Original Article

Authoritarian Surveillance and Public Support for Digital Governance Solutions

David Karpa[1] ⓘ and Michael Rochlitz[2] ⓘ

Abstract

This study investigates factors influencing support for digital governance solutions and compares this support between autocracies and democracies. We conduct survey experiments in Russia, Germany, Turkey, the United States, and Estonia, and find that awareness of potential misuse of digital governance tools by the government reduces support. Importantly, while this effect has previously been documented for China, we find it irrespective of regime type for an autocracy, a hybrid regime and three democracies. Individuals relying on government-controlled information sources are more likely to endorse digital governance tools. Our study challenges prior findings by indicating that gaps in public service quality do not boost support. Instead, satisfaction with government services correlates with trust in the government's capacity to implement digital governance solutions.

Keywords

digitization, big data, surveillance, survey experiment, digital authoritarianism, digital governance solutions, algorithmic governance

[1]University of Bremen, Bremen, Germany
[2]University of Oxford, Oxford, UK

Corresponding Author:
David Karpa, University of Bremen, Max-von-Laue-Straße 1, Building: WiWi2, Room: F 2220, Bremen 28359, Germany.
Email: davidfkarpa@gmail.com

Data Availability Statement included at the end of the article

Introduction

Contemporary autocrats face a substantial dilemma when it comes to administering a modern state. On the one hand, it lies in the nature of authoritarian regimes to prevent political change and ensure political control (Svolik, 2012). In order to achieve these objectives, dictators often weaken or dismantle existing institutions such as an independent press or judiciary, which could act as a counterweight to the regime (Aleksashenko, 2018; Brewer-Carias, 2010; Bugaric, 2019; Tahiroglu, 2020). On the other hand, authoritarian regimes must manage increasingly complex societies and economies in order to compete in a global system characterized by rapid economic and technological change. Managing a modern economy requires efficient institutions that can independently decide on a wide range of issues to prevent antisocial behavior and enforce legal rules.

How to solve this dilemma? One answer could be so-called *digital governance solutions* (DGS), i.e. systems that use digital technologies, artificial intelligence and big data to enforce existing legal rules and provide various services to the population, but also hold the potential for authoritarian surveillance and control. As Jee (2022) argues, such systems can be superimposed on existing institutions in a process she calls *institutional proliferation*. Autocrats thus do not need to reform or strengthen existing institutions but can add an additional layer of new institutions to the existing system. The best-known example of such a system to date are the various versions of a *social credit system* (SCS) that have been introduced in China in recent years (see e.g., Backer (2019) or Kostka (2019)), although other countries are introducing similar systems as well (Engvall & Flak, 2022; Manoharan et al., 2022; Peters et al., 2022). During the next couple of years, the use of novel digital technologies for both public administration and authoritarian control could thus become a game changer in the way we think about modern authoritarian states.

Even strongly entrenched autocracies need the support of the population to make digital governance solutions work, however. While the autocrat can enforce adoption, at least to a certain extent, enforcing adoption can be costly. It might therefore be cost-efficient for the autocrat to instead rely on technologies that are useful and enjoy high public approval, for example because they solve some acutely perceived deficiencies in public administration.[1] If citizens become aware that a digital governance solution is mainly used for repressive purposes, this could lead to citizens boycotting or subverting the system, rendering it less efficient. In addition, if repression becomes too visible, it could trigger public backlash, as happened for example when new lockdowns caused large-scale protests in China in November 2022, forcing the Chinese government to back down on its Covid policy.

Understanding the determinants of public support for digital governance solutions is thus crucial to evaluate their potential future role in autocratic states. For now, this question has only been studied for the Chinese context, where Kostka (2019) identify high rates of approval for SCSs, as citizens see them as a tool to improve the quality of life and fill institutional gaps, rather than as a mechanism of authoritarian control.[2] For example, SCSs are seen as convenient tools to establish trust between economic agents in China's banking sector and economy (Ding & Zhong, 2021; Fang et al., 2024; Krause & Fischer, 2020). Once Chinese citizens learn about the repressive potential of the new technology, however, their approval is significantly reduced (Xu et al., 2022).

To see if these results also hold in other authoritarian states, we investigate the question for an autocracy where digital governance solutions might play an equally important role in the future, the Russian Federation. We use a between-subjects computer-assisted telephone interviewing (CATI) experiment conducted in October 2022 in Russia ($N = 2,462$), to investigate how information about the repressive potential of a digital governance solution affects approval for the system. As a robustness-check and to better understand the effect of political regime type on public support, we complement our study with evidence from four additional online survey experiments ($N = 1,000$ each) in four countries that are in the process of introducing digital governance solutions and that feature different levels of political competitiveness, namely Estonia, Germany, the United States and Turkey.

We find that in the control condition, 70.1% of respondents in Russia approve of the introduction of a digital governance solution that increases bureaucratic efficiency and contains some punitive legal capabilities, a number slightly lower than the 80% identified by Kostka (2019) for China. Once Russian citizens are specifically reminded that the system can be used to identify and prosecute political dissent, support drops by almost 25% to 45.9%. Looking at the mechanisms behind our findings, we show that citizens who generally approve of the government and consume information mainly from state-controlled media are more likely to be in favor of introducing a digital governance solution, linking our results to the literature on media effects in autocracies (Adena et al., 2015; Enikolopov et al., 2022; Peisakhin & Rozenas, 2018). Other than in China (Kostka, 2019), perceived institutional gaps do not seem to influence approval.

Our results for Estonia, Germany, the United States, and Turkey are mostly in line with what we find for Russia, allowing us to reject the hypothesis that political regime type has a significant effect on approval. Approval rates in the control condition are highest in Estonia (74.8%), followed by Turkey (66.7%), Germany (65.9%), and the US (45.9%) (see Table Summary Statistics). Once citizens are reminded that the system can be used to prosecute political dissent, support drops significantly in all of the countries (with the exception of the

US, where the drop is also visible, but not statistically significant). In all four countries, satisfaction with public services significantly *increases* approval of a DGS, refuting the hypothesis that gaps in the quality of public services create a demand for digital governance solutions.

Our results have a number of important implications. First, as in the Chinese context, knowledge about the repressive potential of a digital governance solution can significantly reduce public support for the system. This is important, as even in autocracies public support remains essential for the proper functioning of a DGS.[3] Second, regime legitimacy matters. If citizens trust their government and receive information about the world mainly through state-approved sources, they are significantly more likely to support the introduction of a digital governance solution by the state. Third, contrary to our expectations, frustration with the quality of public services does not increase support for a DGS. On the contrary, citizens who are satisfied with the state and the quality of public services are also more supportive of introducing a DGS. Finally, we do not find any conclusive evidence that regime type matters for the approval of digital governance solutions. Approval rates were highest in Estonia (a democracy), followed by Russia, Turkey, and Germany (an autocracy, a hybrid regime, and a democracy), with the US (another democracy) being somewhat of an outlier with much lower approval than in the other countries.

Our paper is organized as follows. Section Literature and Hypotheses shows how our study fits into ongoing debates in the literature, and introduces our theory and hypotheses. Section Data presents our methodology and data, and section Results our results. Section Discussion of the Experimental Findings discusses the implications of our findings, and section Conclusion concludes.

Literature and Hypotheses

When are citizens in favor of sharing their data with the state? And what factors influence the willingness of citizens to support governance platforms with a data-sharing component? The literature on these questions is extensive, and our paper contributes to a number of ongoing debates.

One branch of the literature studies the trade-off between civil liberties and security. After the terrorist attacks of September 11, 2001, citizens in the United States were significantly more willing to give up certain civil liberties for greater personal security (Davis & Silver, 2004; Lewis, 2005). Respondents with lower trust in government institutions were less likely to give up their liberties, ceteris paribus (Davis & Silver, 2004). Ziller and Helbling (2021) replicate the study for the European context, and expand the space of threats to also include pandemics. They find that public support for surveillance technologies that include data collection and might restrict civil

liberties is generally high, but increases when surveillance is targeted at specific threats rather than being indiscriminate, and when a threat is salient. Concerns about privacy reduce support for sharing data with the state.

The Covid pandemic has led to a vast number of studies investigating this trade-off in the context of a global pandemic. Alsan et al. (2020) conduct a global survey with over 550,000 responses in 2020, and find that major crises, such as terrorist attacks and disease outbreaks, can change preferences on the trade-off. However, the results are not uniform and reflect the heterogeneity of different countries and demographic groups. For example, disadvantaged citizens may be less willing to sacrifice their rights because they have fought harder to obtain them in the first place, or because they have comparatively fewer rights and privileges to lose than more advantaged social groups, a result also found in other studies (Davis & Silver, 2004; Dietrich & Crabtree, 2019; Dragu, 2011; Lewis, 2005). Others found cultural or economic vulnerabilities not to consistently predict concerns about internet surveillance in Arab countries (Martin et al., 2019).

Another development linked to the Covid pandemic is the emergence of contact tracing apps, and the trade-off between civil liberties and public health that they entail (Huang et al., 2022; Kitchin, 2020). A range of empirical studies has investigated sources of public support for contact tracing apps, and found that lack of information and concerns over privacy lower support (Williams et al., 2021), while crisis perceptions only seem to play a limited role in explaining uptake (Habich-Sobiegalla & Kostka, 2022). Habich-Sobiegalla and Kostka (2022) find that citizens in Germany, the US and China are willing to accept contact tracing apps despite concerns about privacy and government surveillance, as long as they perceive them to be efficient. They argue that this might explain higher approval rates in China, where usage of the app was mandatory, thus increasing its efficiency.

The debate about contact tracing apps fits into a larger literature on attitudes toward government surveillance and digital surveillance technologies. When are people concerned about surveillance by the state? If people trust the government (Hillebrand, 2021; Kostka et al., 2023; Liu, 2022; Trüdinger & Steckermeier, 2017) or the police (Gurinskaya, 2020), they seem to be less worried about state surveillance. Surveillance by the state also appears to be better tolerated than digital surveillance by corporations (Steinfeld, 2017), with older people being more tolerant of state surveillance, and younger people more tolerant of corporate surveillance (Kalmus et al., 2022). Political views also seem to play a role, with for example US citizens holding libertarian political views being more critical of facial recognition software than those holding right-wing authoritarian views (Peng, 2022). Once Peng (2022) informed respondents about potential demographic biases in the technology, however, support dropped among all respondents, irrespective of their political orientation.

In some societies, in particular China, citizens appear to be more tolerant of state surveillance than in others (Kostka, 2019; Kostka & Habich-Sobiegalla, 2022; Su et al., 2022). The high approval for state surveillance in these societies seems to be due to citizens perceiving digital governance platforms and digital surveillance not as a threat to their privacy and civil liberties, but simply as tools to enhance their convenience and security (Davis & Silver, 2004; Kostka, 2019; Kostka et al., 2021). Once infringement of privacy is explicitly mentioned, support for digital surveillance drops also in China (Kostka et al., 2023). Positive coverage on state media can also significantly increase public support, especially if citizens use state media as their main source of information (Xu et al., 2022). As the literature on informational autocracies has shown, information control and framing can thus become an important tool to foster public support for specific government policies (Guriev & Treisman, 2020, 2022; Rochlitz et al., 2023). Although a specific theory trying to explain the difference in public acceptance of surveillance across different regime types and societies is still missing in the literature, Thompson et al. (2020) show that cultural factors such as societal collectivism can make it more likely that societies accept surveillance by the state. One factor that seems to increase support for digital surveillance across societies is fear, for example of terrorist attacks (Hillebrand, 2021; Kaskeleviciute & Matthes, 2022; Matthes et al., 2019; Yu & Wong, 2023). Fear seems to remain an important predictor of approval even among people who do not trust their own government (Vasilopoulos et al., 2023).

The debate about the trade-off between civil liberties on the one hand and security and convenient governance solutions on the other exists both in democracies and autocracies (see for example Zuboff (2019) for a discussion of corporate surveillance in democracies). It is however particularly relevant in authoritarian and hybrid regimes, because of the new possibilities inherent in digital technologies for authoritarian control and repression (Feldstein, 2019, 2021; Kendall-Taylor et al., 2020; Strittmatter, 2020; Tirole, 2021). Here it might well be possible that digital surveillance technologies in combination with big data and artificial intelligence, once in place, could become a powerful tool permitting contemporary dictators to firmly entrench their hold on power. In hybrid regimes and countries that swing between more and less authoritarian forms of government, such as Turkey or Hungary, but also the United States, a well-functioning surveillance infrastructure could play the role of a technological "ratchet effect" – permitting a country to switch from softer to harder authoritarianism but preventing it from eventually switching back and democratizing again. As argued by Kostka (2019), citizens in autocracies or weak democracies could also be more tempted by the promises of digital governance solutions, as they might promise an easy fix to the deficiencies of corrupt state administrations.

It is therefore crucial to understand what factors play a role during the establishment of such technologies in authoritarian states and hybrid regimes, with one of the most important elements being public support for digital surveillance and governance platforms. However, for the time being, the literature on this question focuses almost exclusively on China (Kostka, 2019; Kostka & Antoine, 2020; Kostka et al., 2023; Kostka & Habich-Sobiegalla, 2022; Liu, 2022; Strittmatter, 2020; Yu & Wong, 2023), even though the phenomenon is relevant in many hybrid regimes and authoritarian states.[4] In our paper, we test these questions for a range of additional countries. Building on the above-cited literature, we derive four distinct hypotheses:

H1: Informing citizens of its repressive potential will reduce support for a DGS.

H2: Citizens whose main source of information are state-controlled media are more likely to approve of a DGS.

H3: In societies where public services suffer from perceived dysfunctionalities, public approval of a DGS will be higher.

H4: Citizens in democracies are less approving of the introduction of a DGS.

Data

To test our hypotheses, we conducted a computer-assisted telephone interviewing (CATI) survey experiment with 2,462 respondents in October 2022 in Russia. The survey was pre-registered,[5] and carried out by FOM, a leading Russian sociological and public opinion research organization.[6] Participants were contacted with the help of census data, and a weighting-scheme was applied to make the sample nationally representative. We complemented our survey with four nationally representative online surveys conducted in September 2022 by the German company Bilendi in Estonia, Germany, the USA, and Turkey, with 1,000 respondents each.[7] Replication material can be found in the Harvard Dataverse (Karpa, 2024).

The question of whether public opinion polls can still be trusted in the increasingly repressive Russian context has been intensely debated during the last year, with various researchers having a more (Morris, 2022, 2023) or less critical view (Pleines, 2023; Reisinger et al., 2022; Rosenfeld, 2022, 2023; Volkov, 2023) of doing survey research in Russia. We believe that surveys are still a valuable tool to gauge public opinion in contemporary Russia. Unlike the Chinese authorities, the Russian government is not controlling what questions can be asked (Rosenfeld, 2023). There are also still a large number of public opinion polls being conducted in Russia every week.[8] Finally, the fact that we find broadly comparable results across all of the five countries we study suggests that public opinion polls can still be used to understand the

Russian context – especially with an experimental methodology that permits testing the reaction of the public to a set of randomized treatments.[9]

In all surveys, we use a two-factor between-subjects experiment. Participants were randomly assigned to either a control group or three different treatment conditions. The treatments were exposure to various forms of information about the possible uses of DGS, either in spoken language (CATI) or in written text (online survey). Slight technical differences between the Russian survey and the other surveys are discussed in Appendix Full Questionnaire. Beyond technical differences we added two questions to the online survey that are not in the Russian version of the questionnaire, a question on political orientation (*liberal* vs. *conservative*, 10-point slider) and a question on different media sources of information (*Television/News/Radio/ Social Media/Smartphone/Apps/Newspaper/Personal conversations*, multiple-choice). The latter is a substitute for the state versus online media question in the Russian version of the questionnaire. We undertook minimal changes trying to maximize comparability and only changing questions where necessary to ensure validity with the given context. Appendix CATI Questionnaire in Russia provides an English translation of the full text for the Russian survey, and Appendix Online Questionnaire the English-language version of the full text for the online surveys.

Respondents were presented with a scenario where a digital platform uses data collected from citizens to make interaction with the government more efficient. The *institutional gap* (Kostka, 2019) addressed in our scenario is thus inefficient or cumbersome government bureaucracy, a scenario that respondents in all five countries – despite some between-country heterogeneity – can relate to. In addition to rendering governance more efficient, the digital platform is also able to connect data gathered from citizens with data gathered from other sources, such as CCTV cameras. This data can then be used to hold citizens who "violate law and order" accountable.

Our treatment conditions differ with respect to the amount of detail that is used to describe what is meant by "violating law and order", with Figure A2 in the Appendix presenting our control and treatment scenarios. In the no-exposure control condition, we do not explicitly state what *"prosecuting those who violate law and order"* means, with respect to both *prosecution* and *violation of law and order*. In the treatment conditions, different violations of what might be considered *law and order* are specified. The first treatment uses a petty crime – breaking a bench on a playground – as an example of a breach of law and order. In the second treatment, we use "participating in an unauthorized protest" as a proxy for behavior that is illegal but can also be understood as an expression of political dissent.[10] In the third treatment, we follow Xu (2022) and combine both treatments. Across all treatments, the punishment we mention as a consequence of illegal behavior is being excluded from public transport for a period of time.[11]

To ensure that participants are not overwhelmed with information, we introduce the description of the experimental scenario in two steps. We first introduce the concept of a "unified state digital archive" that will store data about all citizens and has the objective to "increase the efficiency of the government and simplify interaction with citizens" – our digital governance solution. The next question then introduces the possibility that the DGS can also be used for policing and exposes respondents to the four treatment conditions. Questions are being kept as short and easily worded as possible, and answer options for our outcome variables are 4-point Likert scales (*Would definitely approve/Would rather approve/Would rather not approve/Would definitely disapprove*). If respondents do not want to answer a specific question, they have the option to select *don't know/no answer*. In most other cases, we used binary answer options to further reduce complexity and enhance comprehensibility.

Table Summary Statistics in the Appendix presents summary statistics for all our variables. Our sample was 55.5% female and 50.7 years old (SD = 16.27), on average. We asked participants on a 1 - 4 scale whether they were satisfied with their income (M = 2.92, SD = 0.82), and about their employment status. From the latter we build a dummy taking the value of 1 if employed, and 0 otherwise (M = 0.59, SD = 0.49). Participants reported having received education on a scale ranging from 1–6 (M = 4.45, SD = 1.56), living in either urban or suburban areas (M = 0.42, SD = 0.49), and living specifically in Moscow (M = 0.07, SD = 0.26). We asked participants about their sources of news consumption, where 42.7% (SD = 0.50) reported consuming mainly news from traditional media sources (TV, radio and newspapers), and 37.6% (SD = 0.49) mainly from online media, such as news sites, blogs or social media. This distinction is important, as in October 2022, all traditional media sources in Russia were tightly controlled by the state. Online media, on the other hand, remain less tightly controlled, even though state control is increasing here as well. Regarding trust in public institutions, when asked a binary question 78.9% (SD = 0.41) reported trusting public services, 77.5% (SD = 0.41) had interacted with online government services at least once in the past year, and 83.4% (SD = 0.37) thought the country was developing in a good direction, which we use as a proxy for government approval.[12] Using a 1 - 4 scale, we asked participants about the frequency of previous experiences with online digital services (M = 2.59, SD = 0.99).

Results

Survey Experiment Russia

What factors determine public support for a digital governance solution in an autocracy? We start by looking at the descriptive statistics. Figure 1 illustrates
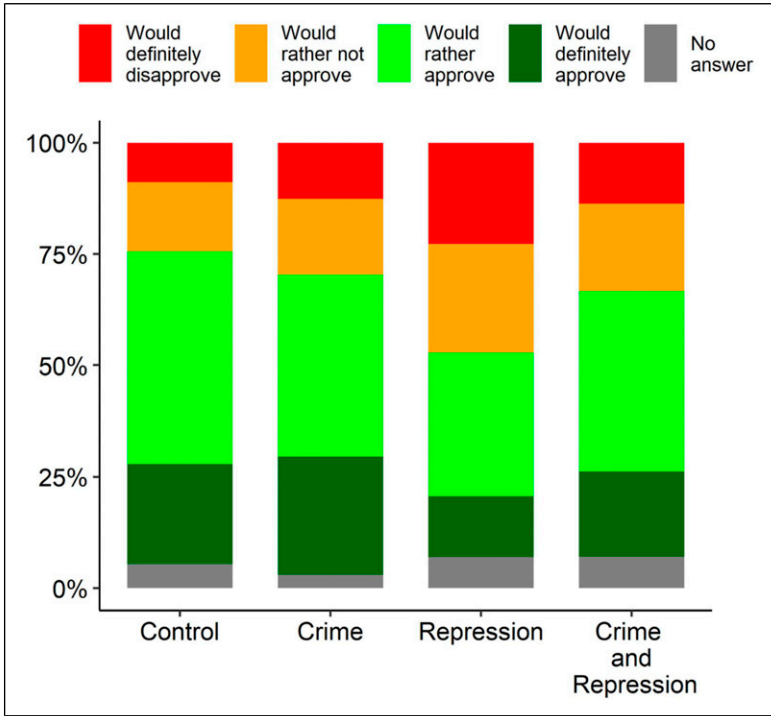
Figure 1. Approval for digital governance solutions in Russia. Notes: See Table Summary Statistics in the Appendix for the underlying calculation.

the effect of the four treatment conditions on support for a DGS that includes a policing component, and the last three columns of Table Summary Statistics in the Appendix provide summary statistics. Our results show that when the policing component is described in general terms ("find and prosecute those who violate law and order"), 70.1% of respondents support the introduction of a DGS. When respondents are provided with the specific example that "a person who broke a bench on a playground could be banned from public transport" (our *crime* treatment), support slightly drops to 67.3%. However, when participants were treated with the *repression* treatment – reminding them that the digital governance solution can be used to identify and prosecute those who participated in "an unauthorized protest" – support decreases by almost 25% to 45.9%. Here it is important to emphasize again that participating in an unauthorized protest, "uchastvovat v nesankcionirovannom mitinge", has become a synonym of political dissent in contemporary Russia, where all anti-government protests are unauthorized. When both treatments are combined, support drops less substantially, to 59.6%, potentially because

adding the crime treatment might somewhat lessen respondents' concerns that the policing component of the DGS is mainly aimed at political repression.

In the next step, we use the following linear equation to conduct a multivariate analysis:

$$y_i = \beta_0 + \beta_1 Crime_i + \beta_2 Repression_i + \beta_3 Crime\ and\ Repression_i + X_i + \epsilon_i,$$
(1)

where y denotes support for a digital governance solution by respondent i, *Crime, Repression*, and *Crime and Repression* are dummy variables that take a value of 1 if a respondent was in the respective treatment group and 0 otherwise, X_i is a vector of socio-demographic controls, and ϵ_i is the error term. Figure 2 presents our results, and Table A6 in the Appendix presents the corresponding regression analysis.[13]

Our main hypothesis (H1) is that approval of a DGS remains high as long as citizens are not aware of its repressive potential, but that citizens – even in a relatively repressive autocracy – will *reduce* their support for a DGS if treated with information that the new technology can be used to suppress political protest. Conversely, our null hypothesis would be that citizens in repressive autocracies are already aware of constant state surveillance, and have therefore internalized the notion of surveillance by the state to the extent that they no longer update their attitudes when reminded about it once again.

Our empirical results confirm H1 and permit us to reject the null hypothesis. While the crime treatment only weakly reduces approval of the DGS, the repression treatment leads to a significant reduction in public support. Compared to the control group, the repression treatment reduces support by
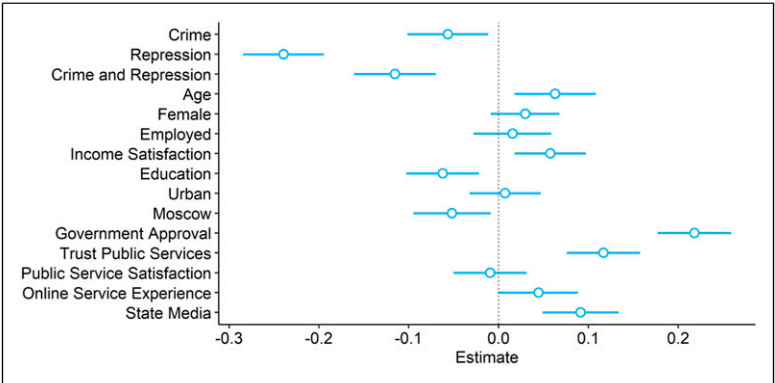

Figure 2. Treatment effects Russia. Notes: Standardized OLS estimates with 95% confidence intervals. See Table A6 in the Appendix for the underlying regression results (specification (3) displayed here).

0.24 SDs[14], which, given a mean of 2.7, is a reduction by 8.8%, with the effect being statistically significant at the 1% level. As before, the combined treatment leads to a somewhat smaller reduction in approval, by 4.3%, potentially because adding the crime treatment might reduce concerns that the DGS is aimed exclusively at political repression. The comparatively strong and negative effect of the repression treatment on approval shows that even in the repressive environment of October 2022, Russian citizens remain genuinely concerned about the surveillance capabilities that a big data governance solution might imply, once they are informed about these capabilities.

In addition to the effect of information on support for a DGS, our empirical analysis reveals a number of further interesting findings, that can help us understand the mechanisms behind our results. First, government approval appears to be a strong predictor of support for a DGS.[15] Citizens who approve of the general direction the country is taking are also significantly more likely to support the introduction of a DGS.

We believe that one important mechanism through which government approval affects preferences for a DGS are channels of information – our hypothesis H2. Citizens who inform themselves mainly through government-controlled sources of information such as state-controlled TV are also significantly more likely to support the introduction of a DGS. Figure 3 splits our sample into respondents who mainly receive information through state-controlled media, and respondents whose main source of information are online media. We see that consumers of online-media such as news sites, blogs or social media – which offer a more pluralistic choice of views – are significantly more sceptical about the introduction of a DGS than consumers of
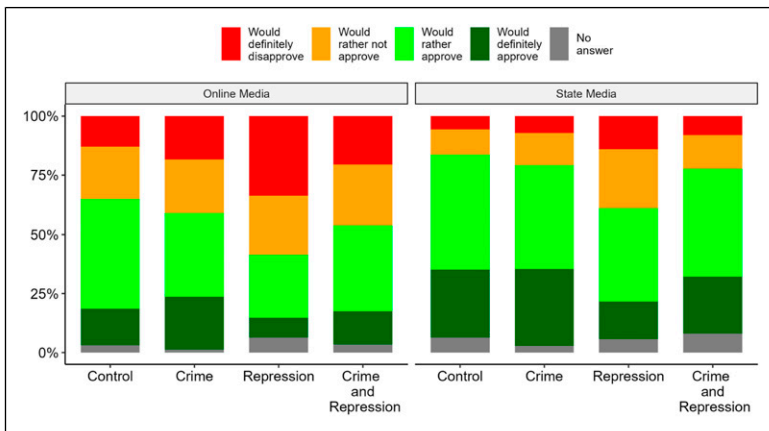

Figure 3. Effects of different media sources on approval. Notes: The sample was split between different primary sources of information for all treatments.

state-controlled media, irrespective of the treatment. We estimate interaction effects between the treatment conditions and state media, finding no heterogeneous effects of state media, which is in line with the previous assessment of Figure 3 (see Table A7 in the Appendix).

Third, general trust in the authorities providing public services also positively predicts support for a DGS.[16] However, other than with the four online surveys discussed in section Online Survey Experiments, a recent positive or negative experience with government service provision has no effect on support. We thus cannot say that existing institutional gaps (i.e. deficiencies with public service provision) might have an influence on support for a digital platform that could address some of these deficiencies (our hypothesis H3).[17]

Finally, citizens who are older and have higher incomes and previous exposure to online services are also slightly more supportive of a digital governance solution, while employment status, gender, and living in a city or a rural location have no clear effect. Conversely, citizens with higher levels of education are less in favor of a DGS, similar to those living in Moscow.

Online Survey Experiments

To complement the experiment we carried out in Russia, we conducted four additional survey experiments in Estonia, Germany, the US and Turkey. The countries were selected to provide us with a range of different regime types, to test if approval of a DGS varies between countries with different political institutions.[18] Estonia and Germany are both consolidated democracies, with the Internet being slightly less free in Germany.[19] The United States, clearly a focal point for the study of contemporary institutional development, scores slightly lower on most institutional indicators. Turkey's political institutions have deteriorated significantly over the last decade, which is reflected in its low democracy scores across the indicators. Similarly, Russia has the lowest institutional indicators in our sample. Both countries have become increasingly authoritarian over the last two decades. It is important to note that the difference between Russia and Turkey is small, while the gap to the other countries is quite substantial.

Figure 4 presents the descriptive statistics of our treatment effects, while Table Summary Statistics in the Appendix provides the underlying summary statistics. We find that approval rates for a DGS vary across countries and treatments. In general, average approval rates in the control condition are highest in Estonia (74.8%), followed by Turkey (66.7%), Germany (65.9%), and the US (45.9%).

First, the fact that the approval rate in the control condition for Russia (70.1%) is somewhere in the middle of what we find for the other countries suggests that the Russian data are meaningful and that survey participants in
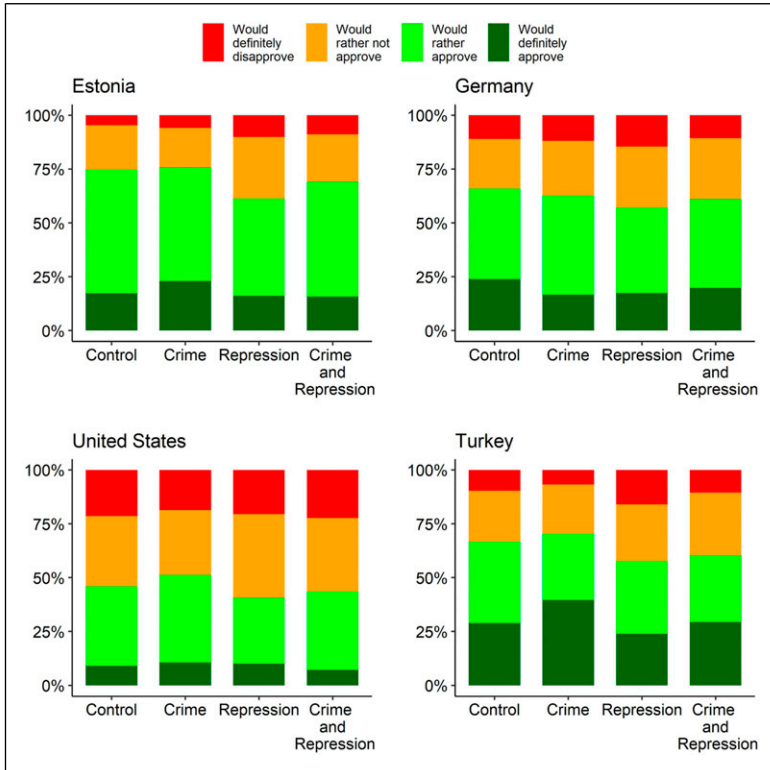
Figure 4. Approval for digital governance solutions.

Russia did not self-censor (Robinson & Tannenberg, 2019) or falsify their preferences (Eck et al., 2021), at least not more than in the other countries.

Second, and more interestingly, we do *not* find a linear relationship between political freedom and approval of a new institution that might potentially limit it, allowing us to reject our hypothesis H4. Our data suggest at least two possible explanations. Either there is non-linearity in the correlation, for example a U-shaped dependence between institutional freedom and support for digital government solutions. Alternatively, individual country characteristics, such as culture, economic development or history, might play a more critical role than indices designed only to measure political institutions. For example, it might be the case that in the United States, a country whose constitution, founding myth and economic system put particular emphasis on the importance of freedom, institutions with the potential to limit freedom are met with more scepticism than in other countries.[20] The US might therefore be an outlier with respect to absolute approval rates for a DGS.

While we find differences across countries with respect to overall approval rates, when comparing the variation between treatments, results are relatively similar across countries. For all four countries, the *repression* treatment caused a visible dent in approval rates, similar to what we found for Russia in section Survey Experiment Russia. The effects for the *crime* and the combined treatment are less pronounced.

For a more precise analysis, we again use equation (1) to conduct a multivariate analysis. Figure 5 presents the results of our treatments, Figure A3 in the Appendix the full set of results, and Tables A8–A11 in the Appendix the underlying regression analyses. Additionally, we estimated a logistic regression model that serves as a robustness check (see Figure A5).

In Estonia, Germany, and Turkey, our main finding from the first experiment could be replicated, i.e., the coefficient for the *repression* treatment has a negative effect and is significant at least at the 95%-level, providing additional evidence in support of hypothesis H1. Results for the US are also negative, but not statistically significant, with a smaller coefficient than for the other three countries. To better understand our results for the US, we looked at the effect of our treatment on different age groups, and found evidence for significant age-related polarization (see Figure A1 in the Appendix, as well as Table A13). It appears that citizens in the US who are 60 years and older are actually *more* in favor of a DGS if the technology features a repression component,
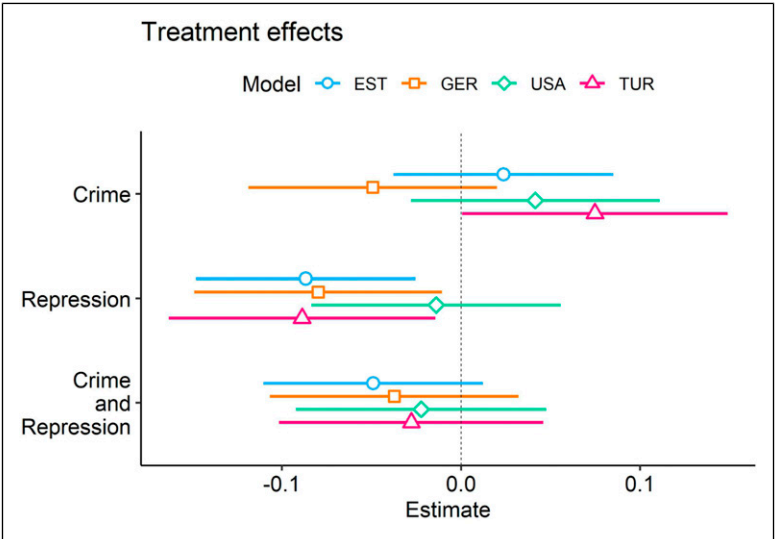

Figure 5. Treatment effects in Estonia, Germany, the United States, and Turkey. Notes: Standardized OLS estimates with 95% confidence intervals. See Appendix Regression Tables for the underlying regression results.

explaining why our *repression* treatment remains insignificant for the country as a whole. This effect, however, can only be found for the US, and not for any other country in our study. In Turkey, there are even statistically significant additional *negative* treatment effects for citizens above 60 years.[21] Finally, other than in the Russian experiment where we find a negative effect, the *crime* and the combined treatment had no statistically significant effects in Turkey, Estonia, Germany and the US. This might be explained by the very low trust rates Russians have for the police (see e.g., Semukhina and Reynolds (2014)), while trust in the police is substantially higher in the other four countries in our sample.[22]

Our results suggest that the effects we find for Russia seem to be robust across countries with different regime types and different levels of political competitiveness (see Figure 6). While in general approval of a DGS is high, once respondents are primed that the technology can be used for purposes of political control, the drop in approval rates is substantial. Interestingly, this drop only occurs in the case of the political repression treatment, and not when respondents are treated with the possibility that the technology could be used for policing petty crime. If anything, the results from countries other than Russia suggest that the policing functionality of a DGS *increases* approval, although not significantly.

Figure A3 in the Appendix presents some additional interesting results. First, trust in the quality of public services, as well as a positive experience with government services during the previous year are positive predictors of approval for a DGS. These results refute our "institutional gaps" hypothesis
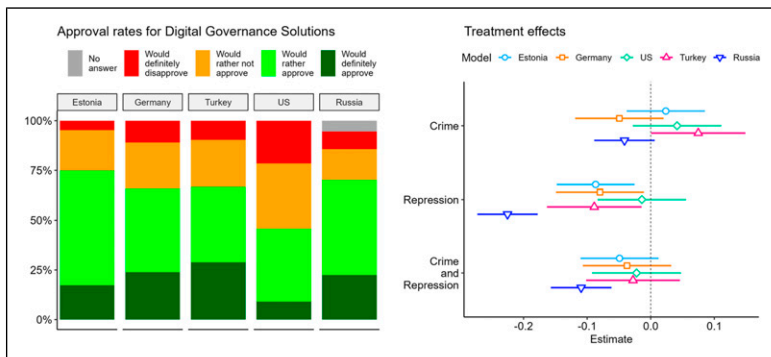

Figure 6. Approval for digital governance solutions and treatment effects summary. Notes: Left panel gives approval rates for Digital Governance Solutions as measured in the control condition. In Russia, due to the nature of CATI, the data includes "don't know/no answer", while no such option was available in the online surveys in the other four countries. Right panel shows treatment effects as estimated in the models in the Section Regression Tables.

(H3). People do not seem to be more likely to approve (or wish for) a DGS because they are experiencing difficulties with existing public services. Rather, they approve of introducing a DGS if they already have a positive view of public services – probably because they expect the authorities to implement it in a responsible and efficient way.

Second, respondents who are satisfied with their personal income situation and who approve of "the direction into which the country is developing" (our "government approval" indicator) are also more likely to approve of a DGS. These results suggest that being satisfied with your personal situation and the overall affairs of the country also makes people more open to the introduction of new governance technology. Interestingly, though, education has the opposite effect. More educated respondents, on average, are more sceptical towards the introduction of a DGS, with the effect being significant for Estonia, Germany, and the US. These findings are robust for specifications including the full sample, see Table A12.

Finally, while we also find a positive effect of TV news consumption on DGS approval for Estonia, Germany, and the US (as in the case of Russia), here the results of the experiments cannot be directly compared with the results we obtain for Russia. While in Russia receiving news about the state of the world mainly from television has become a synonym for being a recipient of state propaganda, the content of TV news in the other countries in our sample is much more heterogeneous, and does not allow a similar conclusion.

Discussion of the Experimental Findings

Perhaps the most important finding of our study is that *information* – about the potential costs of a DGS – *matters*. In other words, public support for a DGS seems to depend on citizens not being aware of its repressive potential, or, more generally, of the costs imposed by the new technology. Once they are being informed about the political risks of a new institution, approval drops significantly, irrespective of the context and country they live in.

When having to decide about the advantages and disadvantages of adopting a new institution, a rational citizen will infer information from priors that stem from her or his *informational* and *institutional* background. Our results show that in this situation, sources of information can play an important role. An extensive literature has shown that the media can be instrumental in influencing human behavior, both in democracies (Barone et al., 2015; DellaVigna & Kaplan, 2007; Durante et al., 2019; Gerber et al., 2009) and in autocracies (Adena et al., 2015; Enikolopov et al., 2011, 2022; Peisakhin & Rozenas, 2018). Autocracies such as Russia are particular, however, in that the state has agenda-setting power over the media, and can suppress alternative sources of information. How the government frames certain issues can then have an important effect on citizens' perceptions and behavior (Kazun, 2016;

Pan et al., 2022). Xu et al. (2022) illustrate this point by showing how Chinese citizens who receive information about the Chinese social credit system through state media subsequently show higher levels of support for the system. In our paper, we document a similar effect for Russia, with Russian citizens who receive information mainly through state-controlled media being significantly more likely to support the introduction of a DGS.[23]

Another informational input influencing citizens' cost-benefit analysis is the institutional environment. When citizens perceive the government and existing government services as trustworthy, they might infer that new institutions can also be trusted. This is indeed what we find. Russian citizens who approve of the direction the country is taking – our proxy for government approval – are almost three standard deviations more supportive of a DGS. We find a similar, albeit smaller effect for trust in public services. Both effects can also be found for Estonia, Germany, the United States and Turkey, although here the effects are not always statistically significant.

In this, our paper relates to an extensive literature investigating the role of institutions in determining acceptance rates for new technologies and tolerance for government surveillance. Similar to our study, a number of experimental papers have found that trust in the government or its institutions plays a key role in the acceptance of facial recognition technology (Kostka et al., 2021, 2023) and correlates positively with support for government surveillance (Su et al., 2022; Trüdinger & Steckermeier, 2017) and sacrificing civil liberties for security (Alsan et al., 2020; Davis & Silver, 2004). It also increases support for social credit systems (Kostka, 2019) and leads to a higher willingness for data-sharing in the context of Covid-19 contact tracing apps (Huang et al., 2022; Kostka & Habich-Sobiegalla, 2022). Looking at the issue from the opposite direction, Kostka and Antoine (2020) show that digital governance solutions such as China's social credit systems work better when confidence in the government is high. Ziller and Helbling (2021) reverse this causality and examine the effect of surveillance on trust in governments. Some studies argue that strong emotions such as fear can moderate the effect of trust in the government, so that even people who normally would not trust their government approve of restricting civil liberties when exposed to risks such as political unrest (Yu & Wong, 2023) or Covid-19 (Vasilopoulos et al., 2023).

In sum, it seems that even in authoritarian contexts such as Russia or China, trust in government institutions is crucial to make digital governance solutions work. This is why contemporary dictatorships often attach a lot of importance to creating public legitimacy for the regime, often through control over channels of information and the media (Guriev & Treisman, 2020, 2022). The media can thus become an important driver of trust in institutions, while also helping to build support for specific policies favoured by the state – as we document in our paper.

Conclusion

In our study, we conducted a survey experiment in five different countries to understand the determinants of public approval for digital governance solutions. We find that information about the potential abuse of a DGS by a government for purposes of political repression can significantly reduce public support for the new technology. Crucially, this effect is consistent across different institutional settings that feature different levels of institutional safeguards against government abuse of power.[24]

Why does this matter? Big data governance technologies as the one described in our paper have the potential to become a game changer in the way we think about government surveillance and political control, in particular – but not only – in autocracies. China is a pioneer in this respect. During the last couple of years, China has tested a number of social credit systems in different regions of the country (Kostka, 2019; Kostka & Antoine, 2020; Li & Kostka, 2022; Liu, 2022; Strittmatter, 2020). The Covid pandemic (Chen et al., 2022; Knight & Creemers, 2021) and recent breakthroughs in artificial intelligence, big data and facial recognition have given the technology an additional boost. China is now using the data gathered via its surveillance systems as an input subsidy for Chinese firms, to promote its domestic industry and further improve its surveillance capabilities in what has become a positive feedback loop (Beraja et al., 2022; 2023b). This has made China an undisputed leader in the market for digital governance, big data and facial recognition technologies (Feldstein, 2023), which are now being offered as integrated packages, for example via so called "smart city" or "safe city" solutions (Große-Bley & Kostka, 2021; Yang & Xu, 2018). Beraja et al. (2023a) find that China is now actively exporting these technologies, in particular to other authoritarian countries. If an authoritarian government was recently challenged by domestic political protests, the likelihood that it will import a DGS with a policing component from China is particularly high (Beraja et al., 2023a). Often, surveillance technologies are offered in bundles with infrastructure and other technologies, as part of global strategies such as the "Belt and Road Initiative". As with the democratizing effects of trade with democratic countries (Tabellini & Magistretti, 2022), trade with China can thus foster authoritarian consolidation, via the export of digital governance solutions (Beraja et al., 2023b; Feldstein, 2023).

One country that is particularly at risk is Russia. Russia has been learning from China with respect to mechanisms of authoritarian governance for some time (Libman & Rochlitz, 2019), has recently been digitizing its service sector and economy (Østbø, 2021), while also becoming increasingly authoritarian. While this paper has been written, Russia started using facial recognition technology from China to identify draft dodgers in the Moscow metro,[25] and its novel DGS "gosuslugi" to deliver conscription orders to Russian men who

were supposed to join the ranks of the Russian army in Ukraine.[26,27] Other countries have also started implementing big data governance technologies from China, for example Kenya, Laos, Mongolia, Uganda, Saudi Arabia and Uzbekistan (Feldstein, 2023). As argued by Feldstein (2023), once put in place, technologies combining digital governance and big data with capabilities of surveillance and control might make it much more difficult than today for civic accountability and democratization movements to challenge autocratic governments, potentially introducing a new wave of autocratization (Lührmann & Lindberg, 2019; Snyder, 2018).

Understanding the factors that determine the often surprisingly high rates of public approval for digital governance solutions is therefore crucial. As our study shows, it seems that once citizens become aware that such technologies could play the role of a "Trojan horse" for introducing methods of authoritarian control, they are much more circumspect about adopting the new technology. This is important, not only in autocracies such as Russia, but also – and probably even more so – in hybrid regimes and democracies that have proven vulnerable to populist leaders with authoritarian tendencies, such as for example Turkey or the United States.

ORCID iDs

David Karpa https://orcid.org/0000-0002-4327-4269
Michael Rochlitz https://orcid.org/0000-0001-8652-8874

Data Availability Statement

The data and replication files can be found here: https://doi.org/10.7910/DVN/A1YQKY (Karpa, 2014).

Supplemental Material

Supplemental material for this article is available online.

Notes

1. Indeed, as shown by Li and Kostka (2022), convincing citizens to actively engage with a DGS is not a trivial task, but might require some effort from the side of the authoritarian government.
2. It seems that Kostka (2019) is for now one of the only papers that explicitly uses the concept of institutional gaps. We find the concept very useful, and build on it in our analysis.
3. As politicians in democracies, authoritarian leaders *do* care about regime legitimacy and public approval (Gerschewski, 2018), and are concerned about the possibility of backlash and public protests (Buckley et al., 2022), which might deter them from introducing a DGS. In addition, digital platforms such as a DGS need a sufficiently large amount of public support and participation to function properly, as shown for example by the literature on e-participation (Kneuer & Harnisch, 2016; Lee & Kim, 2018; Toots, 2019). Finally, because for informational autocrats it is crucial to convince the public of their competence (Guriev & Treisman, 2022), high citizen approval for a DGS might even be one of the objectives of the strategic autocratic planner.
4. One notable exception is Feldstein (2021), who studies digital repression in Thailand, the Philippines, and Ethiopia.
5. https://www.socialscienceregistry.org/trials/9566.
6. https://fom.ru/.
7. https://www.bilendi.de/.
8. https://www.themoscowtimes.com/2022/12/06/what-secret-russian-state-polling-tells-us-about-support-for-the-war-a79596.
9. In conducting the same survey in 5 different countries, our paper thus also makes a valuable contribution to the debate about the validity of survey research in authoritarian political contexts.
10. We specifically decided to use this treatment, as it is particularly salient in the context of our main experiment. In Russia, "participating in an unauthorized protest" ("uchastvovat v nesankcionirovannom mitinge") has become a synonym of expressing political dissent, as all protest actions against the government have in recent years been forbidden by the authorities, and are therefore "unauthorized". For comparability reasons, we keep the same treatment in the other four countries, where, although the costs of participating in "unauthorized protests" is lower, unauthorized protests are also salient (for example in the case of climate activists in Germany, student protests in the US, or anti-government protests in Turkey).
11. This comes close to some of the standard sanctions in the Chinese SCS. Similarly, being banned from driving was introduced as a punishment in Russia in early 2023 for not complying with electronic summons to the military over the DGS Gosuslugi

(https://www.washingtonpost.com/world/2023/04/11/russia-conscription-military-mobilization-war/).

12. Although 83.4% might seem high, this result is in line with the results of other recent surveys, including studies that use list experiments to test if Russian public opinion polls about government approval reflect the true opinion of the population, see e.g., Frye et al. (2017, 2023).

13. In order to add robustness to our study, we further estimate a multinomial model which we report in Figure A4. In this model we do not find evidence for systematic non-reporting between treatment conditions, which is a blind-spot for our linear model.

14. This effect size can be considered to be small to medium. However, because the control condition also implicitly entails the potential for misuse, the treatment effects are potentially underestimated, which should be taken into consideration.

15. To measure government approval, we use a standard question that has been used for many years in social science surveys to measure general support for the policies of the government in Russia, see Question 10 in Appendix CATI Questionnaire in Russia.

16. When using a different coding for this question, as specified in Table A6 under "Coding", the coefficient is still positive but smaller and no longer significant. We thus advise the reader to handle this result with caution.

17. In addition, we estimate interaction effects for these variables in the specifications (2) to (5) which we report in Table A7. We do not find statistically significant interaction effects between our treatment conditions and trust in and satisfaction with public services.

18. See Tables A4 and A5 in the Appendix for the range of different institutional indicators used in our approach.

19. Estonia scores 93 out of 100 on the Freedom on the Net index, while Germany scores 77 out of 100.

20. See for example Kennedy (1999), McPherson (2003), Rana (2014) or Schmidli (2022) for a discussion of the importance of the concept of freedom in recent US history.

21. In addition to age, we also test for heterogeneous treatment effects for political orientation and government approval. We find that the repression and combined treatments reduce approval for a DGS among US citizens with liberal political views (Table A14). We find no heterogeneous treatment effects with respect to government approval (Table A15).

22. Recent survey data show a big variation in trust in the police across countries, with 86% of respondents trusting the police in Estonia, 49% in Germany, 48% in the US, 39% in Turkey, but only 20% in Russia in 2022. See Goldie (2023) for data on Germany, the US, Turkey and Russia, and Kaitseministeerium (2023) for Estonia.

23. Indeed, the subject of the digitization of the Russian state has been extensively and positively covered on Russian state media, in particular since Mikhail Mishustin took over as prime minister in January 2020, who made the digitization of Russia's state

administration one of his priorities (see for example https://tass.com/society/1571181 and https://foreignpolicy.com/2020/01/20/russia-incoming-prime-minister-techno-authoritarianism/).

24. This finding begs the question of whether citizens perceive existing institutional safeguards as *insufficient*, or whether institutional safeguards do not play a significant role in moderating this effect, opening up interesting new avenues for further research.

25. https://www.hrw.org/news/2022/10/26/russia-uses-facial-recognition-hunt-down-draft-evaders.

26. https://carnegieendowment.org/politika/89553.

27. See: https://www.scmp.com/economy/china-economy/article/2186606/chinas-social-credit-system-shows-its-teeth-banning-millions.

References

Adena, M., Enikolopov, R., Petrova, M., Santarosa, V., & Zhuravskaya, E. (2015). Radio and the rise of the nazis in prewar Germany. *Quarterly Journal of Economics*, *130*(4), 1885–1939.

Aleksashenko, S. (2018). *Putin's counterrevolution*. Brookings Institution Press.

Alsan, M., Braghieri, L., Eichmeyer, S., Kim, M. J., Stantcheva, S., & Yang, D. (2020). *Civil liberties in times of crisis*. NBER Working Paper No. 27972.

Backer, L. C. (2019). China's social credit system: Data-driven governance for a 'new era'. *Current History*, *118*(809), 209–214.

Barone, G., D'Acunto, F., & Narciso, G. (2015). Telecracy: Testing for channels of persuasion. *American Economic Journal: Economic Policy*, *7*(2), 30–60.

Beraja, M., Kao, A., Yang, D., & Yuchtman, N. (2023a). Exporting the surveillance state via trade in AI. *NBER Working Paper*, 31676. https://doi.org/10.3386/w31676

Beraja, M., Kao, A., Yang, D. Y., & Yuchtman, N. (2023b). AI-tocracy. *Quarterly Journal of Economics*, *138*(3), 1349–1402. https://doi.org/10.1093/qje/qjad012

Beraja, M., Yang, D. Y., & Yuchtman, N. (2022). Data-intensive innovation and the state: Evidence from AI firms in China. *The Review of Economic Studies*, *90*(4), 1701–1723. https://doi.org/10.1093/restud/rdac056

Brewer-Carias, A. (2010). *Dismantling democracy in Venezuela: The Chávez authoritarian experiment*. Cambridge University Press.

Buckley, N., Reuter, J., Rochlitz, M., & Aisin, A. (2022). Staying out of trouble: Criminal cases against Russian mayors. *Comparative Political Studies*, *55*(9), 1539–1568.

Bugaric, B. (2019). Central Europe's descent into autocracy: A constitutional analysis of authoritarian populism. *International Journal of Constitutional Law*, *17*(2), 597–616.

Chen, W., Huang, G., & Hu, A. (2022). Red, yellow, green or golden: The post-pandemic future of China's health code apps. *Information, Communication & Society*, *25*(5), 618–633.

Davis, D., & Silver, B. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science*, *48*(1), 28–46.

DellaVigna, S., & Kaplan, E. (2007). The fox news effect: Media bias and voting. *Quarterly Journal of Economics*, *122*(3), 1187–1234.

Dietrich, N., & Crabtree, C. (2019). Domestic demand for human rights: Free speech and the freedom-security trade-off. *International Studies Quarterly*, *63*(2), 346–353. https://doi.org/10.1093/isq/sqz011

Ding, X., & Zhong, D. (2021). Rethinking China's social credit system: A long road to establishing trust in Chinese society. *Journal of Contemporary China*, *30*(130), 630–644.

Dragu, T. (2011). Is there a trade-off between security and liberty? Executive bias, privacy protections, and terrorism prevention. *American Political Science Review*, *105*(1), 64–78. https://www.jstor.org/stable/41480827

Durante, R., Pinotti, P., & Tesei, A. (2019). The political legacy of entertainment TV. *The American Economic Review*, *109*(7), 2497–2530.

Eck, K., Hatz, S., Crabtree, C., & Tago, A. (2021). Evade and deceive? Citizen responses to surveillance. *The Journal of Politics*, *83*(4), 1545–1558. https://doi.org/10.1086/715073

Engvall, T., & Flak, L. (2022). Digital governance as a scientific concept. In Y. Charalabidis, L. Flak, & G. Pereira (Eds.), *Scientific foundations of digital governance and transformation: Concepts, approaches and challenges* (pp. 25–50). Springer.

Enikolopov, R., Petrova, M., & Zhuravskaya, E. (2011). Media and political persuasion: Evidence from Russia. *The American Economic Review*, *101*(7), 3253–3285.

Enikolopov, R., Rochlitz, M., Schoors, K., & Zakharov, N. (2022). *The effect of independent online media in an autocracy*. SSRN Working Paper No. 4346225. https://doi.org/10.2139/ssrn.4131355

Fang, H., Chen, L., Xiong, J., & Zhu, Y. (2024). Social trust and entrepreneurship: Insights from China's social credit system. *Finance Research Letters*, *62*(Part A), 105118.

Feldstein, S. (2019). The Road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy*, *30*(1), 40–52.

Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.

Feldstein, S. (2023). Surveillance in the illiberal state. In A. Sajó, R. Uitz, & S. Holmes (Eds.), *Routledge handbook of illiberalism* (pp. 351–364). Routledge. chapter 24.

Frye, T., Gehlbach, S., Marquardt, K., & Reuter, O. J. (2017). Is Putin's popularity real? *Post-Soviet Affairs*, *33*(1), 1–15.

Frye, T., Gehlbach, S., Marquardt, K., & Reuter, O. J. (2023). Is Putin's popularity (still) real? A cautionary note on using list experiments to measure popularity in authoritarian regimes. *Post-Soviet Affairs*, *39*(3), 213–222.

Gerber, A. S., Karlan, D., & Bergan, D. (2009). Does the media matter? A field experiment measuring the effect of newspapers on voting behavior and political opinions. *American Economic Journal: Applied Economics*, *1*(2), 35–52.

Gerschewski, J. (2018). Legitimacy in autocracies: Oxymoron or essential feature? *Perspectives on Politics*, *16*(3), 652–665.

Goldie, J. (2023). *Interactive: Trust in the police around the world*. 360info. https://doi.org/10.54377/9cf8-53dc

Große-Bley, J., & Kostka, G. (2021). Big data dreams and reality in Shenzhen: An investigation of smart city implementation in China. *Big Data & Society*, *8*(2), 1–14.

Guriev, S., & Treisman, D. (2020). A theory of informational autocracy. *Journal of Public Economics*, *186*(C), 104158.

Guriev, S., & Treisman, D. (2022). *Spin dictators: The changing face of tyranny in the 21st century*. Princeton University Press. 9780691211411. https://www.jstor.org/stable/j.ctv1xp9p7d

Gurinskaya, A. (2020). Predicting citizens' support for surveillance cameras. Does police legitimacy matter? *International Journal of Comparative and Applied Criminal Justice*, *44*(1-2), 63–83.

Habich-Sobiegalla, S., & Kostka, G. (2022). Sharing is caring: Willingness to share personal data through contact tracing apps in China, Germany, and the US. *Information, Communication & Society*, *26*(14), 1–28. https://doi.org/10.1080/1369118X.2022.2113421

Hillebrand, K. (2021). The role of fear and trust when disclosing personal data to promote public health in a pandemic crisis. In F. Ahlemann, R. Schütte, & S. Stieglitz (Eds.), *Innovation through information systems: Volumne I: A collection of latest research on domain issues* (pp. 247–262). Springer. chapter 18.

Huang, G., Hu, A., & Chen, W. (2022). Privacy at risk? Understanding the perceived privacy protection of health code apps in China. *Big Data & Society*, *9*(2), 1–13. https://doi.org/10.1177/20539517221135132

Jee, H. (2022). *Credit for compliance: How institutional layering ensures compliance in China*. Phd-thesis, Stanford University. https://purl.stanford.edu/tg087jk8675

Kaitseministeerium. (2023). *Public opinion on national defense*. Kaitseministeerium.

Kalmus, V., Bolin, G., & Figueiras, R. (2022). Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. *New Media & Society*, *29*(6), 1–23.

Karpa, D. (2024). *Replication data for: Authoritarian surveillance and public support for digital governance solutions*. https://doi.org/10.7910/DVN/A1YQKY

Kaskeleviciute, R., & Matthes, J. (2022). A vicious cycle? Threat of terror, perceived media bias, and support for surveillance policies. *Mass Communication & Society*, *26*(3), 463–485.

Kazun, A. (2016). Framing sanctions in the Russian media: The rally effect and Putin's enduring popularity. *Demokratizatsiya: The Journal of Post-Soviet Democratization*, *24*(3), 327–350.

Kendall-Taylor, A., Frantz, E., & Wright, J. (2020). The digital dictators: How technology strengthens autocracy. *Foreign Affairs*, *99*(2), 103–115.

Kennedy, D. (1999). *Freedom from fear: The American people in depression and war, 1929-1945*. Oxford University Press.

Kitchin, R. (2020). Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity*, *24*(3), 362–381.

Kneuer, M., & Harnisch, S. (2016). Diffusion of e-government and e-participation in democracies and autocracies. *Global Policy*, *7*(4), 548–556.

Knight, A., & Creemers, R. (2021) *Going viral: The social credit system and COVID-19*. Working Paper, Leiden University.

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, *21*(7), 1565–1593.

Kostka, G., & Antoine, L. (2020). Fostering model citizenship: Behavioral responses to China's emerging social credit systems. *Policy & Internet*, *12*(3), 256–289. https://doi.org/10.1002/poi3.213

Kostka, G., & Habich-Sobiegalla, S. (2022). In times of crisis: Public perceptions toward COVID-19 contact tracing apps in China, Germany, and the United States. *New Media & Society*, *26*(4), 2256–2294. https://doi.org/10.1177/14614448221083285

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, *30*(6), 671–690.

Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, *40*(1), 101761. https://doi.org/10.1016/j.giq.2022.101761

Krause, T., & Fischer, D. (2020). An economic approach to China's social credit system. In O. Everling (Ed.), *Social Credit Rating: Reputation und Vertrauen beurteilen* (pp. 437–454). Springer. chapter 22.

Lee, J., & Kim, S. (2018). Citizens' E-participation on agenda setting in local governance: Do individual social capital and E-participation management matter? *Public Management Review*, *20*(6), 873–895.

Lewis, C. W. (2005). The clash between security and liberty in the U.S. Response to terror. *Public Administration Review*, *65*(1), 18–30.

Li, H., & Kostka, G. (2022). Accepting but not engaging with it: Digital participation in local government-run social credit systems in China. *Policy & Internet*, *14*(4), 845–874.

Libman, A., & Rochlitz, M. (2019). *Federalism in China and Russia: Story of success and story of failure?* Edward Elgar.

Liu, C. (2022). Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems. *International Sociology*, *37*(3), 391–412. https://doi.org/10.1177/02685809221084446

Lührmann, A., & Lindberg, S. (2019). A third wave of autocratization is here: What is new about it? *Global Policy*, *7*(4), 548–556.

Manoharan, A., Melitski, J., & Holzer, M. (2022). Digital governance: An assessment of performance and best practices. *Public Organization Review*, *23*, 265–283.

Martin, J. D., Naqvi, S. S., & Schoenbach, K. (2019). Attribute substitution and stereotypes about the online Arab public sphere: Predictors of concerns about internet surveillance in five Arab countries. *New Media & Society*, *21*(5), 1085–1104. https://doi.org/10.1177/1461444818821369

Matthes, J., Schmuck, D., & von Sikorski, C. (2019). Terror, terror everywhere? How terrorism news shape support for anti-Muslim policies as a function of perceived threat severity and controllability. *Political Psychology*, *40*(5), 935–951.

McPherson, J. (2003). *Battle cry of freedom: The civil war era*. Oxford University Press.

Morris, J. (2022). Political ethnography and Russian studies in a time of conflict. *Post-Soviet Affairs*, *39*(1-2), 92–100.

Morris, J. (2023). Public opinion still does not exist; war in Ukraine and dictatorship in Russia can help us acknowledge that. *Russian Analytical Digest*, *292*, 7–8.

Østbø, J. (2021). Hybrid surveillance capitalism: Sber's model for Russia's modernization. *Post-Soviet Affairs*, *37*(5), 435–452.

Pan, J., Shao, Z., & Xu, Y. (2022). How government-controlled media shifts policy attitudes through framing. *Political Science Research and Methods*, *10*(2), 317–332. https://doi.org/10.1017/psrm.2021.35

Peisakhin, L., & Rozenas, A. (2018). Electoral effects of biased media: Russian television in Ukraine. *American Journal of Political Science*, *62*(3), 535–550.

Peng, Y. (2022). The role of ideological dimensions in shaping acceptance of facial recognition technology and reactions to algorithm bias. *Public Understanding of Science*, *32*(2), 535–550.

Peters, B., Pierre, J., Sørensen, E., & Torfing, J. (2022). The promise, perils and pitfalls of digital governance. In B. Peters, J. Pierre, E. Sørensen, & J. Torfing (Eds.), *A research agenda for governance* (pp. 133–151). Edward Elgar. chapter 8.

Pleines, H. (2023). Levada polls on the discuss data online platform: Accessing and discussing Russian surveys of public opinion. *Russian Analytical Digest*, *292*, 9–10.

Rana, A. (2014). *The two faces of American freedom*. Harvard University Press.

Reisinger, W., Zaloznaya, M., & Woo, B. D. (2022). Fear of punishment as a driver of survey misreporting and item non-response in Russia and its neighbors. *Post-Soviet Affairs*, *39*(1-2), 49–59.

Robinson, D., & Tannenberg, M. (2019). Self-censorship of regime support in authoritarian states: Evidence from list experiments in China. *Research & Politics*, *6*(3), 1–9. https://doi.org/10.1177/2053168019856449

Rochlitz, M., Schoors, K., & Zakharov, N. (2023). *Can authoritarian propaganda compete with the opposition on social media? Experimental evidence from Russia*. SSRN Working Paper No. 4433145.

Rosenfeld, B. (2022). Survey research in Russia: In the shadow of war. *Post-Soviet Affairs*, *39*(1–2), 38–48.

Rosenfeld, B. (2023). Curious what Russians think about the war? Ask yourself this before you read the polls. *Russian Analytical Digest*, *292*, 4–6.

Schmidli, W. M. (2022). *Freedom on the offensive: Human rights, democracy promotion, and us interventionism in the late cold war*. Cornell University Press.

Semukhina, O., & Reynolds, K. M. (2014). Russian citizens' perceptions of corruption and trust of the police. *Policing and Society*, *24*(2), 158–188.

Snyder, T. (2018). *The Road to unfreedom: Russia, Europe, America*. Tim Duggan Books.

Steinfeld, N. (2017). Track me, track me not: Support and consent to state and private sector surveillance. *Telematics and Informatics*, *34*(8), 1663–1672.

Strittmatter, K. (2020). *We have been harmonized: Life in China's surveillance state*. Custom House.

Su, Z., Xu, X., & Cao, X. (2022). What explains popular support for government monitoring in China? *Journal of Information Technology & Politics*, *19*(4), 377–392. https://doi.org/10.1080/19331681.2021.1997868

Svolik, M. (2012). *The politics of authoritarian rule*: Cambridge University Press.

Tabellini, M., & Magistretti, G. (2022). *Economic integration and the transmission of democracy*. NBER Working Paper No. 30055.

Tahiroglu, M. (2020). How Turkey's leaders dismantled the rule of law. *Fletcher Forum of World Affairs*, *44*(1), 67–96.

Thompson, N., McGill, T., Bunn, A., & Rukshan, A. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology*, *71*(9), 1129–1142.

Tirole, J. (2021). Digital dystopia. *The American Economic Review*, *111*(6), 2007–2048.

Toots, M. (2019). Why E-participation systems fail: The case of Estonia's Osale.ee. *Government Information Quarterly*, *36*(3), 546–559.

Trüdinger, E. M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly*, *34*(3), 421–433. https://doi.org/10.1016/j.giq.2017.07.003

Vasilopoulos, P., McAvay, H., Brouard, S., & Foucault, M. (2023). Emotions, governmental trust, and support for the restriction of civil liberties during the covid-19 pandemic. *European Journal of Political Research*, *62*(2), 422–442. https://doi.org/10.1111/1475-6765.12513

Volkov, D. (2023). Are meaningful public opinion polls possible in today's Russia? *Russian Analytical Digest*, *292*, 2–3.

Williams, S., Armitage, C., Tampe, T., & Dienes, K. (2021). Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study. *Health Expectations*, *24*(2), 377–385.

Xu, X. (2022). *The unintrusive nature of digital surveillance and its social consequences*. Working Paper.

Xu, X., Kostka, G., & Cao, X. (2022). Information control and public support for social credit systems in China. *The Journal of Politics*, *84*(2), 2230–2245.

Yang, F., & Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's cybersecurity law. *Asia & the Pacific Policy Studies*, *5*(3), 533–543.

Yu, Z., & Wong, S. (2023). Social media, fear, and support for state surveillance: The case of China's social credit system. *China Information*, *37*(1), 51–74. https://doi.org/10.1177/0920203X221088141

Ziller, C., & Helbling, M. (2021). Public support for state surveillance. *European Journal of Political Research*, *60*(4), 994–1006.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *Public Affairs*.

Author Biographies

David Karpa is a doctoral student at the University of Bremen, Germany. His research interest lies in the interplay between political and economic institutions, and human behavior.

Michael Rochlitz is Associate Professor in the Economies of Russia, Eastern Europe and Eurasia at the Oxford School of Global and Area Studies. His research is on the interrelation between political institutions, economic development and societal change, with a regional focus on Russia and China.