to work as a fourth power and to knock on the head of a corporation that for some reason decided to fulfill a clearly illegal demand of the CEC and help President Putin’” [95].*

Beyond media interventions, OZI, Roskomsvoboda and other digital rights NGOs have an opportunity to carry out what they call “raising awareness work” both with the general public and major companies on the occasion of international events: Internet Governance Forums (IGF), Internet freedom festivals (IFF), RightsCon etc. These events provide various opportunities for discussions, both public and more or less informal, including with the intermediation of reputable digital freedom NGOs such as Front Line Defenders or Access Now. With the latter, OZI is in close contact: indeed, OZI's co-founder, M.K., is one of its volunteer representatives in Russia. Access Now acts as an intermediary between civil society representatives and major Internet companies (some, such as Google, Twitter or Facebook, are also its donors), particularly in matters concerning the security of user accounts, blocking and unblocking or loss of access to the account [96].

Some Russian digital freedom activists attended an informal meeting with representatives of Twitter and Facebook organized by Access Now in Brussels in 2017, which had as one of the purposes the “exchange of information” on the growing pressure from the Russian authorities on these companies, and to call on them not to yield. However, they failed to establish similar contacts with representatives of Google-Russia [97].

Ultimately, the international socialization of our interlocutors seems to integrate them into a certain culture of “transnational discursive democracy” (Padovani, 2012). Constituted through international Internet events, it is based on a direct dialogue between stakeholders of various levels and nature (NGOs, private sector, academics, shareholders) via horizontal discussion groups. Even if the real influence of actors from civil society on the transnational Internet regulation remains subject to debate, the principle of “multistakeholderism” seems to have become an omnipresent paradigm, with significant effects on the activists' visions of the potential impact on the agenda of the big Internet companies.

However, this trend seems to have been reversed from 2015 onwards, when several terrorist attacks made international headlines. These developments lead to what Félix Tréguer calls the “Snowden paradox”: “rather than rolling-out capacities for large-scale and suspicionless surveillance”, they “provide a detailed legal basis for these capacities, bringing a few new safeguards and slightly decreasing the level of secrecy to secure their legality and legitimacy” [98]. These processes “allow governments to impose new and tougher sanctions on companies refusing to collaborate, but also lead to new private/public partnerships in the field of surveillance, artificial intelligence and defense” [99].

This new delegation of governance to the private sector once again undermines utopian visions of a self-regulated transnational market, detached from any form of national sovereignty or geopolitical allegiance. Internet giants face two important challenges. On the one hand, the institution of reputation (dependent in



part on feedback from the international HRD field and its opinion leaders) which in turn affects profits. On the other hand, depending on the jurisdiction, states either aim to co-opt them or threaten to block them for non-compliance with the new “sovereignisation” laws: *“We [OZI] call on Big Tech (...) not to comply with these laws in Russia. What do they risk? Damage to their reputation, loss of money, drop in stocks. They will be pressured by the American public opinion and their own shareholders, if it turns out that Google is ‘spying for Russian government’. (...) It will be easier for it to leave Russia, although the market in Russia is quite large. Anyway, there will be losses in both cases”* [100].

In this rationale, political factors, including the tense relationship between the United States and Russia, are directly involved in representations of what would be acceptable or not, in the eyes of American public opinion and shareholders: “spying for the Russian government”. Shareholders would be outraged by the suspicion that Google is involved in the Russian state’s surveillance and repression of its citizens, and that Google’s potential cooperation with the state may lead the firm to carry on spying activities on the state’s behalf. It appears that even among Internet freedom defenders, attached to the libertarian political genealogy of the Web, justifications in terms of a self-regulated market can go hand in hand with the consideration of the particularly tense relationship between the United States and Russia, in the wake of Russian interference in the American presidential elections scandal. However, as previously described, the connections of Internet giants with the American government are not addressed by our respondents, both in our interviews and in more “public” interventions in the media. Shareholders, as a collective and market-led entities, are designated as the bearer of geopolitical reason.

Indeed, in the eyes of Internet freedom defenders, judging Internet giants on the basis of coherent ethical values (liberal or libertarian), or taking into full consideration all aspects of their behavior and their impact on the everyday life of the millions of users, does not seem topical. In view of the urgency of the situation, and far from any ideological purism, everything that helps to resist the main enemy — the Russian state — is considered as positive and friendly. Whatever motivations and logics are attributed to Internet giants, they are all beneficial as long as they allow them not to comply with Russian legislation.

This deliberately simplified tactical overview contrasts sharply with the logic of Western digital freedom activists, caught in the ethical dilemmas between the practical inevitability of Google (its widespread use by civil society actors) and its incompatibility with their political values (Tréguer, 2019; Schneier, 2015). For example, during Privacy Camp 2020 in Brussels, an activist from an ecological NGO mentioned the fact that Google was relaying the American climate sceptics’ lobby as one of the reasons why his association was looking for office suite solutions which would be independent from Google [101].

The same tactical reasoning mentioned above can lead some Russian Internet freedom defenders to deliberately neglect particular causes, hotly debated by their counterparts elsewhere, such as the antitrust fight. Thus, Leonid Volkov blames Pavel Durov for criticizing Apple and Google as they hinder, from their monopolistic positions, the development of applications by independent developers [102]. Volkov argues that the latter *“would never even come to existence without the infrastructure created by these big companies”* [103]. The concern expressed by one of the participants in the heated debate under this post, is that *“under the pretext of antitrust struggle, the aim is not to create a competitive environment, but to replace American monopolists with those from here, dependent on the Russian state and to simplify the access to data of Russian users”*.

Several of our interlocutors, fully integrated to the “transnational discursive democracy”, stressed that the misuse of user data by large technology companies is also a real social problem. But the particular national context leads them to prioritize the causes to be defended, thus adopting Internet giants as allies rather than targets. As one of our interlocutors puts it: *“If once in Russia the situation with violation of digital rights of citizens by the state finally normalizes, if the government stops putting pressure on companies, then we ourselves will switch and put pressure on companies in terms of privacy”* [104].

Thus, it appears that the Internet freedom activists we met during our research are neither devoid of any sense of criticism towards Google, nor being fooled by the current risks of the giant’s submission to the



new constraints imposed by state regulators in the context of the “infrastructural turn”. Nevertheless, they continue to highlight Google’s role as a defender of freedom of expression against the growing influence of the Russian State.



## Conclusion


This article has sought to highlight the ways in which the tense confrontation in Russia, between pro-government camp and liberal opposition, contribute to shaping representations about Google among Internet freedom activists and human rights NGOs, as well as to analyze their practices of using its services. Various criteria, data (indexes, statistics) and expert testimony that support practical choices of NGO activists and Internet freedom defenders seem to provide a guarantee of Google’s reliability in an uncertain situation, in which Russian actors are keen to prioritize different risks and to understand what they defend in priority and against whom. “My state is my main enemy” seems to be a formula that sums up well the polarized quasi-war situation in which these actors find themselves in their daily activities as well as in their social and professional representations. This trust in Google is indeed defined by this crude arithmetic of threats and power relations: “the enemy of my enemy is my friend”. Due to their positioning as “giants”, Google and the other platforms can stand up to the Russian state and the Russian state does not dare to block them, despite their very selective compliance with Russian legislation. Thus, a hegemonic position of giants, reproached to these companies in other contexts, is of value for specific groups, while the abuses that this position allows, are relativized, in a context where they are not monopolistic but in competition with Russian platforms. This stands in sharp contrast to the anti-monopolistic ideology of the libertarian founding fathers of the Internet. A reason for confidence are the self-regulatory capabilities of Internet giants: the competitive struggle for market share and the strength of global public opinion will “naturally” force them to comply with the new demands for ethical standards in data use, while any attempt by the state to regulate is perceived as threatening civil liberties.

However, a closer analysis attests to the diversity of understandings of the political role played by Google in Russia today. Some of our interlocutors among Internet freedom defenders adhere to Google’s positioning as a defender of digital freedoms. Others (such as Greenhouse of social technologies and IT security trainers) perceive and promote it, in a more pragmatic way, above all as a technique for circumventing institutional constraints: a tool for remaining active in the public space (YouTube, Google Ads) or an effective security device. In addition to the usability of Google services, civil society actors take advantage of the complexity of its legal status to circumvent the rules of Russian digital sovereignty. But in the increasingly polarized Russian context, the mere practical choice of these actors in favor of Google’s services is *de facto* politicized by the authorities. It places them in the same political “camp” as free Internet activists, rooted in a free-market libertarian utopia.

One of the issues that remains to be explored is how the Internet freedom defenders understand what the “infrastructural turn” consists of. They appear to be evasive about the nature of the link between Google and the U.S. authorities. Is this because the Russian authorities insist on this link in order to delegitimize the use of Google in Russia? Or does their reluctance to accept this link reflect their vision of Internet giants as part of self-regulatory market forces that would place themselves above state regulation?

The second path to explore would be an examination of the use of Google services within the Russian state administration, the public sector and companies with strong state participation. This use seems to be attested by a series of measures designed to prevent it and to replace it with national companies’ tools. However, the effectiveness of these measures seems uncertain. Exploring debates, actions and directives along these lines would reveal the specificities of what it means to be worried about Google and its ubiquitous nature, on the “other side” of the fence.

The third open question is the possible comparison between Russia and other authoritarian regimes by

looking at Google's position within their respective digital ecosystems. Indeed, if Google does not withdraw from the Russian market and does not fully submit to the rules of the game of the authorities as was the case in some other illiberal regimes (China, Iran), can we deduce that Google sees negotiation as a possibility that would not excessively harm its reputation? Answering these questions would contribute to addressing the issues of the "public-private" articulation and the privatization of surveillance" (Tréguer, 2018, Zuboff, 2019) in Internet policies, in comparison with other regimes. 

## About the authors

**Olga Bronnikova** is associate professor at Université Grenoble Alpes in the Department of Russian Studies in Grenoble, France.

E-mail: olga [dot] bronnikova [at] univ-grenoble-alpes [dot] fr

**Anna Zaytseva** is associate professor at University of Toulouse-Jean Jaurès in the Department of Russian Studies in Toulouse, France.

E-mail: anna [dot] zaytseva [at] univ-tlse2 [dot] fr

## Notes

1. Olga Baluk, "Google's blockage will block 30% of Russian sites, including Kremlin's site" (17 October 2019), at [https://www.znak.com/2019-10-17/it\\_ekspert\\_o\\_testirovanii\\_suverennogo\\_runeta\\_kitayskom\\_opyte\\_i\\_ucherbe\\_ekonomiki\\_rossii](https://www.znak.com/2019-10-17/it_ekspert_o_testirovanii_suverennogo_runeta_kitayskom_opyte_i_ucherbe_ekonomiki_rossii), accessed 12 March 2021.

2. Officially, the Federal Law 90-FZ "On amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection" (1 May 2019), obliged telecom operators to install state equipment at traffic exchange points (Deep Packet Inspection) in order to ensure Russia's security in case of disconnection from the Internet from the outside. For more details on "digital sovereignization" in Russia, see Wijermars, 2020; Musiani, *et al.*, 2019.

3. See the article by Ksenia Ermoshina and Francesca Musiani in this special issue.

4. Google search bypassed Yandex in terms of total monthly audience in Russia in April 2016 (Ksenia Boletskaya, "Google can call itself the leader of Runet" (30 May 2016), at <https://www.vedomosti.ru/technology/articles/2016/05/31/643012-google>, accessed 12 March 2021). The key factor in the growth of Google's share in Russia is its control over the Android operating system. But experts say that Yandex has a richer Russian search ("Who's better: Yandex or Google? Five Search Engine Specialists Answer," *Meduza* (1 June 2016), at <https://meduza.io/feature/2016/06/01/kto-kruche-yandeks-ili-google>, accessed 12 March 2021).

5. In 2019, approximately 30 percent of the entire Russian population uses YouTube (Denis Volkov, Stepan Gontcharov, "Russian Media Landscape 2019" (1 August 2019), <https://www.levada.ru/2019/08/01/21088/>, accessed 12 March 2021).

6. Asmolov and Kolozaridi, 2017, p. 20.

7. Michaelsen, 2018, p. 3,862.

8. See the introduction to this issue.

9. See Liudmila Sivetc's article in this issue.

10. See Françoise Daucé and Benjamin Loveluck's article in this issue.

11. This article does not focus on associations loyal to the government, which have a completely different relationship to the use of the services of various Internet companies and issues of digital freedoms.

12. This law qualifies as “foreign agent” any Russian NGO (from 2017 and 2018, also media outlets and journalists) receiving funding from abroad and carrying out “political activity” in Russia.

13. Aimed at closing down and judicially penalizing foreign or international NGOs recognized as a threat to the security of the Russian Federation.

14. Penalizing unregistered individuals or organizations “carrying out political activities in the interests of foreign sources”.

15. This case will be studied more closely in the second part of the article.

16. Michael Malloy and Pavel Arievidh, “Russia: Penalties for Violation of Data Localization Rules are Dramatically Increased” (10 December 2019), at <https://blogs.dlapiper.com/privacymatters/penalties-for-violation-of-data-localization-rules-are-dramatically-increased/>, accessed 12 March 2021.

17. This was the case, for example, on February 2020. It distinguishes Google from Facebook and Twitter: in view of the lack of a foothold on Russian territory and the absence of a legal cooperation agreement between Russia and the United States, many requests from the Russian authorities to them do not even reach their recipients (RSF, 2019 and interview with U.G., Berlin's office of RSF, 12 May 2020).

18. “Putin signed the law banning censorship on the Internet” (30 December 2020), at <https://www.interfax.ru/russia/743586>, accessed 12 March 2021.

19. It is included in the series of laws about “Sovereign Internet”.

20. For security reasons we do not disclose the identities of the NGOs. Our respondents were an IT manager for a human rights NGO dedicated to monitoring political persecution; the head of an NGO specialized in anti-racism and discrimination; a communication manager for an international anti-corruption NGO; and a PR manager for a Russian anti-corruption NGO.

21. For this article, we analyze data on the Belarusian case only to the extent that they contribute to analyze the Russian case.

22. E.g., Panel “Actually, In Google We Trust?” moderated by Resistic members, Privacy Camp, Brussels, January 2020.

23. NGOs focused on ecology, children's rights, and media rights were present at this training.

24. <https://about.google/human-rights/>, accessed 12 March 2021.

25. Global Network Initiative, “The GNI principles at work” (2019), at <https://globalnetworkinitiative.org/wp-content/uploads/2020/04/2018-2019-PAR.pdf>, accessed 12 March 2021.

26. A.S., Panel on the regulation of algorithms, conference “Setevoy Sentyabr”, 3–4 September 2020.

27. Interview with I.S., digital security trainer, Minsk, April 2019.

28. [https://transparencyreport.google.com/user-data/overview?user\\_requests\\_report\\_period=series:requests,accounts;authority:RU;time:&lu=user\\_requests\\_report\\_period](https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:RU;time:&lu=user_requests_report_period).

29. Interview with B.B., IT manager for a human rights association dedicated to monitoring political persecution and the infringement of the right to freedom of assembly, 4 April 2020 (on Telegram).

30. Interview with M.K., 8 April 2020, Jitsi Meet.

31. Interview with I.S., April 2019.

32. Training with S.S., 6–7 March 2020, Paris; discussions during the conference “Setevoy Sentyabr”, 3–4 March (panel “Privacy is not a fad”).

33. Since the law on so-called “foreign agents” (2012).

34. Interview with I.S., April 2019.

35. Interview with A.V., NGO specialized in anti-racism and discrimination, Moscow, August 2019.

36. Interview with L., from an NGO working on arbitrary arrests, Moscow, February 2018.

37. Interview with A.S., civic tech ONG, online, April 2020.

38. Interview with L., left-wing activist, Saint-Petersburg, February 2018.

39. Interview with A.V., August 2019.

40. <https://ssd.eff.org/>.

41. Interview with I.S., Minsk, April 2019. Many Belarusian trainers work in Russia.

42. Interview with I.S., April 2019.

43. E-mail discussion with S.S., April 2020.

44. Interview with L.E., Software Development Engineer at Censored Planet Lab, 6 May 2020.

45. Interview with B.B., 4 April 2020.

46. See e.g., Google’s Transparency Reports or Global Network Initiative’s stated objective to advance freedom of expression and privacy in the IT sector.

47. Interview with trainers.

48. [https://www.cnews.ru/news/top/2020-01-29\\_roskomnadzor\\_zablokiroval](https://www.cnews.ru/news/top/2020-01-29_roskomnadzor_zablokiroval).

49. E-mail discussion with S.S., April 2020.

50. Interview with A.V., August 2019.

51. Interview with B.B., April 2020.

52. Interview with A.S., April 2020.

53. *Ibid.*

54. *Ibid.*

55. [https://www.dp.ru/a/2016/11/15/Microsoft\\_po\\_trebovaniyu\\_R](https://www.dp.ru/a/2016/11/15/Microsoft_po_trebovaniyu_R).

56. <https://www.google.com/intl/fr/nonprofits/>.

57. <https://www.techsoup.org/>.

58. Cit. in Ermoshina, 2018, p. 41.

59. Interview with A.S., April 2020.

60. Interview with B.B., April 2020.

61. Interview with A.S., April 2020.

62. <https://roskomsvoboda.org/>, accessed 12 March 2021.

63. Joint participation in, and organization of events, mutual contributions to publications and expert reports, etc.

64. <https://ozi-ru.org>, accessed 12 March 2021.

65. <https://ozi-ru.org/proekty/indeks-svobod-interneta/>, accessed 12 March 2021.

66. <https://ozi-ru.org/proekty/internet-repressii/karta/>, accessed 12 March 2021.

67. Round table “Actually in Google We Trust ? A ‘Deconstructing’ Conversation on Russian Internet,” Privacy Camp, Brussel, 21 January 2020, at <https://www.youtube.com/watch?v=CjnVq4zLT6s&t=1971s>, accessed 12 March 2021.

68. The law allowing an immediate blocking by RKN of sites deemed extremist and calling for “mass disorder” outside of any legal proceedings.

69. <https://grani-ru-org.appspot.com/>, accessed 12 March 2021.

70. This way of circumventing blockages via the clouds controlled by Internet giants, first discovered by the Chinese activists, was then taken up within the “Collateral Freedom” programs by RSF. Grani.ru was one of Web sites that benefited from its first edition in 2015.

71. Interview with Y.B., chief editor of Grani, Paris, 15 January 2018.

72. Ksenia Boletskaya, “Google started removing websites banned in Russia from its search,” *Vedomosti* (6 February 2019), at <https://www.vedomosti.ru/technology/articles/2019/02/06/793499-google>, accessed 12 March 2021.

73. Google’s Transparency Report, at [https://transparencyreport.google.com/government-removals/by-country/RU?hl=en&removal\\_compliance\\_rate=requestor::period:Y2018H1;authority:RU&lu=removal\\_compliance\\_rate](https://transparencyreport.google.com/government-removals/by-country/RU?hl=en&removal_compliance_rate=requestor::period:Y2018H1;authority:RU&lu=removal_compliance_rate), accessed 12 March 2021.

74. Among multiple categories introduced in Google’s Transparency Reports from 2019, this one seem to be the only one that refers to requests from authorities that have been satisfied in accordance with the country’s legislation.

75. A. Plushev, journalist for Echo of Moscow and Roskomsvoboda’s expert.

76. Aleksander Plushev, “Comment: Has Google begun to censor search results in Russia?” (8 February 2019), at <https://p.dw.com/p/3D038>, accessed 12 March 2021.



77. Leonid Volkov, “Why are Western Internet companies cooperating with the Putin regime to censor the Web?” (9 April 2018), at <https://www.opendemocracy.net/en/odr/western-internet-companies-censor-russia/>, accessed 12 March 2021.

78. Interview with L.E., Software Development Engineer at Censored Planet Lab, 6 May 2020.

79. GGC is a traffic management system made up of servers provided by Google and installed on the networks of local operators to store the most popular heavy content, which makes it possible to lighten cross-border traffic. These servers are owned and managed by Google, at no cost to the ISPs. About 30 percent of the traffic of Russian operators is carried by Google’s resources (Maria Kolomychenko, “Suspicious cache: The FSB is interested in Google servers,” *RBK* (19 September 2017), at [https://www.rbc.ru/technology\\_and\\_media/19/09/2017/59c1544d9a79476b8e8c04e4](https://www.rbc.ru/technology_and_media/19/09/2017/59c1544d9a79476b8e8c04e4), accessed 12 March 2021).

80. Mikhail Klimarev, “Roskomnadzor declared war on Google Global Cache” (20 February 2018), at <https://roskomsvoboda.org/36499/>, accessed 12 March 2021.

81. M.K.’s publication on his channel on Telegram, October 2017.

82. In March 2021, the techniques of slowing down some services, such as Tweeter, are tested again by RKN in the run-up to the 2021 Duma elections, which makes experts fear the same problems for YouTube and Facebook soon.

83. See for more details Soldatov and Borogan, 2015.

84. Our attempts to discuss issues concerning relations with the Russian regulator, during the meeting with the only Google’s muscovite office employee we were able to meet, did not give any result. He was not allowed to communicate on issues related to the Russian state.

85. Powers and Jablonski, 2015, p. 6.

86. Powers and Jablonski, 2015, p. 74. As to Google’s interests in this cooptation, first, in this manner, the company enhances its own security, at the expense of all competitors; second, its very business model, based on the extraction and commodification of big data, implies constantly expanding the number of users and the diversity of domains (tools, services) that would allow it to collect them (Powers and Jablonski, 2015, p. 97).

87. Vladislav Zdolnikov, “Russian society and Google share the same interest,” at <https://roskomsvoboda.org/59942/>, accessed 12 March 2021.

88. Interview with B.B., 4 April 2020, via Telegram.

89. Its importance is confirmed by precedents in other illiberal contexts. For example, international human rights NGOs have criticized Google’s attempts to reintroduce its search engine in China in 2016 in a censored version that complies with Chinese law. These NGOs warned the company against these compromises, which could make it lose the confidence of many users elsewhere in the world, by showing that “all individual freedoms are, for Google, negotiable” (Arsène, 2019).

90. Loveluck, 2015, p. 86.

91. Loveluck, 2015, p. 125.

92. Loveluck, 2015, p. 253.

93. Tréguer, 2018, pp. 18–26.

94. Leonid Volkov, “Don’t move personal data to Russia!” Petition on Change.org, at <https://urlz.fr/dN11>, accessed 12 March 2021.
95. “YouTube blocked ads for the September 9 rally,” Grani.ru (8 September 2018), at <https://grani-ru-org.appspot.com/Internet/m.272609.html>, accessed 12 March 2021.
96. Access Now’s country representatives, who are well integrated into the relevant local communities, often serve as guarantors of the identity of users experiencing account problems and enable them to shorten the response time of large companies to their requests (from several months to a few days). Interview with O. and I., Access Now, online, 2019.
97. Interview with representative of a Russian NGO, April 2020.
98. Tréguer, 2018, p. 40.
99. Tréguer, 2018, p. 40. In Russia, where the international anti-terrorism agenda is since the early 2000s closely followed by the authorities, concerned with domestic terrorism from the Caucasus, this paradox is both a consequence of the Snowden revelations and of the recent confrontation with Western diplomacy after the annexation of Crimea in 2014.
100. Interview with M.K.
101. Round table “Activism and digital infrastructures,” Brussels, 21 January 2020.
102. Pavel Durov, “How Apple is killing off startups around the world — and how to stop it” (9 July 2020), at <https://te.legra.ph/Kak-Apple-unichtozhaet-startapy-po-vsemu-miru--i-kak-ehto-mozhno-ostanovit-07-09>, accessed 12 March 2021.
103. Personal Facebook page of L. Volkov, at <https://www.facebook.com/leonid.m.volkov/posts/3179430715412873>, accessed 12 March 2021.
104. <https://www.youtube.com/watch?v=0pajn1yh9ok&t=2429s>, accessed 12 March 2021.

## References

- Madeleine Akrich, Michel Callon and Bruno Latour, 1988. “A quoi tient le succès des innovations? 1: L’art de l’intéressement; 2: Le choix des porte-parole,” *Gérer et Comprendre. Annales des Mines*, number 11, pp.4–17; number 12, 14–29.
- Séverine Arsène, 2019. “La Chine et le contrôle d’Internet: Une cybersouveraineté ambivalente,” *Annuaire Français de Relations Internationales*, volume XX, at <https://www.afri-ct.org/article/la-chine-et-le-controle-dinternet-une-cybersouverainete-ambivalente/>, accessed 24 April 2021.
- Gregory Asmolov and Polina Kolozaridi, 2017. “The imaginaries of RuNet: The change of the elites and the construction of online space,” *Russian Politics*, volume 2, number 1, pp. 54–79. doi: <https://doi.org/10.1163/2451-8921-00201004>, accessed 24 April 2021.
- Eric Brousseau, Meryem Marzouki and Cécile Méadel (editors), 2012. *Governance, regulation and powers on the Internet*. Cambridge: Cambridge University Press. doi: <https://doi.org/10.1017/CBO9781139004145>, accessed 24 April 2021.
- Jenna Burrell, 2016. “How the machine ‘thinks’: Understanding opacity in machine learning algorithms,” *Big Data & Society* (6 January).

doi: <https://doi.org/10.1177/2053951715622512>, accessed 24 April 2021.

Paul J. DiMaggio and Walter W. Powell, 1983. “The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields,” *American Sociological Review*, volume 48, number 2, pp. 147–160.

doi: <https://doi.org/10.2307/2095101>, accessed 24 April 2021.

Ksenia Ermoshina, 2018. “Au code, citoyens: Mise en technologies des problèmes publics,” Thèse de doctorat en Socio-économie de l’innovation, at <https://pastel.archives-ouvertes.fr/tel-01712465v1>, accessed 24 April 2021.

Evgeny Finkel and Yitzhak M. Brudny, 2012. “No more colour! Authoritarian regimes and colour revolutions in Eurasia,” *Democratization*, volume 19, number 1, pp. 1–14.

doi: <https://doi.org/10.1080/13510347.2012.641298>, accessed 24 April 2021.

Patrice Flichy, 2004. “The imaginary Internet: How utopian fantasy shaped the making of a new information infrastructure,” *Business History Conference*, at <https://thebhc.org/imaginary-internet-how-utopian-fantasy-shaped-making-new-information-infrastructure-0>, accessed 24 April 2021.

Sam Jewler, 2015. Report “Mission creep-y: Google is quietly becoming one of the nation’s most powerful political forces while expanding its information-collection empire,” *Public Citizen* (25 August), at <https://www.citizen.org/article/mission-creep-y-google-is-quietly-becoming-one-of-the-nations-most-powerful-political-forces-while-expanding-its-information-collection-empire/>, accessed 12 March 2021.

Anne Le Naëlou, 2004. “Pour comprendre la professionnalisation dans les ONG: Quelques apports d’une sociologie des professions,” *Revue Tiers Monde*, volume 4, number 180, pp. 773–798.

doi: <https://doi.org/10.3917/rtm.180.0773>, accessed 24 April 2021.

Lawrence Lessig, 2006. *Code*. Version 2.0. New York: Basic Books.

Kevin Limonier, 2017. “Internet russe, l’exception qui vient de loin,” *Le Monde diplomatique*, pp. 1, 22, 23, at <https://www.monde-diplomatique.fr/2017/08/LIMONIER/57798>, accessed 24 April 2021.

Benjamin Loveluck, 2015. *Réseaux, libertés et contrôle: Une généalogie politique d’Internet*. Paris: Armand Colin.

Michael Michaelson, 2018. “Transforming threats to power: The international politics of authoritarian Internet control in Iran,” *International Journal of Communication*, volume 12, pp. 3,856–3,876, and at <https://ijoc.org/index.php/ijoc/article/view/8544>, accessed 24 April 2021.

Francesca Musiani, 2018. “L’invisible qui façonne. Études d’infrastructure et gouvernance d’Internet,” *Tracés. Revue de Sciences humaines*, number 35, pp. 161–176.

doi: <https://doi.org/10.4000/traces.8419>, accessed 24 April 2021.

Francesca Musiani, Benjamin Loveluck, Franoise Daucé and Ksenia Ermoshina, 2019. ““Digital sovereignty”: Can Russia cut off its Internet from the rest of the world?” *The Conversation* (28 October), at <https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-internet-from-the-rest-of-the-world-125952>, accessed 13 May 2020.

Frank Pasquale, 2015. *The black box society: The secret algorithms that control money and information*. Cambridge, Mass.: Harvard University Press.

Patrick Pétin and Félix Tréguer, 2018. “Building and defending the alternative Internet: The birth of the digital rights movement in France,” *Internet Histories*, volume 2, numbers 3–4, pp. 281–298.

doi: <https://doi.org/10.1080/24701475.2018.1521059>, accessed 24 April 2021.

Shawn M. Powers and Michael Jablonski, 2015. *The real cyber war: The political economy of Internet freedom*. Urbana: University of Illinois Press.

Reporters Without Borders, 2019. “Taking control? Internet censorship and surveillance in Russia,” at [https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2019/russiareport\\_web\\_updated.pdf](https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2019/russiareport_web_updated.pdf), accessed 12 March 2021.

Roger Sapsford and Pamela Abbott, 2006. “Trust, confidence and social environment in post-communist societies,” *Communist and Post-Communist Studies*, volume 39, number 1, pp. 59–71. doi: <https://doi.org/10.1016/j.postcomstud.2005.12.003>, accessed 24 April 2021.

Carl Schmitt, 2007. *The concept of the political*. Translation, introduction and notes by George Schwab. Chicago: University of Chicago Press.

Andrey Soldatov and Irina Borogan, 2015. *The red Web: The struggle between Russia’s digital dictators and the new online revolutionaries*. New York: Public Affairs.

Nick Srnicek, 2017. *Platform capitalism*. Cambridge: Polity Press.

Félix Tréguer, 2019. “L’informatique accentue les rapports de pouvoir plus qu’elle n’égale les rapports de force,” *Libération* (15 December), at [https://www.liberation.fr/debats/2019/12/15/felix-treguer-l-informatique-accentue-les-rapports-de-pouvoir-plus-qu-elle-n-egalise-les-rapports-de\\_1769374](https://www.liberation.fr/debats/2019/12/15/felix-treguer-l-informatique-accentue-les-rapports-de-pouvoir-plus-qu-elle-n-egalise-les-rapports-de_1769374), accessed 12 March 2021.

Félix Tréguer, 2018. “US technology companies and state surveillance in the post-Snowden context: Between cooperation and resistance,” at <https://halshs.archives-ouvertes.fr/halshs-01865140>, accessed 12 March 2021.

Zeynep Tufekci, 2015. “Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency,” *Colorado Technology Law Journal*, volume 13, pp. 203–217, and at <https://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf>, accessed 24 April 2021.

Mariëlle Wijermars, 2020. “‘RuNet sovereignty’: How Russia is trying to isolate its Internet segment from the rest of the world, maybe,” *Meduza* (7 February), at <https://meduza.io/en/episodes/2020/02/07/runet-sovereignty-how-russia-is-trying-to-isolate-its-internet-segment-from-the-rest-of-the-world-maybe>, accessed 24 April 2021.

Shoshana Zuboff, 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.

---

## Editorial history

Received 2 April 2021; accepted 7 April 2021.



“‘In Google we trust’? The Internet giant as a subject of contention and appropriation for the Russian state and civil society de Olga Bronnikova et Anna Zaytseva est mis à disposition selon les termes de la [licence Creative Commons Attribution — Pas d’Utilisation Commerciale — Partage dans les Mêmes Conditions 4.0 International](https://creativecommons.org/licenses/by-nc-sa/4.0/).

‘In Google we trust’? The Internet giant as a subject of contention and appropriation for the Russian state and civil society

by Olga Bronnikova and Anna Zaytseva.

*First Monday*, volume 26, number 5 (May 2021).

doi: <https://dx.doi.org/10.5210/fm.v26i5.11709>