State surveillance and the COVID-19 crisis

Kristine Eck & Sophia Hatz

To cite this article: Kristine Eck & Sophia Hatz (2020) State surveillance and the COVID-19 crisis, Journal of Human Rights, 19:5, 603-612, DOI: 10.1080/14754835.2020.1816163

To link to this article: https://doi.org/10.1080/14754835.2020.1816163

© 2020 The Author(s). Published with license by Taylor & Francis Group, LLC

Published online: 11 Nov 2020.

Submit your article to this journal

Article views: 6083

View related articles

View Crossmark data

Citing articles: 1 View citing articles
State surveillance and the COVID-19 crisis

Kristine Eck and Sophia Hatz
Uppsala University

ABSTRACT
The outbreak of COVID-19 has ushered in a global rise in state surveillance. In an effort to trace the spread of the disease and to enforce lockdowns, governments in democracies and autocracies alike have turned to surveillance technologies such as contact tracing apps. Governments have also tightened their hold on communication flows in other ways, through censorship and information manipulation. These kinds of government actions are not new: States have long recognized the value of controlling information in times of crisis. In this article, we consider these tactics in the context of the COVID-19 pandemic, in which, unlike most other security threats, the threat posed is not endogenous to governance and applies to all countries. We consider how observations from this context prompt future research and reflect on the implications of information control for civil liberties.

Introduction
In April 2020, the Norwegian Institute of Public Health (NIPH) launched a mobile app called Smittestopp (“infection stop”) designed to collect users’ geolocated movement data in order to help authorities trace the spread of COVID-19. This app was described by Amnesty International (2020) as one of the most invasive COVID-19 contact tracing apps in the world, alongside those in countries like Bahrain and Kuwait. By June, the Norwegian data oversight agency warned the NIPH that it would stop it from handling data collected through the app (Agence France-Presse 2020).

Norway’s Smittestopp exemplifies an unexpected byproduct of the COVID-19 pandemic: a global rise in state surveillance. Since the outbreak of COVID-19, governments in country after country have turned to surveillance as a means of tracing the spread of the disease and enforcing lockdowns. Autocratic countries like China and Singapore were quick to adapt and extend existing digital surveillance technologies to monitor COVID-19. And democratic countries followed suit: In a matter of months, more than 34 countries enacted surveillance measures; 22 of them were full democracies (OneZero 2020).

Governments have also responded to a rapid outpouring of misinformation in social media outlets. Rumors and falsehoods about the origins, symptoms, and remedies for COVID-19 became so widespread that in February 2020 the World Health Organization (WHO) deemed the situation an “infodemic”—weeks before it declared a pandemic.² In this context, governments have taken measures such as the censorship of online content and the criminalization of “fake news.” But some governments themselves have also contributed to this infodemic by deliberately misrepresenting information about the disease.
These kinds of government actions are not new: States have long recognized the value of controlling information in times of crisis. Scholars will recognize the measures implemented by governments during the COVID-19 pandemic as examples of surveillance, censorship, and information manipulation. Previous research has described how governments use these tactics to contain domestic political threats: Surveillance allows for the detection of dissent and for the targeted application of repression (Gohdes 2019); censorship enables states to restrict criticism of the government, to cut communication necessary for collective action, and to silence reports of abuse (Gunitsky 2015); and information manipulation can serve as a tool for distracting the public, for discourse framing, and for counternobilization (Gunitsky 2015; King, Pan and Roberts 2017). Although a pandemic is a different context than contentious politics, we have seen an analogous tendency of states to ramp up personal data collection and to tighten their control over information.\(^3\)

In this article, we begin by defining surveillance, censorship, and information manipulation, and anchoring these concepts in the existing literature. Although researchers tend to study these tactics separately, we observe that these practices often cooccur. We suggest that jointly considering the array of information control tactics governments have at their disposal may provide insights into how states adjudicate between them. We probe this idea in the context of the COVID-19 pandemic, which prompted a global rise in information-control practices, especially state surveillance. We conclude by reflecting on the implications of information control during COVID-19 for the protection of civil liberties.

**Surveillance, censorship, and information manipulation**

We view surveillance, censorship, and information manipulation as distinct tactics that are components of a more general strategy, which we label *information control*. Information control tactics differ in the means by which control is achieved, as well as in the types of information that are controlled. A government may use these tactics individually or in tandem, and it may change its strategy over time.

*State surveillance* involves the monitoring, collecting, and/or processing of personal data by a government. This can include the monitoring of online activity, location tracking via Bluetooth or Global Positioning System (GPS), tracking financial transactions, video surveillance, facial scans, and the collection of biometric data. The kinds of information states have the capacity to collect and connect is vast, precise, and often private in nature. Foundational works in sociology, economics, and philosophy consider state surveillance as fundamental to both governance and social control: It is a method of identifying individuals, ordering society, and ensuring discipline.\(^4\)

State surveillance received renewed scholarly attention with the advent of the internet and other advanced information and communications technology (ICT). ICT massively increases the power, reach, and capacity of governments to monitor their populations (Lyon 2007; Marx 2015). Within political science, much research on surveillance has come to focus on its application by authoritarian regimes, as a tool to counter domestic political threats (e.g., Kuran 1997; Jiang and Yang 2016), as state surveillance for the detection of dissent and the extraction of intelligence, which enables the targeted application of repression (Gohdes 2019).

*State censorship* involves a government blocking or altering communication in order to control the information individuals disseminate to one another. For example, states can place filters to restrict the results returned by online search engines, remove specific online content and block websites, disable social media, remove leaks by whistleblowers,\(^5\) and shut down the internet. Like most recent research on surveillance, contemporary studies of censorship take ICT as a point of departure and tend to focus on authoritarian regimes (e.g., Roberts 2018; Gohdes 2019; Glässel and Paula 2020). ICT has facilitated the spread of popular sentiments and provided new tools for collective action, but it has also bolstered governments’ capacities to intervene in communications
and social networks (Weidmann and Rød 2019). By deleting information from the public eye, states are able to restrict criticism of the government, silence reports of abuse, limit communication necessary for the coordination of collective action, and curtail the dissemination of information the public uses to form policy opinions (Hayes and Reineke 2007; King, Pan, and Roberts 2013; Gunitsky 2015). Governments may also cut digital communication completely; when information flows may be too great to selectively censor, governments may resort to internet shutdowns.

States do not only censor information, however: They also actively engage in state information manipulation, which is the manipulation, fabrication, or cooptation of information for strategic purposes (Gunitsky 2015). Examples include a government’s production of fake news, fabrication of social media posts, dissemination of propaganda or libel, and restriction of access to governmental data. For example, the Chinese government hires internet commentators to post large numbers of fabricated social media comments as if they were the genuine opinions of ordinary Chinese people, a tactic aimed at distracting the public and shifting focus (King et al. 2017; Roberts 2018). Other scholars have pointed to how states disseminate propaganda or false information for purposes such as shaping the political attitudes of citizens (Geddes and Zaller 1989) and for countermobilization of a regime’s support base (Gunitsky 2015).

Although some research contains an implicit recognition that states employ an array of tactics to collect and control information (e.g., Geddes and Zaller 1989), the field more often tends to silo these different tactics. For instance, although the monitoring of individuals and of communications is necessary for their silencing, studies of state censorship rarely account for ongoing state surveillance, theoretically or empirically. In practice, state uses of surveillance, censorship, and information manipulation often occur in tandem.

Information control in the context of the COVID-19 pandemic

The COVID-19 pandemic provides a unique setting for understanding state information control as, unlike most other security threats, the threat posed by the disease is not endogenous to governance and is applicable to all countries. Because information control is routine in most autocracies, we focus particularly on consolidated democracies, where new information control practices risk undermining established civil liberties.

Surveillance

Surveillance is the tactic that has been most readily embraced by democratic governments, which they have seemingly adopted with the same energy as their autocratic counterparts. The types of surveillance measures adopted in response to the COVID-19 pandemic include public surveillance of population movements under lockdown through closed-circuit television (CCTV), drones, mobile phone usage data, and biometric tracker bracelets. But the most prominent form of surveillance has been the adoption of mobile applications that allow for COVID-19 tracking. The basic premise is to scale up traditional contact tracing by leveraging digital technology. Yet there is a tension in the digital utopianism that sees mobile phones as a means by which to help protect from disease and fears of privacy invasion. Concerns about digital overreach in democracies are not new, but the high stakes of the COVID-19 pandemic have seen official state surveillance efforts fast-tracked and securitized in a way that is new to the digital landscape.

There is no single approach to these surveillance apps, and they vary depending on whether they are the result of public or private initiatives, what sort of technology is used to track contact between individuals, whether data storage is centralized or decentralized, whether the app is voluntary, whether limitations are placed on data collection, whether there are provisions for destroying the data, whether the data is anonymized, and whether the app is transparent (e.g.,
through open-source code). All of these technologies raise questions not only of privacy infringement but also of whether they are even effective to begin with (Stanley and Granick 2020).

Most democratic governments have reiterated their commitment to ensuring privacy in this context, but concerns remain. Anonymized data, for example, are at risk of reidentification (De Montjoye, Hidalgo, Verleysen and Blondel 2013), and although data may be stored on users’ phones rather than centralized in order to minimize privacy concerns, there are fears that the data can be hacked. Citizens have generally allowed governments a wide berth in responding to the pandemic, but privacy activists have raised questions about the extent to which these surveillance measures are truly “extraordinary,” as opposed to extensions of already ongoing moves by democratic states to engage in domestic surveillance.

Importantly, we see variation across democratic governments in terms of the extent to which they have sought to ensure that encroachments on civil liberties are necessary, effective, and proportionate. If we consider the Norwegian example, the benefits of the app were ultimately deemed insufficient to warrant its overreach into citizen privacy. Indeed, numerous governments’ own oversight bodies have pushed back in relation to the design of contact tracing apps. Slovakia, for example, fast-tracked several amendments to its telecommunications act that expanded telecom companies’ obligations to retain individual location data. These measures were challenged at the Slovakian Constitutional Court and were subsequently suspended due to their “vagueness and insufficient safeguards against misuse” (Electronic Frontier Foundation 2020).

Table 1 shows the development of COVID-19 tracking apps across European democracies as of June 19, 2020. Fifteen countries had already launched COVID-19 tracking apps. They were in development in an additional seven countries, whereas 14 countries had opted against the apps for the time being. There are likely to be numerous and heterogeneous reasons for this cross-national variation, but eyeballing the data, it is evident that it is not only a question of feasibility: Many countries that have the technological resources to quickly develop an app have opted not to do so. Similarly, many countries that are famously concerned with personal privacy protection, such as Germany, have been forerunners in adopting apps.

This variation in surveillance is evident not only in Europe but across the globe. In India, for example, the government and many major private employers are requiring employees to download the official, ostensibly voluntary COVID-19 tracking app. India has no national data privacy law, and critics have pointed out that it is not clear who has access to data from the app and in what situations (O’Neill 2020).

| Country                  | Govt app | Country                  | Govt app |
|--------------------------|----------|--------------------------|----------|
| United Kingdom           | in development | Macedonia                | yes      |
| Ireland                  | in development | Croatia                 | in development |
| Netherlands              | no       | Montenegro               | no       |
| Belgium                  | no       | Slovenia                 | no       |
| Luxembourg               | no       | Greece                   | no       |
| France                   | in development | Cyprus                  | yes      |
| Switzerland              | in development | Bulgaria                | yes      |
| Spain                    | Basque region only | Moldova                | no       |
| Portugal                 | no       | Romania                  | no       |
| Germany                  | yes      | Estonia                  | in development |
| Poland                   | yes      | Latvia                   | yes      |
| Austria                  | yes      | Lithuania                | yes      |
| Hungary                  | yes      | Armenia                  | no       |
| Czech Republic           | yes      | Georgia                  | yes      |
| Slovak Republic          | yes      | Finland                  | in development |
| Italy                    | yes      | Sweden                   | no       |
| Albania                  | no       | Norway                   | yes      |
| Kosovo                   | no       | Denmark                  | yes      |
| Serbia                   | no       |                         |          |

Sources: MIT Technology Review, Digital Rights Tracker, individualized online searches.
There are certainly reasons to fear mission creep—that governments will not be willing abandon the new surveillance opportunities these apps offer and that personal data will be collected indefinitely and used for unanticipated ends. In the United Kingdom, the government plans to retain the data it collects for up to 20 years and denies individuals an absolute right to have their data deleted upon request (Hern 2020). Rights groups have raised fears that the data may be used for other purposes, and have pointed out that the government has failed to conduct a legally mandated data protection impact assessment (Sabbagh and Hern 2020). There are precedents for these fears. For example, the US Patriot Act, passed in 2001 in response to the terrorist attacks of September 11, 2000, gave the government broad surveillance powers with limited oversight. It remains in place today, despite the lack of any indication there is an immediate threat of a foreign attack on US soil.

Censorship and information manipulation

During the COVID-19 pandemic, censorship has primarily been justified as a response to the infodemic. The spread of rumors, falsehoods, and conspiracy theories, primarily on social media, rapidly became a serious threat to governments’ efforts to contain the disease. The WHO has warned that false and misleading information by nonhealth actors has dangerous consequences for individuals’ health and undermines trust in health authorities (WHO 2020). In this context, governments have imposed various measures of censorship, including regulating online content and criminalizing “fake news.”

Autocratic countries with existing censorship regimes were quick to tune their filters to COVID-19-related content. For example, as Chinese citizens began to share information about a mysterious disease in Wuhan, online posts and hashtags related to disease were quickly deleted and the users’ accounts blocked (Shiji 2020). In democracies, governments have taken a less top-down approach, often collaborating with the private sector to remove falsehoods from the internet (Goldsmith and Woods 2020). Tech companies such as Facebook, Twitter, and Google have used human censors and computer algorithms to remove pandemic-related falsehoods, ban events in contradiction of social distancing directives, and alert users who have been exposed to content later found to be misleading.11

In more extreme cases, the regulation of COVID-related content has involved prohibiting information not attributable to the government or a public health authority.12 This has primarily taken place in authoritarian countries, where states have tighter controls over the media; but it has also occurred in democracies. In March 2020, Armenia introduced legislation requiring any dissemination of information regarding the disease to draw on information provided by a special emergency office under the prime minister (International Center for Not-for-Profit Law/ICNL 2020).

Another, more extreme form of censorship that has arisen in the context of COVID-19 has been the criminalization of misinformation. This has been widespread across both autocracies and democracies. At least 24 countries have passed laws or orders restricting or punishing the dissemination of false information,13 and in 15 of these countries, the dissemination of false information is punishable with prison time. Although Hungary is the only EU member to have passed laws on fake news, there have been calls within the European Commission to go beyond the current self-regulatory nature of online media (Stolton 2020).

Even as governments have taken steps to contain the spread of COVID-related misinformation, governments have also participated in the manipulation of information themselves. The most obvious examples come from countries with low levels of expressive freedoms to begin with, but well-known examples of government information manipulation have taken place in consolidated democracies, as well. Most notably, US President Donald Trump initially dismissed the
virus as a “hoax” and has continuously promoted the drug chloroquine as a remedy for COVID-19, even though experts have refuted these claims (Haberman 2020).

Aside from distributing false information, many countries have restricted access to official information. In Georgia, regulations introduced in connection with the containment of COVID-19 extended the timeframe for government responses to requests for public information, essentially exempting the government from ordinary deadlines set by law. Similar exemptions to the Freedom of Information Act were passed in some US states (e.g., New Jersey and Washington, DC). The Brazilian government has stopped releasing counts of COVID-19 cases and deaths (ICNL 2020), and Sweden has concealed from the public certain government communications and information concerning preparedness for the virus (Rudbäck 2020).

**Discussion**

Although much of what know about state information control comes from the literature on authoritarian regimes, during the Covid-19 pandemic we have witnessed a dramatic rise in information control among democracies and autocracies alike. The rise among democracies is particularly troubling, as democracy rests on principles such as freedom of expression and the right to privacy, and democratic countries have become the cornerstones of international efforts toward protection of human rights (Beutz 2003).

The empirics of the COVID-19 pandemic illustrate that states can deploy different means of informational control. During the pandemic, surveillance has dominated as the information control tactic of choice. Indeed, surveillance is often a necessary first step toward censorship and information manipulation; in order to control information, communications must first be monitored. On the other hand, some forms of censorship have not increased or may have even lessened during the COVID-19 pandemic. The critical necessity to access information during the pandemic makes it difficult for governments to justify internet shutdowns on the grounds of public order or national security (UN 2020b). The empirics also illustrate that different tactics of information control often co-occur and reinforce each other; in some countries, laws criminalizing fake news and granting governments special privileges to surveil have been packaged together under emergency orders passed in response to the pandemic (ICNL 2020).

Information control has been a priority for governments, even relative to other modes of crisis response. But states’ intentions behind information control are difficult to infer, even when explicitly deployed in the name of a public health emergency. Although many countries have justified censorship on the basis of the infodemic, this is not the only possible chronology. Rumors on social media may have arisen in response to perceived information vacuums or due to discrepancies between official figures and experiences on the ground. If this is true, states may have had other motives for censorship and information manipulation, including as a pretext to silence critics and consolidate political power (Roth 2020).

Observations such as these prompt questions for future research. Scholars will need to tackle the question of explaining variation in information control. Why have some democratic countries adopted surveillance measures while others have not? How do we explain the differences in privacy protections? Why do some countries use multiple information control tactics while others do not? In the longer term, researchers will also be able to examine which countries dismantled information control apparatuses after the pandemic and which retained them.

The COVID-19 pandemic also indicates that different types of existential threats may prompt different types of government intervention and, as a consequence, regimes may adjust their expectations of the political costs of information control. For example, as the pandemic hit Israel, Prime Minister Benjamin Netanyahu revealed the existence of a secret national database containing private personal data on all Israeli citizens, their daily movements, transactions, and social contacts. The pandemic, Netanyahu inferred, provided a good moment for the revelation of these
data and their overt deployment (Silverstein 2020). To understand how state leaders adjudicate between tactics, researchers will need to consider how different securitization processes may face different levels of contention.

Researchers will also need to study the consequences of information control measures adopted during the COVID-19 pandemic. How do citizens assess whether the government has their welfare in mind or ulterior motives? How do preexisting levels of trust impact the citizen–state relation as a consequence of the pandemic, in both the short term and the long term? A growing body of research indicates that states’ efforts to control information may have profound effects on individuals’ political attitudes and behaviors, and that these effects can run in multiple directions (Penney 2016; Stoycheff 2016; Brayne 2017; Eck, Hatz, Crabtree and Tago, forthcoming). Will the information control responses adopted in response to COVID-19 shift citizen attitudes relating to trust and legitimacy and, if so, in which direction?

In addition to the COVID-19 pandemic and the infodemic, the United Nations has warned of a third “parallel epidemic of authoritarian and repressive measures” (UN 2020b). Not only are falsehoods spread by nonstate actors dangerous, individuals are jeopardized when states withhold information, when they have diminished trust in public authorities, and when official statements contain propaganda and disinformation (UN 2020b). This third trend has the potential to be endemic: Activists across the globe have articulated fears that the COVID-19 pandemic may have ushered in a new era of normalized state surveillance. For states to mitigate these fears requires extraordinary levels of transparency and oversight to ensure the new information control measures are being used to promote the safety and security of citizens and not to strengthen government control. The United Nations has warned that the potential for abuse is high and that “what is justified during an emergency now may become normalized once the crisis has passed. … All measures must incorporate meaningful data protection safeguards, be lawful, necessary, and proportionate, time-bound and justified by legitimate public health objectives” (UN 2020a). Whether governments heed these admonitions to ensure and protect civil liberties will be a major post-pandemic issue.

Notes

1. We identified democracies as a score of 6 or above on the Polity2 variable (see https://www.systemicpeace.org/csprandid.html).
2. The WHO declared a Public Health Emergency of International Concern on January 30, 2020, referred to the “infodemic” on February 15, and declared a pandemic on March 11 (see www.who.int and www.euro.who.int).
3. We focus on government actions, as these have the clearest implications for civil liberties under international human rights law. We discuss private efforts when they are undertaken at the behest of, or are promoted by, governments. Although many surveillance apps have been developed by private actors, such as companies or universities, governments have encouraged or even mandated their use. Also, when it comes to online content regulation, much private action can be viewed as action by the state, as states often impose obligations to regulate communication and information (Land 2019).
4. See Marx (2015) and Lyon (2007) for overviews of the literature on surveillance.
5. We restrict our definitions to state policies and practices that target information, rather than people. For this reason, we consider the removal of information leaked by whistleblowers and the removal of media content as examples of censorship, whereas we bracket the targeting of whistleblowers and journalists.
6. What we will define as “information manipulation” is referred to by various terms, such as “flooding” (Roberts 2018), “propaganda” (Geddes and Zaller 1989), “false news” (Gläßel and Paula 2020), “astroturfing” and “reverse censorship” (King et al. 2017), and “social media co-option” (Gunitsky 2015). Other terms popular during the COVID-19 pandemic are “misinformation” and “disinformation.”
7. Although the scope of the threat may be perceived by countries differently, depending on the quality of their healthcare systems or demographic characteristics, the pandemic was arguably understood as a threat by every country.
8. Adopted in Lichtenstein, Bahrain, and Hong Kong (OneZero 2020).
9. Notably, the rare Apple–Google partnership allows governments to use its open-source application programming interface (API) to develop national apps. Some governments have opted to adopt this technology, whereas others have developed their own apps. There have been extensive debates about how to ensure privacy protections in these mobile apps. In many of these discussions, companies have been less willing than governments to encroach on personal privacy (McGee, Murphy, and Bradshaw 2020), although they have not gone far enough for many privacy activists. Some government officials have criticized the stranglehold companies have on countries’ ability to design surveillance apps (Ilves 2020).

The complicated relationships between public and private interests in digital surveillance is a promising avenue for future research.

10. Bluetooth technology records what other phones an individual has come into proximity with, whereas geolocation technology records locations where the phone has been physically. For reasons relating to both accuracy and privacy protection, the Bluetooth approach is typically favored by privacy advocates.

11. These measures include responses to misinformation from government officials; corporate measures have occurred both in collaboration with and in opposition to governments.

12. Here it becomes clear how censorship differs from fact-checking.

13. Argentina, Algeria, Azerbaijan, Bolivia, Bosnia and Herzegovina, Botswana, China, Ethiopia, Hungary, India, Lesotho, Malaysia, North Macedonia, Philippines, Russia, Solomon Islands, South Africa, Thailand, United Arab Emirates, the United States (Puerto Rico), Uzbekistan, Vietnam, and Zimbabwe (ICNL 2020).

14. We view this as information manipulation, as the information targeted is produced by the government rather than the populace, as in censorship.

Notes on contributors

Kristine Eck is an associate professor of peace and conflict research at Uppsala University. Her research interests concern state coercion and policing.

Sophia Hatz is an assistant professor at the Department of Peace and Conflict Research at Uppsala University. Her research interests relate to state-led human rights violations and restrictions on civil liberties, particularly civilian responses to state coercion and repression. Methodologically, she specializes in survey methods and experimental design. She has conducted research in diverse contexts such as Israel, Palestine, the United States, Japan, and China. Her work is published in journals such as Journal of Politics, Journal of Conflict Resolution, and Conflict Management and Peace Science. She earned her PhD from Uppsala University in May 2019.

References

AGENCE FRANCE-PRESSE. (2020) Norway suspends virus-tracing app due to privacy concerns, The Guardian, 15 June. [Online]. Available: https://www.theguardian.com/world/2020/jun/15/norway-suspends-virus-tracing-app-due-to-privacy-concerns [28 July 2020].

AMNESTY INTERNATIONAL. (2020) Bahrain, Kuwait and Norway Contact Tracing Apps Among Most Dangerous for Privacy. [Online]. Available: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/ [18 June 2020].

BEUTZ, Molly. (2003) Functional democracy: Responding to failures of accountability. Harvard International Law Journal, 44(2), 387–432.

BRAYNE, Sarah. (2017) Big data surveillance: The case of policing. American Sociological Review, 82(5), 977–1008. doi:10.1177/0003122417725865

DE MONTJOYE, Yves-Alexandre, HIDALGO, César A., VERLEYSEN, Michel, and BLONDEL, Vincent D. (2013) Unique in the crowd: The privacy bounds of human mobility. Scientific Reports, 3, 1376.

ECK, Kristine, HATZ, Sophia, CRABTREE, Charles, and TAGO, Atsushi. (forthcoming) Evade and deceive? Citizen responses to surveillance. Journal of Politics.

ELECTRONIC FRONTIER FOUNDATION. (2020) International Proposals for Warrantless Location Surveillance to Fight COVID-19. [Online]. Available: https://www.eff.org/deeplinks/2020/05/global-contact-tracing-international-proposals-track-COVID-19 [14 July 2020].

GEDDES, Barbara, and ZALLER, John. (1989) Sources of popular support for authoritarian Regimes. American Journal of Political Science, 33(2), 319–347.

GLÄBEL, Christian, and PAULA, Katrin. (2020) Sometimes less is more: Censorship, news falsification, and disapproval in 1989 East Germany. American Journal of Political Science, 64(3), 682–698.

GOHDES, Anita R. (2019) Repression technology: Internet accessibility and state violence. American Journal of Political Science, 64(3), 488–503.
SILVERSTEIN, Richard. (2020) Israel is militarising and monetising the COVID-19 pandemic, The Wire, 20 April. [Online]. Available: https://thewire.in/world/israel-is-militarising-and-monetising-the-covid-19-pandemic [28 July 2020].

STANLEY, Jay, and GRANICK, Jennifer Stiusa. (2020) The Limits of Location Tracking in an Epidemic. [Online]. Available: https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic [18 June 2020].

STOLTON, Samuel. (2020) Regulation Against Fake News ‘Very Important,’ Reynders Says. [Online]. Available: https://www.euractiv.com/section/digital/news/regulation-against-fake-news-very-important-reynders-says/ [28 July 2020].

STOYCHEFF, Elizabeth. (2016) Under surveillance: Examining Facebook’s spiral of silence effects in the wake of NSA internet monitoring. Journalism & Mass Communication Quarterly, 93(2), 296–311.

UNITED NATIONS. (2020a) COVID-19 and Human Rights: We Are All in This Together. [Online]. Available: https://www.un.org/en/un-coronavirus-communications-team/we-are-all-together-human-rights-and-covid-19-response-and [28 July 2020].

UNITED NATIONS. (2020b) Disease Pandemics and the Freedom of Opinion and Expression. UN Doc. A/HRC/44/49. [Online]. Available: https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ReportDiseasePandemics.aspx [17 August 2020].

WEIDMANN, Nils B, and RØD, Espen Geelmuyden. (2019) The Internet and Political Protest in Autocracies (Oxford, UK: Oxford University Press).

WORLD HEALTH ORGANIZATION (WHO). (2020) Working Together to Tackle the ‘Infodemic.’ [Online]. Available: https://www.euro.who.int/en/health-topics/Health-systems/pages/news/news/2020/6/working-together-to-tackle-the-infodemic [28 July 2020].