JeDEM Issue 13(1): 71-100, 2021
ISSN 2075-9517
http://www.jedem.org
Date of submission: 27.01.2021
Date of acceptance: 23.04.2021
Article DOI 10.29379/jedem.v13i1.633

I Agree to the Terms and Conditions: Negotiating Privacy in Central Asia

Malika Toqmadi

PhD candidate, University College London
Gower St, London WC1E 6BT, UK

Author ORCID Nr: 0000-0003-4016-3499
malika.toqmadi.20@ucl.ac.uk

Natalia Zakharchenko

Independent researcher[1]
Galvanistraat 1001, 3029AD, Rotterdam, the Netherlands

Author ORCID Nr: 0000-0001-6953-0411
n.zakharchenko@osce-academy.net

Abstract: This study explores the formation of privacy as a value for different stakeholders in Kazakhstan and Kyrgyzstan. Building on fieldwork in the two states, the study represents one of the few attempts to map out the interpretations and practices of privacy in Central Asia. The rapid digitalization processes unfolding in these two countries, which have similar cultural and historical roots, provide an illustrative setting of how privacy can be scrutinized in dissimilar political contexts, how its value is defined by the policies of the past, and what the apparent and dormant risks for society are.

Keywords: privacy; digitalization; democracy; Kazakhstan; Kyrgyzstan

Acknowledgment: The research was supported by a grant from the Foundation Open Society Institute in cooperation with the Eurasia Program of the Open Society Foundations.

[1] The author will also take upon the role of the Marie-Curie PhD candidate in the field of human rights at Ruhr University Bochum (RUB), Germany, in September 2021.

1. Introduction

The penetration and diffusion of the Internet and digital technologies have aroused policy and scholarly discussions over the potential impact that these technologies can have in the context of different political systems. Meanwhile, hopes for new media's ability to transform oppressive regimes and lead to democratization have faded as both authoritarian and democratic states have employed ubiquitous and pervasive surveillance, reconfiguring the concept of privacy (Ambay et al., 2019; Diamond, 2019; Shahbaz, 2018).

Being a concept-in-the-making, privacy is actively molded in policy "kitchens" by various actors across political contexts. While the European Union has been vocal in its aspirations to develop the "golden standard" of privacy through the General Data Protection Regulation (GDPR) (Arora, 2019, p. 369), parallel standards have been continuously appearing across the globe. Japan's Act on the Protection of Personal Information, the California Consumer Privacy Act, the APEC Privacy Framework, Australia's Notifiable Data Breaches, and India's Personal Data Protection Bill are just a few of the numerous national and regional initiatives that address the pressing issue of protecting personal privacy and data online. On the other hand, China has aspired to be an alternative trendsetter for a range of countries through its successful introduction of the social credit system, which is based on ubiquitous surveillance and the intrusion of its citizens' privacy (Wong & Dobson, 2019).

What is privacy? What stands behind its "universality" and can it, in fact, be universal in the first place? While there is a general consensus that interpretations of privacy might vary in different cultural contexts (De George, 2003; Solove, 2008), academia remains persistently Western-centric, still drawing its empirical evidence from a limited area of the world (Arora, 2019, pp. 368, 371). However, research beyond the Western world can reveal the multidimensional nature of privacy and the numerous ways it can be comprehended in a diversity of contexts.

Accordingly, the current study explores how the concept of privacy is interpreted in one of the least studied regions of the world, Central Asia, in the cases of neighboring Kazakhstan and Kyrgyzstan. A comparative analysis of these two countries allows us to examine privacy in the context of two states with different political and economic profiles but with shared cultural, historical, and social settings.

Kazakhstan and Kyrgyzstan share a common history in the form of their Soviet past; prior to this, they formed part of the historical region of Turkestan, and territories of both countries were predominantly populated by societies that led a nomadic lifestyle (Brower, 2003). Modern borders between Central Asian countries were delimited only during Soviet rule (Abazov, 2008; Sabol, 1995), and, identity-wise, the two nations go as far as describing each other as siblings, citing the common proverb "*Kyrgyz kazak bir tugan*" in Kazakh or "*Kyrgyz kazak bir tuugan*" in Kyrgyz (which translate to "Kyrgyz and Kazakh are siblings"). Moreover, during more than 70 years of Soviet rule, Central Asia was largely considered as a common unit of governance with somewhat uniform policies applied and practiced (Sabol, 1995). This legacy still influences and shapes the politics and bureaucracies in both countries. As such, it is unsurprising that there is an abundance of research that has selected

Kazakhstan and Kyrgyzstan as comparable Central Asian cases, especially those scrutinizing divergent political regimes in similar cultural and historical settings (Cummings & Nørgaard, 2004; Furstenberg, 2017; B. Junisbai & A. Junisbai, 2019; Melvin, 2004, Sharshenova 2015).

Kazakhstan is an upper-middle-income country, rich in natural resources, mostly in oil and gas (The World Bank, n.d.). The country has been ruled by Nursultan Nazarbayev (currently in an official position of the 'Leader of the Nation') since its independence gained as a result of the Soviet Union collapse in 1991 (Bohr et al., 2019). Kyrgyzstan, on the other hand, is a lower-middle-income country, heavily relying on remittances from its migrants in Russia as well as gold mining.[2] The country has a turbulent political portfolio: it has faced two revolutions in 2005 and 2010, as well as political turmoil in 2020, jiggling between authoritarian and democratic regimes (The World Bank, n.d.). Currently, access to the Internet continues to expand in both states, with an overall penetration rate of 77% in Kazakhstan and 78% in Kyrgyzstan (Freedom on the Net, 2019). Since the early 2000s, the governments in the two countries have placed special attention on their policy agendas to digitalization, accelerating these processes throughout the 2010s (see Appendix 1).

Building on fieldwork in Kazakhstan and Kyrgyzstan, the present analysis reveals the politics and interpretations of privacy in these countries' public sectors. This research chooses to leave the discussion of the role of private actors beyond its scope and instead, narrows the focus to individual privacy vis-a-vis the state. Thus, we examine interpretations of privacy by three major stakeholders: the state, civil society, and individuals.

Based on the theoretical premise that privacy is inherent to democracy, we demonstrate the role of privacy in democratic and authoritarian practices and discuss the intricacies of governance in such settings. As the further analysis reveals, Kazakhstan's policies in the digital domain are driven by its highly authoritarian government structures, securitizing the sphere, and embracing paternalistic narratives around privacy, while the more liberal but less politically stable Kyrgyzstan predominantly neglects privacy in its policy agenda in favor of the pursuit of rapid modernization. These contrasting contexts, however, have brought similar outcomes in the form of the inherent dangers of the infringement of the general population's privacy.

2. Methods

Given the multidisciplinary nature of privacy, the present study's methods incorporated different disciplinary angles and examined the dynamics of the formation of the value of privacy by various actors. The study was based on focus group discussions (FGDs) with citizens and in-depth interviews with relevant actors, such as state officials, experts in information and communication technologies (ICT), lawyers, civil society representatives, individual activists, and scholars. The field study took place between September 2019 and March 2020 in three major cities of the two states: Almaty and Nur-Sultan (Kazakhstan) and Bishkek (Kyrgyzstan).

[2] Although the state shares only around 30% of the Canadian mining company managing the largest gold deposit (Bankwatch, n.d.).

A comprehensive desk review was conducted prior to the field research, analyzing the relevant legislations and digitalization and privacy policies in Kyrgyzstan and Kazakhstan. The study also attempted to integrate feedback and reflect on the debates raised during presentations, conferences, and other relevant events that the authors attended at local and international levels.

To explore the topic in-depth, semi-structured interviews with high-level representatives of relevant governmental agencies, prominent members of civil society, and scholars were conducted (see Appendix 2). In total, nine interviews in Kazakhstan and seven in Kyrgyzstan were held. In the initial stage, a "map" of stakeholders and experts was drawn based on key informant sampling through pilot interviews (Patton, 2002, p. 430), desk research, and the authors' extensive local network. This "map" was then supplemented with suggestions for interviewees based on the chain-referral snowball sampling method. A set of semi-structured questions was prepared for each category of participants, with a focus on interpretations and major paradigms related to privacy, state efforts/policies in the field of privacy, training/education about privacy, citizens' stance on their own privacy and personal data, and the risks and precedents of privacy breaches. Often, the debates unfolded beyond the anticipated directions and sparked discussion of other important issues, such as what triggered privacy concerns among citizens or the role of private companies in shaping public privacy policies. All interviews were audio-recorded and notes were taken with the consent of participants.

Two FGDs with everyday users of digital technologies were held in Almaty and Bishkek to understand privacy interpretations on the individual level, as well as the behaviors, threats, and issues citizens encounter in the digital domain. The participants were selected through multi-stage purposeful random sampling (Omona, 2013, p. 181). In the initial stage, professional marketing agencies were commissioned to undertake random street recruitment. The recruiters asked bypassers in major malls, central streets, and other busy public places to complete prepared questionnaires. Each group comprised of nine to 10 people (see Appendices 3 and 4). We excluded experts in ICT, digital security, sociology, marketing, ICT hardware production and sales, social media specialists, and software engineers to avoid "expert" bias and its subsequent influence on the opinions of the rest of the group. We also excluded foreigners in order to narrow the research focus to only citizens of the two selected countries. The common denominator of the stakeholder group was that they all were smartphone and Internet users, which it was assumed meant they were exposed to digital privacy concerns daily. Special attention was paid to ensuring even distribution and diversity among the selected participants, considering their age, gender, and ethnic balance according to the demographic compositions of the corresponding countries (Bole et al. 2017, Kumer & Urbanc, 2020). The discussions were organized around several predefined thematic blocks. During the introductory part, the participants were asked to visually describe how they understood the word "privacy" (*privatnost*) and then explain their drawings. In the second part, they were asked to compile and discuss a "hierarchy" of information about themselves, in which they expressed what kind of data they were willing to share comfortably (with the state, businesses, and fellow citizens) and what they preferred to conceal and why. We then discussed their everyday behaviors and perceptions regarding the protection of their privacy, including digital hygiene, public surveillance infrastructure, e-governance, the collection of biometric data by the state, data leaks, and other

issues. Exit questions provided the participants with an opportunity to raise their concerns over other topics that had not been explored.

All attendants were encouraged by a small reward for participation (around 15 USD) and signed an informed consent form prior to the FGDs. The focus groups were audio-recorded, and notes were taken by one of the authors during the discussions. In the case of both the FGDs and expert interviews, a non-verbatim method was applied to transcribing the materials. A thematic qualitative content analysis was then used to explore the collected data. All interviews and FGDs were conducted in the Russian language, and translation into English was made by the authors.

3. Privacy Genesis in Central Asia

3.1. Culture

Privacy is a multidisciplinary phenomenon. For example, a recent handbook authored by leading scholars in the field of privacy explores the variety of disciplinary prisms within the concept, from medicine to technology and from law to anthropology (Van der Sloot & De Groot, 2018). With some adaptations, most scholars studying privacy have referred to its textbook definition developed by privacy studies pioneer Alan Westin (1967, p.7), which describes it as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others."

While acknowledging the cultural pervasiveness of the notion of privacy, extant scholarship has tended to neglect global diversities. As Arora (2019, p. 368) summarizes, "it disproportionately draws from empirical evidence on privacy attitudes and behaviors of Western-based, white, and middle-class demographics to theorize privacy in this digitally mediated world."

Indeed, the concept of privacy belongs to the realm of the so-called "untranslatables"— culturally-specific notions that can never be translated totally adequately (Boym, 1994, pp. 3, 76) into most of the world's languages (Arora, 2019). Neither the Kazakh, Kyrgyz, nor Russian languages have direct translations of the term but embrace only separate aspects of the phenomenon, referring to it as "secretness" (*qupïyalılıq* (KZ), *kupuyaluuluk* (KG)), "confidentiality" (*konfidentsialnost* (RU)), "private" (*chastnaya* (RU), or "personal" life (*lichnaya* (RU); *jeke* (KZ); *zheke* (KG)). Klepikova (2015, p. 358), for instance, points to the fact that the linguistic transfer of the word "privacy" into Russian as "*privatnost*" remains absent in "colloquial or literary style."

However, we should remain conscious of the risks of exotifying various cultural contexts, stripping the communities outside the West of the value of privacy (Arora, 2019). There is arguably no culture that does not have even a minimal requirement of privacy (Moore, 1984), which is formed under the influence of various environmental factors, such as religious and cultural characteristics, historical preconditions, technological developments, political regimes, and economic settings, etc. Therefore, the concept of privacy "must be mapped like terrain" (Solove, 2008, cited in Arora, 2019, p. 371) when accepting and studying its variations across nations and cultures. Central Asia, in particular, has been often overlooked in academia, even though it represents a vibrant field for

analysis considering the complicated privacy setting of the Soviet past and its swift digitalization following independence in 1991.

3.2. Political Regime

Political regimes are a particularly important variable that we discuss in more detail here. Despite the fact that privacy has become an issue on the radars of democratic and authoritarian regimes alike (Csaky, 2021), theorists agree that privacy is intrinsic to democracy. Following the simplest definition of democracy as a form of governance in which people have the authority to choose their governing legislators (Merriam-Webster Dictionary), privacy is essential to democratic voting and open public discussion (Lever, 2016). However, democracy is not only centered around elections but should also ensure the "individual autonomy, identity formation, and intimate relationships" of free and equal citizens (Loh, 2019). As argued by Lever:

> *…[P]rotection for anonymity, confidentiality, seclusion, and intimacy – to name a few characteristics of privacy – helps to foster the freedom and equality necessary for democratic politics, by structuring and limiting competition for power in ways that enable people to see and treat each other as equal despite incompatible beliefs, interests and identities (Lever 2016, 7).*

Of course, democracies vary in type and are often accused of illiberal and authoritarian practices when governing new technologies (Michaelsen & Glasius, 2018). However, the continuing response and public discussion around privacy in state–society interactions define the resilience of democratic practices and values, as Loh (2019) succinctly states, "For their own sake, democracies need to protect the informational privacy of its citizens, in some instances, even against their inclinations and impulses to abundantly share information online."

Indeed, the major threats to privacy, such as surveillance, the violation of freedom of speech, and the disclosure of personal data, etc., are all unrestrictedly practiced by authoritarian regimes, and the lowest-ranking countries in digital rights indices are all ruled by illiberal governments (Freedom House 2019a, 2019b; Garside 2020).

3.3. Communist Legacy

Another important variable to be considered is history. The early Communist project of the Soviet Union imagined a utopian communal lifestyle, elevating "the collective, giving it moral and historical primacy over the individual" (Klepikova, 2015, p. 357). Behind this "privatelessness" (Klepikova, 2015, p. 353) was a "complicated economic and demographic situation in the cities and the Soviet state's ideologically saturated housing policy." Dense communal flats (so-called *kommunalka*) were a prevalent type of housing all over the Soviet Union, driven by the "condensation policy" and leaving no space for the privacy of their residents:

> *Control over one's own information was not in the hands of individuals in the overcrowded fiats: In the early Soviet Union instead of private possession of information collective possession arose. [...] The appropriation of information was facilitated by the architectural features of the kommunalka, namely*

> *the thinness of walls or partitions between the rooms, which increased one's exposure to the others. (Klepikova, 2015, p. 371)*

Moreover, by the 1930s, a "police state" based on an extensive network and culture of informants was consolidated: official policy endorsed "witch-hunts" of potential "enemies of the state" (*vrag naroda*) (Knight, 1988). There was limited private space even within families; for instance, the propagated story of a child-martyr, Pavlik Morozov, who denounced his father in favor of the Soviet state, was part of the elementary school curriculum (Encyclopaedia Britannica, 2020). The political "thaw" (*ottepel*) of the 1960s and Khrushchev's mass housing project, which manifested the idea "to every family its own apartment" (Attwood, 2010), allowed political dissent to take place in the kitchen (*na kukhne*) (NPR, 2014), a space that was considered a luxury for many families as it was previously common to share it with several other households. Nevertheless, amid the heyday of the Cold War, individual privacy remained limited and was discouraged under the continuing surveillance and secrecy policies of the centralized communist regime.

The collapse of the Soviet Union brought with it sudden freedoms that people had yet to embrace and internalize. In terms of privacy, the process was "traumatic and inspiring" being "the result of an unhindered, unlimited explosion of the previously shadow individual self" (Agadjanian, 2006, p. 175). Considering the collectivist cultures of Central Asia, which permit greater tolerance to intrusion into the private space than Western cultures, people in countries such as Kazakhstan and Kyrgyzstan were left alone to process and negotiate the new affordances and freedoms in the context of the historical past, their cultural identities, and political developments and amid accelerating technological developments.

4. Privacy in Kyrgyzstan: Scattered Policies, Limited Civil Expertise, and Societal Indifference

The political climate in Kyrgyzstan, a country habitually referred to in Central Asia as "the island of democracy" (Anderson, 1999), allows for anticipated state accountability, a vibrant civil society, and active public involvement in various policy issues. However, this has not necessarily contributed to the formation of a firm value of privacy among its citizens nor prevented privacy infringement by the state. Being complicated and highly interdisciplinary, the question of privacy has been scattered across diverse policies and state bodies and hindered by limited civil expertise and societal indifference to the issue. Considered as being of rather secondary importance (if at all), privacy and its regulation in contemporary Kyrgyzstan embody the inherent risks that could be exposed at any future moment.

4.1. The State

At the avant-garde of the development of the ICT sector in the region, Kyrgyzstan adopted the first related national strategy, "Information and Communication Technologies (ICT) for Development in the Kyrgyz Republic for 2002–2010," in March 2002 (National Institute for Strategic Studies of the Kyrgyz Republic, State Committee of Information Technologies and Communications of the Kyrgyz

Republic, & The World Bank, 2017). However, state efforts in ICT were then delayed by the country's political turbulence in 2005 and 2010, which transformed the state from an authoritarian to a relatively democratic political regime. Despite Kyrgyzstan's commitment to the ICT sphere being relatively recent, policy decisions regarding the country's digitalization are mass scale and have been already acknowledged at the international level. Owing to the state-owned inter-agency interoperability system "Tunduk," Kyrgyzstan was foreseen to reach the list of the top "countries [in] the development of e-gov systems in the UN ranking" (Civil Initiative on Internet Policy, 2019). Having declared both 2019 and 2020 as "years of digitalization," state leadership identified numerous and broad policy priorities in digital development, including e-governance, shared databases, cybersecurity, e-tourism, developing e-content, and equipping citizens with digital skills (see, for instance, Digital Kyrgyzstan 2019-2023). At the same time, the country is among only two in the region (along with Kazakhstan) to have adopted privacy legislation as early as 2008. However, despite the political will, policy, and legal advances in the ICT sector, the current research argues that the value of privacy is missing on the country's policy radar, resulting in its misapprehension and potential infringements by various agencies.

The confusion and overlap of national strategies, concept notes, and programs to develop the country's digital domains have contributed to the overall dispersion of the focus on privacy. The absence of a unified, lineal policy towards digitalization builds upon the peculiarities of political decision-making in the state, where policies are a product of individual political will. The endurance of such initiatives could potentially be further challenged by changes of those in power. One of the "grandiose" (Yusupova, 2020) initiatives for the country's digitalization, the national project "Taza Koom," came to life in 2017 under the administration of former president Almazbek Atambayev and with the personal involvement of then prime-minister, Sapar Isakov, who has been called the project's "locomotive" (Yusupova, 2020) and "champion" (KYR_4, 2019). After the change of political cadres and Isakov's controversial imprisonment for alleged corruption offenses in 2018, the project initially slowed; however, it was then transformed into the concept of "Digital Kyrgyzstan," thus changing its "signboard" and distancing itself from its forerunner (KYR_4, 2019). In this regard, the lack of continuity among digitalization policies may foster disruptions to major advances in the expertise and progress achieved by the preceding efforts.

Despite the country's legislative advances in the protection of privacy and personal data, there are major pitfalls in its oversight of the implementation of these legal provisions. Law No. 58, "On information of a personal nature," dated April 14, 2008, provides for the establishment of an authorized body to ensure the state's responsibility for regulating compliance with the law (Art. 13). The creation of this agency was lobbied for by civil society, including through court petitions throughout the 2010s, and though it has been already confirmed at the highest political levels, it has not yet been established (KYR_1, 2019). Though this has been rationalized by a lack of budget and the resistance to the expansion of state bodies (KYR_2, 2019), the state may, in fact, be reluctant to create such an authority considering the record of violations committed by different government agencies. For instance, a major scandal erupted around the collection and storage of biometric data in 2015 and was associated with the manipulation and fraud seen during the country's subsequent elections. In this case, the biometric information was not qualified as personal, and the state was

declared as its owner (KYR_1, 2019); however, the rapid introduction of biometric data collection and the state's lack of preparedness to protect it, resulted in the absurd cases of alleged lost flash drives containing citizens' biometric data (Kozhobayeva, 2017). The amendments to the Law "On the registration of the biometric data of citizens of the Kyrgyz Republic" improved the state's compliance with international standards by qualifying the biometric data as personal; however, given the absence of an enforcement authority and with several state bodies taking responsibility for the implementation of different aspects of the digitalization strategy, the risk of privacy infringement is high.

Finally, the vivid absenteeism of privacy as a value in state discourses led to a lack of understanding of its necessity from the beginning. Often referred to as "confidentiality" in policy documents, the concept has been neither elaborated on, nor strategized over, but has rather received only honorary mentions (Ministry of Digital Development of the Kyrgyz Republic, n.d.). The "nothing to hide" rhetoric is still largely prevalent among state agencies: the presumed ownership of citizens' data by the state, from one side, and the paradoxical negligence towards it, from another, have been inherited in the context of the Soviet past (KYR_4, 2019). Moreover, considering the clear linkage of digitalization with modernization and progress in state discourses, privacy is often seen as an obstacle to the unfolding digital development. When asked about privacy concerns amid the advances in digitalization, one of the state representatives noted:

> *We have the presumption of virtue. All people are good, the state is good, so we should not protect but give opportunities. Active connections are in progress. As for protection, let the architecture be built first, [and when] real threats arise, the construction of such a safeguarding system will begin. (KYR_6, 2019)*

This participant also argued against the development of privacy policy in the country, seeing it as a potential obstacle to the buildout of its planned ICT infrastructure. While providing the illustrative analogy of a house (digitalization) and a fence (privacy), the respondent explained the incommodity of building a fence without having a house in the first place (KYR_6, 2019). Further, despite acknowledging the importance of privacy in international discourses, another high-ranking official questioned its value for citizens in Kyrgyzstan, framing privacy as foreign to Kyrgyz culture (KYR_7, 2019)

The problematic perception of privacy as a value is exacerbated by its complexity. As an interdisciplinary issue that straddles various fields from human rights to technology, the concept requires basic education and awareness among information holders about rules and protocols. According to one of the respondents who provided training for government agencies on the technical basics of cybercrime, the supervision of access to personal data, and digital security, "most leaks happen due to negligence, people's ignorance, and a lack of expertise" (KYR_3, 2019). Whereas the discourse on the protection of personal data among state officials has often been lively due to the active involvement of civil society, the concept of privacy in a more general sense seems to have been abandoned and rarely makes it into the policy agenda.

4.2. Civil Society

Among the various stakeholders, civil society had most widely embraced the most up-to-date expertise and legal and technological skills when it came to privacy rights. The pioneers of digitalization, the Civil Initiative on Internet Policy (CIIP), addressed a variety of policy-related issues, from e-governance to cybersecurity. The CIIP was among the whistleblowers during the previous major cases of privacy infringement, including the abovementioned collection of biometric data. The organization also supported the lobby for an authorized body to oversee compliance with the law on personal data (KYR_1).

While standing among the avant-garde of civic activism in the digital domain, the CIIP acknowledges its limitations and constraints in the privacy field. Recognizing the issue as important, the CIIP has nevertheless been focusing on the question of data protection in a narrower sense than far-reaching privacy:

> *Privacy is a more comprehensive thing that includes many aspects: the right to private life and numerous other rights, as well as the protection of the data that is at someone's disposal …. We have not yet begun to develop this topic from the point of view of privacy. We concentrate on data protection since we at least need to develop the understanding of this matter. (KYR_2, 2019)*

The organization also provided education modules to state officials engaged in the sphere of digitalization; however, the participants of these modules were limited mostly to the high-level echelon that is predominantly concentrated in the capital. While positively setting discourses through key executives, the training excluded everyday operators of data and information, who may unintentionally disregard public privacy. Contemplating the state's considerable digitalization ambitions, with more and more agencies joining the process, the efforts of a single NGO amid the knowledge vacuum of the vast majority of bureaucrats raises questions about the quality of services provided over their quantity.

The aforementioned complexity and interdisciplinarity of online privacy require comprehensive expertise embracing various, often highly differentiated, disciplinary angles. The human rights lawyers and activists who raise concerns over the infringement of the right to privacy in the offline domain, face challenges in their expertise when dealing with digital spheres (KYR_2). Meanwhile, the relatively recently introduced international standards, such as the GDPR, are demanding and multifaceted and still focus on Europe-specific peculiarities, and a relatively low public concern for the issue, may potentially distract the focus of civil society away from privacy rights.

4.3. Citizens

During our fieldwork, the responsibility for privacy was often observed to be assigned to its primary stakeholders—citizens—both by the state and civil society alike. The topic was even described as complex and foreign to the population and as "rocket science" (KYR_2, 2019). This can be explained by the Soviet legacy and culture of collectivism, the lack of education and awareness campaigns after independence, the references that have been made to the existential value of privacy, and its applicability in the local context. Two extremes were pronounced in the expert interviews: "As a

rule, there are two opposing rhetorics: either paranoia to the point of absurdity … or those who have nothing to hide" (KYR_3, 2019). The prevalent majority among the population was described by the respondents as belonging to the second group. The active groups among citizens, aware and concerned about their privacy according to the experts, remain limited and predominantly located in Bishkek and its vicinity.

The FGD with citizens in Bishkek revealed more nuanced fluctuations in their readings of privacy: the majority of the participants had at least a basic understanding of privacy as seclusion from others and freedom from interference. When asked to provide a graphical representation of their associations of privacy, some focus group participants (representing various ages, ethnicities, and genders) resourcefully delivered a wide range of visuals of the private and personal space, such as shields, curtains, passwords, or stop signs. Others struggled with the drawings and preferred to explain the phenomenon with textual descriptions, framing privacy as anonymity, inviolability, or something "personal, individual, with regards to only oneself." One elderly participant found the term foreign and unclear and preferred to abstain from giving any description.

When deciding what and who to share their private information with, the participants demonstrated unified, rather than contested, views and opinions. They entrusted a vast majority of their information to the state; while acknowledging the already immense penetration of the state into the personal space, the participants did not foresee risks of such penetration and were not ready to actively protest against it. A more active civic engagement, however, was exposed in response to the idea of privacy being potentially infringed by other citizens, rather than the state. The participants agreed that online bullying and exposure by fellow citizens constitute "an obvious violation" of privacy, for example, "when being filmed without permission." All the participants agreed that such visibility could harm a person and bring them "stigma for their whole life." On several occasions, the participants identified privacy through gendered perspectives; for instance, when asked about who has access to their personal mobile phones, female participants shared how their devices were a family commodity, with children and other family members using them unrestrictedly, whereas male respondents perceived their phones as rather personal gadgets.

There were several trigger points for privacy concerns to be raised or debated. First, the potential exposure of one's close or extended network was discussed with careful consideration of the associated risks and consequences. The participants were unwilling to share their contact lists or pictures of their family members, while publishing similar content of themselves was not seen as a problem. One of our expert interviewees, for example, mentioned that the argument for the protection of family and close contacts is often "successfully" used to explain the value of privacy to the population:

> *We tried to persuade the population that their accounts can be used to attack others. Thus, we are trying to indirectly motivate [citizens] to protect their private belongings …. "Think, first, who is in your phonebook."* (KYR_3, 2019)

Considering the importance of formal and informal networks in the everyday lives of Central Asians (Schatz, 2005), including but not limited to patronage and nepotism, such concerns seem feasible in the sensitivity they triggered.

4.4. Discussion

As has been shown, there are several challenges for different stakeholders in Kyrgyzstan that prevent privacy from becoming a priority in the country's digitalization process. This process is fragmented, and there is an overlap and confusion in related state policies and concepts. When state policies arise as individual initiatives, they could potentially be compromised by continuous political turbulence and changes of cadres. The absence of an authorized body that can ensure the protection of privacy by state officials, undermines the enforcement of existing legislation. When it comes to civil society, despite being vibrant and active, there are only a few organizations that deal with digitalization policies and the concept of privacy. Their resources are limited, and the comprehension of such an enigmatic concept as information privacy in the digital domain requires multidisciplinary expertise. The main stakeholders of personal data and privacy, citizens, showed limited or no understanding of privacy issues. While there were sensitive concerns and taboo topics that influenced their appreciation of personal privacy, such as the privacy of family members, their overall tendency demonstrated their lack of readiness to protect their privacy and lack of knowledge about the risks associated with its infringement. Considering that the FGD was limited to Bishkek residents only, citizens beyond the capital might be even less informed about the concept and their own rights.

While one should be conscious about drawing causal conclusions, all three factors discussed in Section 3—cultural roots, political regimes, and the Soviet past—were mentioned as important for the formation of the value of privacy by different stakeholders. Thus, during the discussion, FGD participants alienated privacy as a foreign concept and demonstrated how privacy was gendered, with male and female participants tolerating different levels of intrusion into their personal space. Similarly, state officials expressed existential concerns about the necessity of privacy for Kyrgyz people and questioned its cultural value.

Moreover, there was an obvious Soviet legacy in the Kyrgyz state officials' interpretations of privacy, which favored a "nothing to hide" rhetoric and even a view of privacy as a potential obstacle to the development of essential digital infrastructure. The eldest FGD participants, who had almost inevitably been exposed to Soviet politics and ideology, had the most difficulties in describing privacy and understanding it as a right. Civil society representatives and the experts who participated in the research also expressed their concerns that the culture of collectivism and Soviet legacy could have contributed to the neglect of privacy both by the state and citizens.

Finally, when combined, the perceptions, attitudes, and practices of the different state, civil society, and citizen stakeholders may signal the fundamental jeopardies of democratic developments in the country. As argued above, privacy lies at the core of democratic political regimes, which should (ideally) embrace the concept as essential for the participation and dignity of free and equal citizens, even through their own limitations of power. The vacuum of policies that occurred after the collapse of the USSR, the state's commitment deficit in ensuring the legal protection of personal information, data leaks, and the manipulation of elections through citizens' biometric data could potentially indicate the utmost instability of democracy-building in Kyrgyzstan

and, from a different perspective, explain noticeable fluctuations in the country's democracy rankings.

5. Kazakhstan: Authoritarian Bargaining

Kazakhstan is a consolidated authoritarian state, which has benefited from its abundant oil and gas reserves since its independence (Bohr et al., 2019; Hale, 2014; B. Junisbai 2010; McGlinchey 2011). The country's civil society has been systematically weakened through legislative and administrative measures (Knox & Yessimova, 2015; Human Rights Watch 2019). As will be shown in this section, the state has taken a paternalistic approach to regulating the privacy of its citizens; however, even in an authoritarian setting with strict top-down regulation, there is space for privacy policies to be negotiated and bargained by the major stakeholders, that is, state institutions, civil society, and citizens.

5.1. The State

Kazakhstan's strategy toward digitalization has been driven by a mix of modernization and securitization forces, with the Ministry of Digital Development and the National Security Committee jointly responsible for the country's digitalization processes. Since the early 2000s, the country has begun to position itself as a major ICT power in the region and a regional leader in e-government development (Astana Times, 2019). Kazakhstan is ranked among countries with a "very high E-Participation Index level" by the UN E-Government Survey (United Nations, 2020, p. 119). Moreover, some scholars have argued not only that "informatization has always been associated by policymakers and practitioners in Kazakhstan, with the ongoing progress in building national economic competitiveness" (Kassen, 2019, p. 307) but also, perhaps, more importantly, that digitalization has symbolic importance for the legitimacy of the regime (Maerz, 2016). Indeed, the regime's legitimacy—and maybe even the national idea itself—has been based on a forward-looking promise of modernization (Akulov, 2019), of which informatization is one of the major pillars.

Nevertheless, the protection of privacy and cybersecurity concerns has only recently become a part of the policy agenda according to one of the study's participating officials:

> *Everyone is in the euphoria of digitalization. It makes everything more transparent and faster. [...] For a long time, our KPIs [key performance indicators] have been [focused on] the introduction of the maximum number of services for the maximum number of people. Cybersecurity issues are slowing digitalization processes, so they have been postponed. (KAZ_7)*

Another interviewed expert confirmed this view:

> *The goal is to digitize [everything], but little attention has been paid to safety. Take EGOV.com [e-government platform]. It lacks a security certificate. ... This is just not a priority. Currently, they [the government] are trying to reach wider, not deeper. (KAZ_1)*

Kazakhstan was among the first in the region to adopt data privacy legislation (the Law "On Personal Data and Its Protection"), with the digital sphere itself being highly securitized. The state

has extensive control over the Internet and telecommunications, steadily expanding its legal and technical infrastructure to enable mass communication surveillance.

In 2004, the Rules Providing for Mechanisms for Monitoring the Telecommunications Operators and Networks were approved, introducing a legal basis for using the System for Operative-Investigative Activities (SORM). This Russian-developed technical framework allows security agencies to monitor the activities of users, including the targeted surveillance of both telephone and Internet communications (OpenNet Initiative, n.d.). Furthermore, control over activities in the field of communication and information was transferred to the National Security Committee (KNB) in 2017, including the introduction of a centralized management of telecommunications networks (Kapital.kz, 2017). According to the Freedom on the Net report, Kazakhstan is among countries that cooperated with China on the development of the surveillance infrastructure, including intelligent monitoring systems and facial recognition technology (Shahbaz, 2018). In July 2019 and December 2020, mobile users in Kazakhstan received a request to install a "national security certificate" to continue to have uninterrupted access to the Internet. The root certificate, which was developed by the KNB, allowed the state to intercept and monitor users' encrypted connections, essentially launching a "man in the middle" attack on its residents (OCCRP, 2019). The requirement was withdrawn shortly thereafter following resistance from civil society and businesses, and the president consequently stated that the certificate may be used in the future in the case of "a threat to national security" (Kim, 2019).

Since 2017, the KNB has overseen digitalization processes, sharing control of the communication sphere with the Ministry of Digital Development. The contradiction between the two agencies' priorities creates a space for them to bargain about policies; the Ministry sees digitalization as a modernization process that requires compliance with international standards for data protection, while the KNB is more interested in securitizing the digitalization processes and pushing for further control and surveillance. Moreover, during an interview, one high-profile representative of the Ministry of Digital Development noted that the Ministry meets resistance from other agencies when trying to promote digitalization:

> *The state is often seen as a monolith, but each body has its own priorities, its own indicators that it is trying to reach. Our ministry is in such a position that all other ministries want us not to interfere with them. (KAZ_5)*

For example, according to this interviewee, the creation of an independent agency to promote the protection of personal data is facing resistance from the Ministry of Economy since such an agency contradicts its priorities of reducing the number of regulatory bodies and limiting the growth of the state apparatus.

Nevertheless, it was apparent from the interviews with state representatives that the Kazakh government has a very clear and current understanding of the policy issues surrounding privacy, in terms of both international legal standards and technical aspects. However, this understanding does not necessarily convert into measures to protect the privacy of its residents.

5.2. Civil Society

Another important stakeholder in Kazakhstan's policy formation process is its civil society, which has been systematically weakened and oppressed (CIVICUS, 2020). During the interviews, Kazakh civil society representatives acknowledged that they had little influence on the decision-making processes and little understanding of how policies are formed (KAZ_7) due to the excessive securitization of the digital domain (KAZ_1). However, interestingly, civil society sometimes finds itself involved in the state inter-agency competition as it is instrumentalized for the legitimation of policy decisions. As described by the representative of the Ministry of Digital Development: "The ministry needs citizens and civil society to be on its side so we can justify our initiatives when meeting resistance from other ministries" (KAZ_5).

Moreover, given the relative novelty of the digital challenges in its agenda, Kazakh civil society has limited expertise in digital technologies and the related social and political processes. Currently, the civil society experts working on this issue are represented mostly by human rights lawyers who have previously worked on freedom of speech or other adjacent offline rights.

One of the major civil society actors is an unusual suspect. The Center for Analysis and Investigation of Cyber Attacks (CARCA) is a curious case of a business turning to activism. CARCA is a company that develops cybersecurity solutions and became quite famous on social media for investigating vulnerabilities in government services and making them public. The company's dependence on government procurement contracts and the necessity to promote more government spending for the provision of cybersecurity services, were the key motivations for CARCA to become a major civil society force, as the head of the company explained:

> *We are on a train, and if we want it to move, we have to get off and push it. As a business, it is not natural for us to engage in activism, but we have to get involved in promoting the importance of cybersecurity for our business interests. As soon as we stop stimulating the state, it stops working [in this direction]. 80% [of our income] is government commissions, so we have to deal with this. (KAZ_7)*

5.3. Citizens

In 2019 alone, Kazakhstan saw several large data breaches, including a leak of the Central Election Commission's database of the personal data of 11 million Kazakhstanis (the entire adult population of the country) during the presidential elections; a leak of medical data from the state medical information system DamuMed; and data leaks from the information system of the General Prosecutor's Office, containing data of all citizens and foreigners for whom administrative proceedings have ever been conducted (Gussarova & Dzhaksylykov, 2020). However, these incidents attracted little attention from the public.

In addition to our limited field research, previous studies have shown that Kazakhstan's citizens show an interesting mix of suspicion towards the state and fatalism. On the one hand, people believe that they are under increasing control and surveillance, balancing on the edge of conspiracy theories (Gussarova & Dzhaksylykov, 2020). Our focus group participants were especially aware and alarmed by the government's excessive penetration into the personal space. However, when asked

what data they would share with which stakeholders, they stated that they would agree to share almost all types of personal data with the state explaining that "we are under control anyway." One respondent expressed a conviction that the data they share through the Internet "has long ceased to be personal, even if it is [legally] personal and you might want it to stay personal." A lot of distrust was expressed by focus group participants in connection to the perceived widespread corruption of government structures and the possible use of their personal data in falsified criminal cases or data that could be sold on the black market.

At the same time, we observed their unwillingness to resist the perceived expanding state surveillance. As one of our respondents said, "Soon we will not have personal space at all, but we do not try to prevent it." Some of the focus group participants were aware of the large data leaks, although most agreed that nothing could be done about it: "No one is asking for our opinion." Along these lines, the majority of the users did not take proactive measures to protect their data: they used weak passwords or the same passwords for multiple accounts, rarely updated them, and shared passwords with their family members and colleagues.

Attempts to understand the reasoning behind this mix of alarm and an unwillingness to take protective measures should take into account both the universal struggles of technology users with the rapid development of technologies and the confusing and often unfeasible nature of digital safety rules (Acquisti & Grossklags, 2004; Barth & Jong, 2017; McDonald & Cranor, 2008), as well as local context, which features a lack of democratic mechanisms and specific historical legacies. Indeed, that the heritage and practices of the Soviet surveillance state are largely preserved was often mentioned by both the experts and individual users of digital technologies in the FGDs. One participant noted:

> *The culture of "personal life" was not formed initially when we gained independence. We have been accustomed [since Soviet times] to the fact that the state decides everything for us, protects us, takes care of us. We don't even think that we have to secure our data on our own.*

Another often mentioned opinion was that the collectivist nature of Kazakh society influences people's behavior on the Internet: "It is our mentality. We allow everyone into our personal space. You will be judged if you ask for privacy."

5.4. Discussion

We have seen that our participants often referred to factors that can be broadly categorized as those relating to culture, political regimes, and the Soviet legacy when trying to explain the situation and perceptions of privacy by various actors in Kazakhstan. However, taking into account the limited sample and the conceptual broadness of those factors, we refrain from making causal links here and, instead, sketch some directions of further exploration.

We found that despite the relatively high qualifications and awareness of the staff, as well as the resourcefulness of Kazakhstan's state bodies, the motives behind policies for increased data security are rather technocratic and more concerned with state security and the use of modernization as a regime legitimization tool, rather than driven by concerns about the protection of citizens' privacy

and rights. Reflecting on the premise discussed in the literature that privacy is essential to democracy, the case of Kazakhstan reveals how the regime has recognized and taken the importance of privacy "seriously" by implementing proactive measures to comprehensively limit it, from promoting a paternalistic and modernizing discourse to adopting state-of-the-art surveillance technologies, investing in the qualification and capacity of its apparatus, introducing invasive legislation, and monopolizing and centralizing communication infrastructure in the country. The paternalistic narratives of the state were distinctively reflected in the perceptions of privacy held by the FGD participants, who acknowledged the population's inability/unwillingness to push back against the invasive state that "decides everything for us, protects us, takes care of us." Consequently, we found that citizens did not greatly trust the state and demonstrated alienation, bordering on fatalism, when it came to protecting their own privacy, on which the limited and suppressed civil society was unable to have a major influence.

As can be seen, the value of privacy is comprehended by the Kazakhstan regime, which embraces it as a tool of control. However, it would be wrong to see the authoritarian state as a monolith, since our field study revealed a dynamic process of the formation of privacy policies. There is space for negotiation and bargaining even in this authoritarian setting, where various actors influence the formation of the two seemingly conflicting policy processes taking place in Kazakhstan: the development and introduction of advanced surveillance technologies and the simultaneous efforts to push for data security in the digital domain.

6. Conclusion

This study attempted to widen the geographical scope of privacy studies, introducing the often-overlooked context of Central Asia. While not embarking on deconstructing privacy as a concept, the current research aspires to enrich our understanding of this concept and introduce new evidence on how the value of privacy is formed beyond the West.

The studied two Central Asian countries represent an illustration of how privacy can be scrutinized at policy levels in dissimilar political and economic contexts. Whereas Kazakhstan took the path of securitizing the digital sphere in its authoritarian agenda, and the more democratic Kyrgyzstan has been mostly neglecting privacy issues in its pursuit of fast modernization, the result is strikingly similar in both cases: the risks of privacy infringement remain high in both states, and an acknowledgment of the value of privacy is rarely found among the general population.

The study's focus groups demonstrated differences between citizens of the two states in their appreciation of the value of privacy and comprehension of the risks associated with privacy infringements. In Kazakhstan, the participants were more alert and anticipated potential dangers posed by the state; however, they manifested fatalism in confronting the government and standing up for their rights. Contrastingly, despite being politically vocal, Kyrgyzstani citizens in the FDGs did not foresee threats, nor did they fear intrusion into their privacy, and they were prepared to entrust the state with most of their personal data. Such attitudes and perceptions originate not only

from cultural and historical preconditions but also from the divergent political contexts and policy trajectories in the two countries.

In Kazakhstan, the state's consolidated understanding can be traced through official documents, narratives, and decisions on digitalization. However, the notion of privacy is interpreted predominantly in terms of the necessity to protect the country and its citizens from external threats, in effect distracting attention from the state itself and occasionally infringing the privacy of its subjects. On the other hand, in Kyrgyzstan, the dispersion of policies towards digitalization, which has resulted from the country's political turbulence and changes of political cadres, has generally prevented privacy from becoming a policy focus, leaving it marginalized on the official agenda. State officials do not necessarily endorse the value of privacy and may even see it as an obstacle to the rapid modernization of the country. Remarkably, as demonstrated, privacy can be recognized (although misused) in an authoritarian setting, while it may also not be formed at all in a more democratic climate, problematizing the presumption that the value of privacy is innate to democracy. It rather requires a more proactive approach and initiative when filling a conceptual void.

The study's data collection had certain limitations that should be noted. The focus groups were only conducted in the major cities due to limited resources and to ensure comparability between the two countries. Since there is a considerable urban-rural divide in both Kazakhstan and Kyrgyzstan (The World Bank, 2018; Nikolova, 2020; Thelwell, 2020), this study's focus on major cities means its results might not be representative of the whole population. According to one of the interviewed experts, the most active population and civil society alike is concentrated predominantly in capitals (KYR_2, 2019), therefore, the collected data might represent a more informed part of society.

Moreover, both FGDs were conducted in the Russian language. This decision was made due to limited resources and, as we discussed particular concepts, such as the perception of the word "privacy" (*privatnost*) and other linguistic peculiarities, to ensure better comparability in the results between participants from Kazakhstan and Kyrgyzstan. Hence, this limited sample might have skewed the results due to the possible greater exposure of the Russian speakers to discourses available in the Russian language. Considering both of these limitations, further research is needed to depict the perceptions of all possible groups among the two countries' populations.

Further, although the private sector was beyond the scope of this paper, exploring the dynamic between industry and individual privacy can be a fruitful avenue for future scholarly endeavors. Some of the occasional insights of our field study revealed, interestingly, that private companies in Central Asia were pushing the policy agenda in line with the international privacy standards, in order to remain competitive in international markets or to gain credibility for their international clients. Moreover, as the fieldwork was conducted prior to the outbreak of COVID-19, the impact of the pandemic was not reflected in the present analysis. However, the important developments that took place in the region in the context of this crisis may reveal important contributions in further research. Relevant both globally and in Central Asia, the pandemic has been used as a pretext for various violations of privacy (Csaky, 2021), including the right to privacy (Imanaliyeva, 2020; OHCHR, 2020; Privacy International, 2020; Putz, 2020). While there have been various attempts to

reflect the unfolding developments, further research might help to scrutinize the transformations in perceptions, values, and norms of privacy.

References

Abazov, R. (2008). Nation-State Delimitation in Central Asia, 1924–1926. In R. Abazov (Ed.), *The Palgrave Concise Historical Atlas of Central Asia* (pp. 82-83). New York: Palgrave Macmillan. https://doi.org/10.1057/9780230610903_37

Acquisti, A., & Grossklags, J. (2004). Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting. In L. J. Camp & S. Lewis (Eds.), *Economics of Information Security* (pp. 165-178). Boston, MA: Springer. https://doi.org/10.1007/1-4020-8090-5_13

Agadjanian, A. (2006). *The Search for Privacy and the Return of a Grand Narrative: Religion in Post-Communist Society*. Social Compass, 53(2), 169-184. https://doi.org/10.1177/0037768606064318

Akulov, M. (2019). Eternal Futurostan: Myths, Fantasies and the Making of Astana in Post-Soviet Kazakhstan. In R. Isaacs R & A. Frigerio (Eds.), *Theorizing Central Asian Politics: The State, Ideology and Power* (pp. 189-210). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-97355-5_9

Ambay III, M. A. V., & Gauchan, N., & Hasanah, M., & Jaiwong, N. K. (2019). *Dystopia is Now: Digital Authoritarianism and Human Rights in Asia*. Global Campus Human Rights Journal, 3, 269-285. https://doi.org/20.500.11825/1575

Anderson, J. (1999), *Kyrgyzstan: Central Asia' s Island of Democracy*? The Netherlands: Harwood Academic Publishers.

Arora, P. (2019). *Decolonizing Privacy Studies*. Television & New Media, 20(4), 366–378. https://doi.org/10.1177/1527476418806092

Astana Times. (2019). Kazakhstan's digitisation is improving lives, businesses. Retrieved November 20, 2020, from https://astanatimes.com/2019/10/kazakhstans-digitisation-is-improving-lives-businesses/

Attwood, L. (2010). The Khrushchev Era: "To Every Family its Own Apartment." In L. Attwood & P. Sharpe (Eds.), Gender and Housing in Soviet Russia (pp. 154-173). Manchester, UK: Manchester University Press. https://doi.org/10.7228/manchester/9780719081453.003.0010

BankWatch. Kumtor Gold Mine, Kyrgyzstan. Retrieved December 13, 2020, from https://bankwatch.org/project/kumtor-gold-mine-kyrgyzstan

Barth, S., & De Jong, M. D. (2017). *The Privacy Paradox: Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior–A Systematic Literature Review*. Telematics and Informatics, 34(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Bohr, A., & Brauer, B., & Gould-Davies, N., & Kassenova, N., & Lillis, J., & Mallinson, K., & Nixey J., & Satpayev D. (2019). Kazakhstan: Tested by Transition. Chatham House Report. The Royal Institute of International Affairs. Retrieved December 10, 2020, from https://www.chathamhouse.org/sites/default/files/2019-11-27-Kazakhstan-Tested-By-Transition.pdf

Bole, D., & Šmid, H. M., & Pipan, P. (2017). *Participatory Research in Community Development: A Case Study of Creating Cultural Tourism Products*. AUC Geographica, 52(2), 164-175. https://doi.org/10.14712/23361980.2017.13

Boym, S. (1994). *Common Places: Mythologies of Everyday Life in Russia*. Cambridge: Harvard University Press.

Brower, D. (2003). *Turkestan and the Fate of the Russian Empire*. Abingdon, UK: Routledge.

CIVICUS. (2020). Live Rating: Kazakhstan. Retrieved November 20, 2020, from https://monitor.civicus.org/country/kazakhstan

Civil Initiative on Internet Policy. (2019). Kyrgyzstan has every chance to break into TOP 10 countries on the development of e-gov systems in the UN ranking. Retrieved April 10, 2021, from https://internetpolicy.kg/en/2019/04/14/kyrgyzstan-has-every-chance-to-break-into-the-top-10-countries-on-the-development-of-e-gov-systems-in-the-un-ranking/

Csaky, Z. (2021). Nations in Transit 2021: The Antidemocratic Turn. Freedom House. Report. Retrieved May 14, 2021, from https://freedomhouse.org/report/nations-transit/2021/antidemocratic-turn

Cummings, S. N., & Nørgaard, O. (2004). *Conceptualising State Capacity: Comparing Kazakhstan and Kyrgyzstan*. Political Studies, 52(4), 685-708. https://doi.org/10.1111/j.1467-9248.2004.00503.x

De George, R. T. (2003). *The Ethics of Information Technology and Business*. Malden, MA: Blackwell.

Diamond, L. (2019). The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism. Journal of Democracy, 30(1), 20-24. https://doi:10.1353/jod.2019.0001

Encyclopaedia Britannica. (2020). Pavlik Morozov: Russian communist youth. Retrieved April 10, 2021, from https://www.britannica.com/biography/Pavlik-Morozov

Freedom House. (2019a). Freedom on the Net: Kazakhstan. Retrieved December 8, 2020, from https://freedomhouse.org/country/kazakhstan/freedom-net/2019.

Freedom House. (2019b) Freedom on the Net: Kyrgyzstan. Retrieved December 8, 2020, from https://freedomhouse.org/country/kyrgyzstan/freedom-net/2019.

Furstenberg, S. (2017). *Applying Global Governance Agenda in Post-Soviet States: The Case of EITI in Kazakhstan and Kyrgyzstan* [PhD thesis, Universität Bremen]. Universität Bremen Repository. http://nbn-resolving.de/urn:nbn:de:gbv:46-00106001-18

Garside, S. (2020). Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom. EU Diplomacy Paper 01. Retrieved May 15, 2021, from http://aei.pitt.edu/102381/1/edp_1%2D2020_garside.pdf

Gussarova, A., & Dzhaksylykov, S. (2020). Protection Of Personal Data In Kazakhstan: Status, Risks And Opportunities [Защита персональных данных в казахстане: статус, риски и возможности]. Soros Foundation Kazakhstan. Retrieved November 20, 2020, from https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf

Hale, H. E. (2014). *Patronal Politics: Eurasian Regime Dynamics in Comparative Perspective*. New York: Cambridge University Press. https://doi.org/10.1017/CBO9781139683524

Human Rights Watch. (2019). World Report 2019: Kazakhstan. https://www.hrw.org/world-report/2019/country-chapters/kazakhstan

Imanaliyeva, A. (2020, May 8). Kyrgyzstan's coronavirus tracking app alarms privacy advocates. Eurasianet. Retrieved May 14, 2021, from https://eurasianet.org/kyrgyzstans-coronavirus-tracking-app-alarms-privacy-advocates

Junisbai, B. (2010). *A Tale of Two Kazakhstans: Sources of Political Cleavage and Conflict in the Post-Soviet Period*. Europe-Asia Studies, 62(2), 235-269. https://doi.org/10.1080/09668130903506813

Junisbai, B., & Junisbai, A. (2019). *Regime Type Versus Patronal Politics: A Comparison of "Ardent Democrats" in Kazakhstan and Kyrgyzstan*. Post-Soviet Affairs, 35(3), 240-257. https://doi.org/10.1080/1060586x.2019.1568144

Kapital.kz. (2017, 2 August). State Technical Services is transferred to the KNB [В ведение КНБ перешла Государственная техническая служба]. Retrieved May 14, 2021, from https://kapital.kz/gosudarstvo/61914/v-vedeniye-knb-pereshla-gosudarstvennaya-tekhnicheskaya-sluzhba.html

Kassen, M. (2019). *Building Digital State: Understanding Two Decades of Evolution in Kazakh e-Government Project*. Online Information Review, 43(2), 301–323. https://doi.org/10.1108/oir-03-2018-0100

Kim, S. (2019). President Tokayev: Testing of the Safety Certificate was Carried Out on My Behalf. Retrieved November 13, 2020, from https://factcheck.kz/dajdzhest/prezident-tokaev-testirovanie-sertifikata-bezopasnosti-provodilos-po-moemu-porucheniyu/

Klepikova, T. (2015). *Privacy as They Saw It: Private Spaces in the Soviet Union of the 1920–1930s in Foreign Travelogues*. Zeitschrift für Slavische Philologie, 71(2), 353–89.

Knight, A. W. (1988). *The KGB: Police and Politics in the Soviet Union* (1st ed.). Winchester, MA: Unwin Hyman.

Knox C., & Yessimova Sh. (2015). *State-Society Relations: NGOs in Kazakhstan*. Journal of Civil Society, 11 (3), 300-316.

Kozhobayeva, Z. (2017). Biometric Data Security Concerns [Обеспокоенность безопасностью биометрических данных]. *Radio Azattyk*. Retrieved November 13, 2020, from https://rus.azattyk.org/a/28945751.html.

Kumer, P., & Urbanc, M. (2020). Focus Groups as a Tool for Conducting Participatory Research: A Case Study of Small-Scale Forest Management in Slovenia. In J. Nared & D. Bole (Eds.), *Participatory Research and Planning in Practice* (pp. 207-220). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-28014-7_13

Law of the Republic of Kazakhstan "On Personal Data and Its Protection". (2013). No. 94-V. Retrieved November 20, 2020, from https://online.zakon.kz/document/?doc_id=31396226.

Lever, A. (2016). Democracy, Privacy and Security. In A. D. Moore (Ed.), *Privacy, Security, Accountability: Ethics, Law and Policy* (pp.105-124). London: Rowman & Littlefield Publishers.

Loh, W. (2019). Informational privacy: A precondition for democratic participation? Retrieved 20 May 2021, frohttps://blogs.lse.ac.uk/businessreview/2019/12/13/informational-privacy-a-precondition-for-democratic-participation/

Maerz, S. F. (2016). *The Electronic Face of Authoritarianism: E-Government as a Tool for Gaining Legitimacy in Competitive and Non-Competitive Regimes*. Government Information Quarterly, 33(4), 727–735. https://doi.org/10.1016/j.giq.2016.08.008

McDonald, A. M., & Cranor, L. F. (2008). *The Cost of Reading Privacy Policies*. I/S: A Journal of Law and Policy for the Information Society, 4(3), 543-568. http://hdl.handle.net/1811/72839

McGlinchey, E. (2011). *Chaos, Violence, Dynasty: Politics and Islam in Central Asia*. Pittsburgh, PA: University of Pittsburgh Press.

Melvin, N. J. (2004). Authoritarian Pathways in Central Asia: A Comparison of Kazakhstan, Kyrgyz Republic, and Uzbekistan. In Y. Ro'I (Ed.), *Democracy and Pluralism in Muslim Eurasia* (pp. 119-142). London: Frank Cass.

Merriam-Webster Dictionary. Democracy. Retrieved May 14, 2021, from https://www.merriam-webster.com/dictionary/democracy

Michaelsen, M., & Glasius, M. (2018). *Authoritarian Practices in the Digital Age: Introduction*. International Journal of Communication, 12, 3788–3794.

Ministry of Digital Development of the Kyrgyz Republic. N.d. Digital Kyrgyzstan 2019-2023. Retrieved April 10, 2021, from http://ict.gov.kg/index.php?r=site%2Fsanarip&cid=27

Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan. (2017). Digital Kazakhstan. Retrieved May 20, 2021, from https://digitalkz.kz/wp-content/uploads/2020/03/ЦК-рус.pdf

Ministry of Justice of the Kyrgyz Republic. (2008). Law of the Kyrgyz Republic "On Information of a Personal Manner." Retrieved September 23, 2020, from http://cbd.minjust.gov.kg/act/view/ru-ru/202269

Moore, Jr, B. (1984). *Privacy: Studies in Social and Cultural History* (3rd ed.). Routledge. https://doi.org/10.4324/9781315172071

National Institute for Strategic Studies of the Kyrgyz Republic, State Committee of Information Technologies and Communications of the Kyrgyz Republic, & The World Bank. (2017). Digital Development Assessment–Kyrgyzstan. Retrieved October 23, 2020, from http://www.ict.gov.kg/uploads/ckfinder/files/KG_Digital%20Development%20Assessment_Final.pdf

National Security Committee of the Republic of Kazakhstan and the Agency of the Republic of Kazakhstan for Informatization and Communication. (2004). Joint order "On Approval of the Rules for Interaction of State Bodies and Organizations in the Implementation and Operation of Hardware, Software and Technical Means for Conducting Operational-Search Measures on Telecommunication Networks of the Republic of Kazakhstan," No. 199. Retrieved November 20, 2020, from https://tengrinews.kz/zakon/komitet_natsionalnoy_bezopasnosti_respubliki_kazahstan/svyaz/id-V040003187_/

National Statistics Committee of the Kyrgyz Republic. (2020). Annual Demographic Report of the Kyrgyz Republic. Retrieved May 23, 2021, from http://www.stat.kg/ru/publications/demograficheskij-ezhegodnik-kyrgyzskoj-respubliki/

Nikolova, M. (2020, December 2). To reduce urban-rural divide, Central Asia must embrace freedom of movement. Emerging Europe. https://emerging-europe.com/news/to-reduce-urban-rural-divide-central-asia-needs-more-freedom-of-movement/

NPR. (2014). How Soviet kitchens became hotbeds of dissent and culture. Retrieved September 10, 2020, from https://www.npr.org/sections/thesalt/2014/05/27/314961287/how-soviet-kitchns-became-hotbeds-of-dissent-and-culture

OCCRP. (2019). Experts suspicious about Kazakhstan's security certificates. Retrieved December 9, 2020, from https://www.occrp.org/en/daily/10323-experts-suspicious-about-kazakhstan-s-security-certificates

OHCHR. (2020). Intrusive, omnipresent surveillance growing during COVID-19 pandemic, UN expert warns. Retrieved May 14, 2021, from: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26446&LangID=E

Omona, J. (2013). *Sampling in Qualitative Research: Improving the Quality of Research Outcomes in Higher Education*. Makerere Journal of Higher Education, 4(2), 169-185. https://doi.org/10.4314/majohe.v4i2.4

OpenNet Initiative (n.d.). Kazakhstan. Retrieved December 9, 2020, from https://opennet.net/research/profiles/kazakhstan

Patton, M.Q. (2002). *Qualitative Research and Evaluation Methods* (3rd ed.). Thousand Oaks, CA: SAGE.

Privacy International. (2020). Kazakhstan cities use mobile app to enforce quarantine. Retrieved May 14, 2021, from https://privacyinternational.org/examples/3628/kazakhstan-cities-use-mobile-app-enforce-quarantine

Putz, C. (2020). Technology and policing a pandemic in Central Asia. *The Diplomat*. Retrieved May 14, 2021, from https://thediplomat.com/2020/05/technology-and-policing-a-pandemic-in-central-asia/

Sabol, S. (1995). *The Creation of Soviet Central Asia: The 1924 National Delimitation*. Central Asian Survey, 14(2), 225-241. https://doi.org/10.1080/02634939508400901

Schatz, E. (2005). *Reconceptualizing Clans: Kinship Networks and Statehood in Kazakhstan*. Nationalities Papers, 33(2), 231-254. doi:10.1080/00905990500088594

Shahbaz, A. (2018). Freedom on the Net 2018: The Rise of Digital Authoritarianism. *Freedom House*. Retrieved November 20, 2020, from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Sharshenova, A. (2015). European Union democracy promotion in Central Asia: Implementation in Kazakhstan and Kyrgyzstan [PhD thesis]. University of Leeds.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Statistics Committee of the Ministry of National Economy of the Republic of Kazakhstan. (2020). Annual Demographic Report of Kazakhstan. Retrieved May 23, 2021, from https://stat.gov.kz/edition/publication/collection

Thelwell, K. (2020, September 18). Poverty in Kyrgyzstan. *The Borgen Project*. Retrieved May 14, 2021, from https://borgenproject.org/tag/poverty-in-kyrgyzstan/

The World Bank. (2018, April). A New Growth Model for Building a Secure Middle Class. Kazakhstan Systematic Country Diagnostic (No. 125611-KZ). https://documents1.worldbank.org/curated/en/664531525455037169/pdf/KAZ-SCD-April-2018-FINAL-eng-with-IDU-05012018.pdf

The World Bank. (n.d.). Kazakhstan Overview. Retrieved December 8, 2020, from https://www.worldbank.org/en/country/kazakhstan/overview

The World Bank. (n.d.). Kyrgyzstan Overview. Retrieved December 15, 2020, from https://www.worldbank.org/en/country/kyrgyzrepublic/overview.

Telecommunications Services of the Republic of Kazakhstan transferred to the KNB. (2017). Retrieved November 20, 2020, from https://total.kz/ru/news/vnutrennyaya_politika/v_upravlenie_knb_peredali_sluzhbu_telekommunikatsii_v_rk_date_2017_08_02_20_04_188

United Nations. (2020). UN E-Government Survey: Digital Government in the Decade of Action for Sustainable Development. (Retrieved November 20, 2020, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020 - Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

United Nations. (2018). UN e-governance knowledgebase. Retrieved May, 15, 2020, from https://publicadministration.un.org/egovkb/en-us/Data-Center

Van der Sloot & A. de Groot. (eds.). (2018). *Handbook of Privacy Studies*. Amsterdam University Press, Amsterdam.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

Wong, K. L. X., & Dobson, A. S. (2019). *We're Just Data: Exploring China's Social Credit System in Relation to Digital Platform Ratings Cultures in Westernised Democracies*. Global Media and China, 4(2), 220-232. https://doi.org/10.1177/2059436419856090.

Yusupova, D. (2018). Taza Koom a year later: What has already been done and what is still in development [Таза коом год спустя. Что уже сделано, а что пока в разработке]. Kaktus Media. Retrieved November 13, 2020, from https://kaktus.media/doc/373845_taza_koom_god_spystia._chto_yje_sdelano_a_chto_poka_v_razrabotke.html

Appendix 1. Country Profiles of Kazakhstan and Kyrgyzstan

	Kazakhstan	**Kyrgyzstan**
Population (national statistics)	18,631,779	6,389,500
Income (WB)	Upper middle income	Lower middle income

Gross national income (GNI), USD (WB)	8,820	1,240
E-Government Development Index (UN)	0.7597 (Rank 39 of 193)	0.5835 (Rank 91 of 193)
E-Participation Index (UN)	0.8371 (Rank 42 of 193)	0.6854 (Rank 75 of 193)
World Freedom Index total score (FH)	Not Free (23)	Partly Free (39)
Internet freedom score (FH)	Not Free, 32/100	Partly Free, 62/100
Internet speed (FH)	44.1 Mbps (fixed-line connection)	35.77 Mbps (fixed-line connection)
The average price of an Internet connection, USD (FH)	from 9.40/month (unlimited broadband subscription)	from 7.40 to 8.79/month (unlimited broadband subscription)
The average price of an Internet connection against the gross national income (GNI) per capita (%) (FH)	1	8,3
Internet penetration (% of population) (FH)	84.2%	88.3%
Mobile penetration rate (FH)	131.5%	162.5%
Privacy Legislation	Law "On Personal Data and Its Protection"	Law of the Kyrgyz Republic "On Information of a Personal Manner", dated April 14, 2008, No. 58, Ministry of Justice of the Kyrgyz Republic.
Current state strategy/policy	Digital Kazakhstan (2018-2022)	Digital Kyrgyzstan (2019-2023)
Main regulatory body(ies)	Ministry of Digital Development, Innovation and Aerospace Industry and the National Security Committee	Ministry of Digital Development of the Kyrgyz Republic

Notes: *All data is indicated as of 2019.

** WB refers to the World Bank, UN refers to the United Nations, and FH refers to the Freedom House

Sources: World Bank (n.d.); UN E-governance knowledgebase (2018); Freedom House' Freedom on the Net Report (2019); National Statistics Committees of Kazakhstan and Kyrgyzstan (2020), Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan (n.d.), Ministry of Digital Development of the Kyrgyz Republic (n.d.)

Appendix 2: Interviews (affiliation indicated at the time of interviewing).

Respondent	Affiliation	Date of the interview	Place of the interview
Kyrgyzstan (KGZ)			
KGZ_1	Civil Initiative on Internet Policy	October 8, 2019	Bishkek
KGZ_2	Civil Initiative on Internet Policy	October 8, 2019	Bishkek
KGZ_3	ICT expert	October 9, 2019	Bishkek
KGZ_4	Former advisor to the Office of the Prime Minister of the Kyrgyz Republic	October 11, 2019	Bishkek
KGZ_5	Political scientist/new media expert	October 11, 2019	Bishkek
KGZ_6	Inter-agency interoperability system "Tunduk"	October 15, 2019	Bishkek
KGZ_7	Inter-agency interoperability system "Tunduk"	October 15, 2019	Bishkek
Kazakhstan (KAZ)			
KAZ_1	Internet Society Kazakhstan	February 28, 2020	Almaty
KAZ_2	Internet Freedom Kazakhstan	February 29, 2020	Almaty
KAZ_3	Kazakh State Humanities and Law University (KazGUU)	March 4, 2020	Nur-Sultan
KAZ_4	Human rights activist	March 5, 2020	Nur-sultan
KAZ_5	Ministry of Digital Development,	March 5, 2020	Nur-Sultan

	Innovation and Aerospace Industry		
KAZ_6	National Information Technologies Joint Stock Company (NITEC)	March 5, 2020	Nur-Sultan
KAZ_7	Center for Analysis and Investigation of Cyber Attacks	March 6, 2020	Nur-Sultan
KAZ_8	Legal Media Center	March 7, 2020	Nur-Sultan
KAZ_9	International University of Information Technologies (IITU)	March 14, 2020	Almaty

Appendix 3. List of FGD participants in Bishkek, Kyrgyzstan. October 13, 2019.

participant	sex	age	ethnicity
Participant 1	male	25	Uzbek
Participant 2	male	56	Kyrgyz
Participant 3	female	20	Kyrgyz
Participant 4	female	52	Korean
Participant 5	female	36	Kyrgyz
Participant 6	female	46	German
Participant 7	male	30	Tatar
Participant 8	female	27	Tatar
Participant 9	male	48	Kyrgyz
Participant 10	male	43	Kyrgyz

Appendix 4. List of FGD participants in Almaty, Kazakhstan. February 29, 2020.

participant	sex	age category	ethnicity
Participant 1	male	55	Kazakh
Participant 2	female	52	Kazakh
Participant 3	male	47	Kazakh
Participant 4	female	44	Kazakh
Participant 5	male	38	Kazakh
Participant 6	male	35	Kazakh
Participant 7	female	21	Kazakh
Participant 8	male	37	Korean
Participant 8	female	36	Russian
Participant 9	female	26	Tatar

About the Author

Malika Toqmadi

Malika Toqmadi is a PhD candidate at UCL, UK. She holds an MA in Politics and Security in Central Asia from the OSCE Academy in Bishkek, Kyrgyzstan and an MA in Global and European Security from the University of Geneva, Switzerland. Malika is a co-founder of PaperLab, a public policy research center based in Kazakhstan. Her research interests are Central Asian politics and democratization.

Natalia Zakharchenko

Natalia Zakharchenko is an independent researcher. She holds an MA in Politics and Security in Central Asia from the OSCE Academy in Bishkek, Kyrgyzstan, and LLM in International Law and Politics from Vrije University Amsterdam, the Netherlands. She has been working in the field of human rights for various international human rights organizations. Her interests include Central Asian politics, human rights and international law.

