Long-term Prescription? Digital Surveillance is Here to Stay

AHMED MAATI	Eberhard-Karls-Universität Tübingen, Germany
E-MAIL	ahmed.maati@uni-tuebingen.de
ORCID	https://orcid.org/0000–0002–5546–553X
ŽILVINAS ŠVEDKAUSKAS	Eberhard-Karls-Universität Tübingen, Germany
E-MAIL	zilvinas.svedkauskas@uni-tuebingen.de
ORCID	https://orcid.org/0000–0001–7256–2502

ABSTRACT

An emerging literature has shown concerns about the impact of the pandemic on the proliferation of digital surveillance. Contributing to these debates, in this paper we demonstrate how the pandemic facilitates digital surveillance in three ways: (1) By shifting everyday communication to digital means it contributes to the generation of extensive amounts of data susceptible to surveillance. (2) It motivates the development of new digital surveillance tools. (3) The pandemic serves as a perfect justification for governments to prolong digital surveillance. We provide empirical anecdotes for these three effects by examining reports by the Global Digital Policy Incubator at Stanford University. Building on our argument, we conclude that we might be on the verge of a dangerous normalization of digital surveillance. Thus, we call on scholars to consider the full effects of public health crises on politics and suggest scrutinizing sources of digital data and the complex relationships between the state, corporate actors, and the sub-contractors behind digital surveillance.

KEYWORDS	digital surveillance, COVID-19, pandemic, privacy, human rights, surveillance capitalism
DOI	https://doi.org/10.32422/mv-cjir.1821

Times of crises open opportunity structures that can change the nature of politics and society as we know them. The "war on terror" doctrine that started after the the 9/11 attacks illustrates that in such cases, structural changes remain even after the original emergencies are over. The COVID-19 pandemic likewise invites us to rethink the political ramifications of global crises (LIPSCY 2020). In this essay, we focus on how the pandemic brought transformations related to the field of digital surveillance in particular. We argue that it has facilitated digital surveillance in three ways.

The first impact that the pandemic has on digital surveillance is social. The unprecedented restrictions on movement and interaction have increased the reliance of a sizeable portion of the world's population on digital means of communication. The trend towards digitization has captured the attention of many scholars in recent years (KOSINSKI – STILLWELL – GRAEPEL 2013; KUNER – CATE N.D.; ZWITTER – HADFIELD 2014). However, during the pandemic, personal, educational, and business communications have moved to the online world to limit the spread of the virus to previously unseen extents. At the same time, the ongoing great migration to the digital world generates a generous data pool awaiting the manipulation of surveillance technologies. In this context, we believe that the impact of the pandemic on the exponential migration from the analog to the digital has been generally understudied.[1]

The pandemic has also highlighted the agency of national governments around the world in facilitating the proliferation of new and innovative surveillance tools. Even before COVID-19, the literature has been increasingly concerned with the fast-paced growth of digital surveillance techniques and capacities (DIAMOND 2019; FARRIES 2019, 2019; FRIEDEWALD ET AL. 2017; LEWIS 2014; MICHAELSEN 2020; PRIVACY INTERNATIONAL 2014; QIANG 2019; XU 2021). The pandemic has fast-forwarded the movement on this track. Many countries in the world developed digital tools to trace the contacts of infected individuals as well as to enforce quarantine measures (AMIT ET AL. 2020; CALVO – DETERDING – RYAN 2020; ECK – HATZ 2020; GOLINELLI ET AL. 2020; STEHLÍKOVÁ 2020; WHITELAW ET AL. 2020). In parallel, many observers continuously raise concerns regarding the breach of individual and collective privacy (EUROPEAN PARLIAMENT 2020; GIGA 2021; GREITENS 2020; RANISCH ET AL. 2020; SEKALALA ET AL. 2020).

Finally, the ability of governments to justify the wide-ranging employment of digital surveillance has been broadened due to the global public health

emergency. The pandemic provided the perfect ingredient for both democratic and authoritarian governments to frame digital surveillance as necessary for dodging an imminent public health crisis. Governments have combined different liberal and illiberal rhetorical elements to create a hegemonic discourse that justifies the prolonged use of digital surveillance. In the following, we provide anecdotal empirical evidence for all three transformations.

In our empirical exercise, we have reviewed reports prepared by the Global Digital Policy Incubator at Stanford University and zoomed in on instances of digital surveillance between July 2020 and September 2021.[2] Looking at the second and third waves of the global COVID-19 pandemic, we believe that digital surveillance is being continuously normalized across different regime types. First, it is being done by governments promoting digital tools and data collection techniques as pandemic counter-measures. Second, the mass migration to online platforms has provided previously unseen amounts of digital data that are vulnerable to varying forms of state and "outsourced" surveillance. In the sections below, we use evidence from around the globe to illustrate how these tendencies come together to form a self-enforcing vicious circle or "the long-term surveillance prescription."

AVAILABILITY OF DATA

Social media, mobile applications, and specialized software have enabled millions to continue interacting, and connecting to workplaces and study rooms throughout the ensuing waves of the global pandemic. At the same time, the shift to the digital amassed previously unseen amounts of data exposed to state and "outsourced" surveillance. What is more, the very structure of remote work and study encourages us to accept pervasive digital supervision, socializing workers and students for the "long-term prescription."

The heightened vulnerability to surveillance is best illustrated by evidence from authoritarian and autocratizing regimes. For instance, in June 2020, Zoom, the biggest video-conferencing platform to emerge in the wake of the pandemic, admitted that it had complied with Chinese government requests to block users from meetings commemorating the June 4th Tiananmen Square incident. According to Zoom, it identified and suspended four such meetings without providing *"any non-China-based user information or any meeting content to the Chinese government [...] other*

than a limited amount of user data concerning China-based attendees" (ZOOM 2020). Despite admitting fault, by identifying, suspending, and terminating host accounts Zoom effectively served as a surveillance arm of the Beijing regime. Similar examples of autocratic governments using domestic regulations to subject online platforms have abounded in the past years.[3] In addition, democratic governments have also found ways to capitalize on the expanding pool of digital data available for surveillance.

The surveillance industry has also fed on the increasing migration to the digital world during the COVID-19 pandemic. Clearview facial recognition software, trained on a database of billions of images scraped from social media platforms like Facebook, Instagram, LinkedIn, and Twitter, has been at the forefront of this industry. Using Clearview AI, as of February 2020, 88 law enforcement and government-affiliated agencies in 24 countries, including the U.S., Canada, the UAE, Saudi Arabia, Brazil, Australia, and several EU countries, had matched photos of suspects with samples scraped online (MAC ET AL. 2021). Though marketed as a tool for fighting child abuse, Clearview has been deemed unlawful in a few countries due to its incongruency with privacy regulations. For instance, Canada's data privacy commissioner ruled in February 2021 that Clearview had violated federal and provincial privacy laws and called the company to stop collecting and delete any scraped images and biometrics of Canadian citizens (MAC ET AL. 2021). However, recent reports reveal that law enforcement agencies around the world continue using the tool both with and without leadership oversight. For example, reports from different states in the U.S. have indicated that Clearview had been employed to identify and arrest protestors captured on CCTV cameras during the 2020 Black Lives Matter protests (KATE COX 2020).

Moreover, downloads of mobile applications have skyrocketed with the outbreak of COVID-19[4] and presented an additional entry point for "outsourced surveillance." As reported by Vice's Motherboard, the U.S. government has been harvesting location data from mobile applications used around the world, including the most popular Muslim-oriented apps (JOSEPH COX 2020). Exploiting a loophole in federal privacy regulations prohibiting the collection of location data without a warrant, X-mode, a third-party data broker, has been subcontracted to source data from original apps and forward it to government agencies (Express VPN). Some mobile applications

sending information to X-mode include Muslim Pro, which reminds users when to pray and indicates the direction of Mecca, the dating app Muslim Mingle, and some local social media apps widely used in Iran, Turkey, and Colombia. Targeting broader audiences, the X-mode network also includes weather, sports, dating, and home repair applications (JOSEPH COX 2020). In an interview, Joshua Anton, the founder and head of X-Mode, said the company tracks 25 million devices inside the United States every month, and 40 million more around the globe (CNN BUSINESS 2020). In December 2020, Apple and Google app stores announced that any application that would continue using tracking software would be removed. However, a 2021 research by ExpressVPN and the Defensive Lab Agency, found nearly 200 apps still sending information to X-Mode and 450 apps downloaded at least 1.7 billion times containing various location tracker software development kits (SDKs)[5] (EXPRESS VPN 2021; O'BRIEN 2021).

Finally, the pandemic has not only accelerated the usage of existing digital communication tools, but also facilitated the mass adoption of previously little-explored software solutions which pervasively monitor and amass pools of data on students and employees. Alongside the so-called "bossware" promoted by employers for "activity monitoring" of employees during remote work (CYPHERS – GULLO 2020), proctoring software is the most vivid illustration of how COVID-19 has facilitated the normalization of everyday surveillance. Programs like ProctorU, which oversee students taking online exams and doing homework, have long drawn criticism from human rights activists, who point to the discriminatory nature of these systems. Students of colour, students with learning disabilities, and low-income groups are more likely to be subjected to errors of proctoring algorithms (KELLEY 2020). With the increasing adoption of proctoring software in schools and universities during the pandemic, concerns about the security of vast amounts of student data have also arisen. Alongside leveraging of student data for commercial purposes, breaches of proctoring databases and subsequent data dumps are among the most likely risks. In 2020, over 440,000 user records were leaked from the ProctorU database to a hacker forum, including email addresses, full names, addresses, phone numbers, hashed passwords, the affiliated organizations, and other information (KELLEY 2020).

All in all, with the growth of the digital data pool in the past years, the individual susceptibility to digital surveillance only increases. What is

more, in the "new normal" workers and students have a choice of forfeiting their data and subjecting themselves to surveillance by proctoring and various worker efficiency applications or facing professional and academic consequences. Thus, in a slow but steady manner, we are socialized into "the long-term prescription."

TOOLS FOR SURVEILLANCE

The ensuing waves of the pandemic have also served as an excuse for governments around the world to develop long-term surveillance solutions and strike long-term data sharing agreements with "surveillance capitalists."[6] China, where digital COVID-19 response measures have been particularly embraced by the communist regime, has been among the frontrunners in this regard.

As early as May 2020, officials in the eastern Chinese city of Hangzhou announced plans to create a permanent version of the surveillance application developed by the home-grown tech giant Alibaba. The current health app works like a traffic light, where red indicates that a person poses a public health risk, and green allows individuals to access public facilities (KHARPAL 2020). The extended version of the application could have also been linked to electronic medical records and taken into consideration lifestyle choices such as drinking, smoking, and sleeping. Though the Hangzhou government backed down from its proposal after criticism for its alleged disrespect for individual privacy, it has already connected its health code to electronic health and social security cards. The governments in Shanghai and Guangzhou have also followed suit and integrated local health codes with electronic identification, health insurance, and users' bank accounts (CONG 2021), thus making the digital surveillance in China even more comprehensive.

Private entities in western democracies, very much like the Chinese Alibaba, have also seized the chance to offer technical expertise to the public sector and gain access to pools of invaluable individual data. The ensuing states of emergency and rollouts of mass vaccinations have turned into "the hour of surveillance capitalists". This is because governments have found themselves on the losing end, reliant on tech corporations and unable to lobby for appropriate privacy safeguards. As reports vividly illustrate, Google's free smartphone software used by countries around the

world as a blueprint for contact-tracing applications was called into question in June 2020. Despite assurances of data security, governments were surprised to learn that location-tracking must be active for the software to work with Android phones, allowing Google to determine and track the location of millions. Numerous European governments voiced their concerns; however, without feasible alternatives, none said that they will stop using the blueprint (SINGER 2020).

The struggle over access to patients' data has been probably the most pronounced in the United Kingdom. In the light of the COVID-19 emergency, tech companies saw an opening for gaining access to national health data, which would serve as real-life lab material for training commercial artificial intelligence models. The now published Google contract with the National Health Service (NHS) signed in March 2020 hints at the data-for-expertise exchange as it promised free *"technical, advisory and other support"* to the NHSX lab for the development of a data platform to streamline the public health response to COVID-19. Moreover, the Google-owned DeepMind's co-founder Mustafa Suleyman was also reportedly consulting the NHS on how to collect patient data in a *pro bono* advisory capacity (LOMAS 2020). Another company which benefited from data-sharing deals with the UK government, is Palantir Technologies, known for providing analytics and data to law enforcement, military, and intelligence agencies around the world. After signing the contract stipulating that it would support the NHS data platform, Palantir Technologies recorded £22 million in profits despite reporting a loss the previous year (WILLIAMS 2021).

After "No Palantir in our NHS" activists from openDemocracy and Foxglove sued the government in February 2021 for an *"'unprecedented' transfer of patients' information,"* the court ordered not to extend Palantir's contract beyond the pandemic without public consultation. In September 2021, the government ended one of its data-sharing contracts with Palantir by *"seeking to move away from reliance on third-party data analytics platforms"* (BYCHAWSKI 2021). Nonetheless, another consulting agreement with Palantir for COVID-19 data analysis will continue running until December 2022. Furthermore, in May 2021, the NHS announced new plans to scrape nearly 55 million medical records, including information on mental and sexual health, criminal records, and abuse, into a database to share with third parties (MURGIA 2021). Despite promises that the scraped

data will be "gatekept," the tainted NHS track record raises red flags about yet another opening for "surveillance capitalists" in the United Kingdom.

In sum, just as citizens around the world become more dependent on social media, mobile applications, and online platforms in their everyday communication, so have governments grown increasingly reliant on tech corporations for streamlining digital pandemic counter-measures. In turn, economic profit is overtaking political control as the key variable in the global pandemic surveillance equation.

HEGEMONIC JUSTIFICATIONS

Finally, the ability of governments to justify new data-sharing parnerships with private surveillance actors and the wide-ranging employment of digital surveillance have been broadened during the ensuing waves of COVID-19. With COVID-19, both democracies and autocracies have found the perfect rhetorical ingredient to politically justify prolonged surveillance.

In October 2020, France rebranded its contact-tracing application StopCovid and reframed it as a liberal, inclusive, and "open-sourced" pandemic counter-measure, looking to boost its small user base (DILLET 2020). EveryoneAgainstCovid (*TousAntiCovid*), the new name of the app, echoes the liberal rhetoric that surrounded the launch of Singapore's 'TraceTogether,' one of the most successful national contact tracing applications worldwide. By early 2021, nearly 80 percent of Singaporeans were using TraceTogether on their smartphones or had connected it to wearable Bluetooth tokens for accessing workplaces and public facilities (ILLMER 2021).

However, despite a lot of energy being invested into encouraging the use of the application in early 2020, presenting it as being developed in a decentralized manner and highlighting its internationally-endorsed privacy safeguards (MAATI – ŠVEDKAUSKAS 2020: 17–20), the Singaporean government has gone back on its promises. Officials have switched from assurances that the collected data would only be used for contact tracing, arguing that privacy regulations could and should be overruled. In January 2021, Minister for Foreign Affairs Balakrishnan claimed that data collected through TraceTogether is no different from *"other forms of sensitive data like phone or banking records,"* the privacy of which should be overruled because *"police*

must be given the tools to bring criminals to justice and protect the safety and security of all Singaporeans" (BALAKRISHNAN 2021). The shift to a "harder," more securitized framing of digital surveillance in Singapore and the reverse rhetorical trajectory in France follow our prediction that more blurring of the line between liberal and illiberal rhetoric is to be expected with the new waves of the pandemic (MAATI – ŠVEDKAUSKAS 2020).

Though national rhetorical and policy trajectories vary, it is evident that at the time of writing, the pandemic has become a lasting rhetorical symbol in the vocabularies of governments and tech corporations. Mixing liberal and illiberal arguments, these actors produce hegemonic discourses necessitating permanent digital public-health-surveillance, as in China, or repeated harvests of patients' data, as in the UK.

TAKEAWAYS

Taken together, the three realms of data, tools and justifications, through which the pandemic facilitated the proliferation of digital surveillance, point towards two broad conclusions. The first is that digital surveillance is here to stay. As we have hypothesized elsewhere, governments mixing liberal and illiberal rhetorical elements are already refitting their justifications for digital surveillance in a way that outlives the COVID-19 emergency. The illiberal tone and hegemonic discourses necessitating long-term digital surveillance are especially concerning since public health experts increasingly agree that the pandemic has entered a long-lasting "endemic stage" (PHILLIPS 2021).

The second conclusion is that we might be on the verge of a dangerous normalization of digital surveillance. This results not only from internalizing government discourse and practices (FOUCAULT 2007), but also from the emergency discourse that the pandemic readily provides (CSERNATONI 2020). The COVID-19 pandemic offers the perfect ingredients for such a normalization: It motivated a voluntary though necessary migration to the digital world, creating large pools of digital data that are amassed through teleconferencing platforms, social media, and mobile applications. This provided a corporate and governmental motivation to develop new tools of surveillance for harvesting these sources. The pandemic has also threatened people and governments enough so that they would accept digital surveillance as necessary even if it threatens privacy. In the

background of a global public health crisis, we have also seen the *de facto* acceptance of a new type of surveillance medium. With so-called "bossware" and proctoring applications deployed for remote work and study, everyday surveillance is yet more comprehensive.

In the light of our anecdotal evidence, we believe that future research should not only focus on digital surveillance tools and the discourses surrounding them. Following Phillip Lipscy (2020), we think that scholars should also rethink public health crises as openings for increasing the availability of digital data, a necessary condition for the future proliferation of the digital surveillance industry. Research should also focus on better understanding the motivations of and complex relationships between the state agencies, corporate actors, and sub-contractors behind digital surveillance. Since these actors exist and operate transnationally and across regime types and socio-economic orders, future investigations should adopt a multitude of approaches to uncover the full complexity of this surveillance ecosystem. By taking this course, the academic community could assist in the ensuing struggle against the unnecessary long-term deployment of digital surveillance.

ENDNOTES

1 For a testimony on how relevant this could be see Ronald Deibert's testimony in front of the House of Commons (Kenyon 2020).

2 See Freeman Spogli Institute of International Studies (2021).

3 For the most vivid illustrations, see Krishnan (2021) on India, Coşkun (2021) on Turkey, and Rumyantsev (2021) on Russia.

4 In the U.S. alone, education, remote work and grocery delivery applications respectively saw 1,087%, 1,457% and 322 % increases in their download numbers in the first half of March 2020 (Statista 2021).

5 For the list of SDKs and "infected" apps, see O'Brien – Onfroy (2021).

6 For more on the concept of surveillance capitalism, see Zuboff (2019).

REFERENCES

A Amit, Moran – Kimhi, Heli – Bader, Tarif – Chen, Jacob – Glassberg, Elon – Benov, Avi (2020): Mass-Surveillance Technologies to Fight Coronavirus Spread: The Case of Israel. *Nature Medicine*, Vol. 26, No. 8, pp. 1167–1169.

B Balakrishnan, Vivian (2021): Clarification on the Usage of TraceTogether, <https://www.smartnation.gov.sg/whats-new/speeches clarification-on-the-usage-of-tracetogether-data-by-dr-vivian-balakrishnan>.

Bychawski, Adam (2021): UK Health Department Ends Data Deal with 'Spy Tech' Company Palantir. *openDemocracy*, <https://www.opendemocracy.net/en/opendemocracyuk/uk-health-department-ends-data-deal-with-spy-tech-company-palantir/?fbclid=IwAR0cJI3_LP2MT49-JsEJO88DbDyRg8tlQS3VtBthkrVApPhPbx0AA97VfhI>.

C

Calvo, Rafael A. – Deterding, Sebastian – Ryan, Richard M. (2020): Health Surveillance during COVID-19 Pandemic. *BMJ*, Vol. 369, pp. 1–2, <doi:10.1136/bmj.m1373>.

CNN Bussiness (2020): This Company Tracks Millions of Devices Worldwide. Could It Help Fight COVID-19? *CNN*, <https://www.cnn.com/videos/business/2020/04/03/coronavirus-device-tracking-xmode-pandemic-orig.cnn-business>.

Cong, Wanshu (2021): From Pandemic Control to Data-Driven Governance: The Case of China's Health Code. *Frontiers in Political Science*, Vol. 3, No. 8, <doi:10.3389/fpos.2021.627959>.

Coşkun, Gülçin Balamir (2021): Turkey's New Internet Law and Its Effects on Freedom of Media. *Reset Dialogues*, <https://www.resetdoc.org/story/turkey-internet-law-freedom-media/>.

Cox, Joseph (2020): How the U.S. Military Buys Location Data from Ordinary Apps. *Vice*, <https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>.

Cox, Kate (2020): Cops in Miami, NYC Arrest Protesters from Facial Recognition Matches. *Ars Technica*, <https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/>.

Csernatoni, Raluca (2020): Coronavirus Tracking Apps: Normalizing Surveillance during States of Emergency. *Carnegie Europe*, <https://carnegieeurope.eu/2020/10/05/coronavirus-tracking-apps-normalizing-surveillance-during-states-of-emergency-pub-83039>.

Cyphers, Bennett – Gullo, Karen (2020): Inside the Invasive, Secretive "Bossware" Tracking Workers. *Electronic Frontier Foundation*, <https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers>.

D

Dillet, Romain (2020): France Rebrands Contact-Tracing App in an Effort to Boost Downloads. *TechCrunch*, <https://social.techcrunch.com/2020/10/22/france-rebrands-contact-tracing-app-in-an-effort-to-boost-downloads/>.

E

Eck, Kristine – Hatz, Sophia (2020): State Surveillance and the COVID-19 Crisis. *Journal of Human Rights*, Vol. 19, No. 5, pp. 603–612, <doi:10.1080/14754835.2020.1816163>.

European Parliament (2020): COVID-19: Digital Surveillance, Borders and Human Rights. European Parliament, <https://www.europarl.europa.eu/news/en/headlines/society/20200618STO81514/COVID-19-digital-surveillance-borders-and-human-rights>.

ExpressVPN (2021): ExpressVPN's Research on Smartphone Location Tracking. *ExpressVPN*, <https://www.expressvpn.com/digital-security-lab/investigation-xoth>.

F

Foucault, Michel (2007): *Discipline and Punish: The Birth of the Prison*. Duke University Press.

Freeman Spogli Institute of International Studies (2021): Global Digital Rights Digest. *Cyber Policy Center*, <https://cyber.fsi.stanford.edu/gdpi/content/global-digital-rights-digest>.

Friedewald, Michael – Burgess, J. Peter – Čas, Johann – Bellanova, Rocco – Peissl, Walter (2017): *Surveillance, Privacy and Security: Citizens' Perspectives*. Taylor & Francis.

G

GIGA (2021): Digitale Überwachung und die Bedrohung ziviler Freiheiten in Indien, <https://www.giga-hamburg.de/de/publikationen/24697659-digital-surveillance-threat-civil-liberties-india/>.

Golinelli, Davide – Boetto, Erik – Carullo, Gherardo – Nuzzolese, Andrea Giovanni – Landini, Maria Paola – Fantini, Maria Pia (2020): How the COVID-19 Pandemic Is Favoring the Adoption of Digital Technologies in Healthcare: A Literature Review. *MedRxiv*.

Greitens, Sheena Chestnut (2020): Surveillance, Security, and Liberal Democracy in the Post-COVID World. *International Organization*, Vol. 74, No. S1, pp. E169–E190.

I

Illmer, Andreas (2021): Singapore Reveals Covid Privacy Data Available to Police. *BBC News*, 5. 1. 2021, <https://www.bbc.com/news/world-asia-55541001>.

K

Kelley, Oliver (2020): Proctoring Apps Subject Students to Unnecessary Surveillance. *Electronic Frontier Foundation*, <https://www.eff.org/deeplinks/2020/08/proctoring-apps-subject-students-unnecessary-surveillance>.

Kenyon, Miles (2020): Ronald Deibert Delivers Testimony to the House of Commons on Parliamentary Duties and the COVID-19 Pandemic. *The Citizen Lab*, <https://citizenlab.ca/2020/04/ronald-deibert-delivers-testimony-to-the-house-of-commons-on-parliamentary-duties-and-the-COVID-19-pandemic/>.

Kharpal, Arjun (2020): Chinese City Proposes Permanent Health Tracking with a Score Based on Drinking and Exercise Habits. *CNBC*, 26. 5. 2020, <https://www.cnbc.com/2020/05/26/chinese-city-hangzhou-proposes-permanent-health-tracking-app-with-score.html>.

Khrishnan, Murali (2021): Why are Twitter and WhatsApp Miffed with Indian Authorities? *Deutsche Welle*, <https://www.dw.com/en/india-social-media-conflict/a-57702394>.

Kosinski, Michal – Stillwell, David – Graepel, Thore (2013): Private Traits and Attributes Are Predictable from Digital Records of Human Behavior. *Proceedings of the National Academy of Sciences*, Vol. 110, No. 15, pp. 5802–5805.

Kuner, Christopher – Cate, Fred H. – Millard, Christopher – Svantesson, Dan Jerker B. (2012): The Challenge of 'Big Data' for Data Protection. *International Data Privacy Law*, Vol. 2, No. 2, pp. 47–49, <doi:10.1093/idpl/ips003>.

L

Lipscy, Phillip Y. (2020): COVID-19 and the Politics of Crisis. *International Organization*, Vol. 74, No. S1, pp. E98–E127.

Lomas, Natasha (2020): UK's COVID-19 Health Data Contracts with Google and Palantir Finally Emerge. *TechCrunch*, <https://social.techcrunch.com/2020/06/05/uks-COVID-19-health-data-contracts-with-google-and-palantir-finally-emerge/>.

M

Maati, Ahmed – Švedkauskas, Žilvinas (2020): Framing the Pandemic and the Rise of the Digital Surveillance State. *Mezinárodní vztahy*, Vol. 55, No. 4, pp. 48–71.

Mac, Ryan – Haskins, Caroline – Pequeno IV, Antonio (2021): Clearview AI Offered Free Facial Recognition Trials to Police All around the World. *BuzzFeed News*, <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table>.

Murgia, Madhumita (2021): England's NHS Plans to Share Patient Records with Third Parties. *Financial Times*, 26. 5. 2021, <https://www.ft.com/content/9fee812f-6975-49ce-915c-aeb25d3dd748>.

O

O'Brien, Sean (2021): We Found Location Trackers in 450 Apps. *ExpressVPN Blog*, <https://www.expressvpn.com/blog/digital-security-lab-location-trackers-smartphone-apps-research/>.

O'Brien, Sean – Onfroy, Esther (2021): Investigation Xoth: Location Trackers. *GitHub*, <https://github.com/expressvpn/xoth_location_tracker_investigation>.

P

Phillips, Nicky (2021): The Coronavirus Is Here to Stay-Here's What That Means. *Nature*, Vol. 590, No. 7846, pp. 382–384.

R

Ranisch, Robert – Nijsingh, Niels – Ballantyne, Angela – van Bergen, Anne – Buyx, Alena – Friedrich, Orsolya – Hendl, Tereza – Marckmann, Georg – Munthe, Christian – Wild, Verina (2020): Digital Contact Tracing and Exposure Notification: Ethical Guidance for Trustworthy Pandemic Management. *Ethics and Information Technology*, pp. 1–10.

Rumyanstev, Stanislav (2021): Be My Guest – Internet Companies Must Go Local in Russia. *Gorodissky*, <https://www.mondaq.com/russianfederation/corporate-and-company-law/1093534/be-my-guest-internet-companies-must-go-local-in-russia>.

S

Sekalala, Sharifah – Dagron, Stéphanie – Forman, Lisa – Meier, Benjamin Mason (2020): Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights*, Vol. 22, No. 2, p. 7.

Singer, Natasha (2020): Google Promises Privacy with Virus App but Can Still Collect Location Data. *The New York Times*, 20. 7. 2020, <https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html>.

Statista (2021): Increase in Downloads of COVID-19 Impacted Apps in the United States between March 2 and March 16, 2020, by Category. *Statista Research Department*, <https://www.statista.com/statistics/1108469/coronavirus-impact-app-downloads-by-category-usa/>.

Stehlíková, Jana (2021): The Corona Crisis, Data Protection and Tracking Apps in the EU: The Czech and Austrian COVID-19 Mobile Phone Apps in the Battle against the Virus. *Mezinárodní vztahy*, Vol. 56, No. 1, pp. 35–67.

Surber, Regina Sibylle (2020): Corona Pan (Dem) Ic: Gateway to Global Surveillance. *Ethics and Information Technology*, pp. 1–10.

W

Whitelaw, Sera – Mamas, Mamas A. – Topol, Eric – Van Spall, Harriette GC (2020): Applications of Digital Technology in COVID-19 Pandemic Planning and Response. *The Lancet Digital Health*.

Williams, Martin (2021): 'Spy Tech' Firm Palantir Made £22m Profit after NHS Data Deal. *openDemocracy*, <https://www.opendemocracy.net/en/dark-money-investigations/spy-tech-firm-palantir-made–22m-profit-after-nhs-data-deal/>.

X

Xu, Xu (2021): To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance. *American Journal of Political Science*, Vol. 65, No. 2, pp. 309–325.

Z

Zoom (2020): Improving Our Policies as We Continue to Enable Global Collaboration. *Zoom Blog*, <https://blog.zoom.us/improving-our-policies-as-we-continue-to-enable-global-collaboration/>.

Zuboff, Shoshana (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.

Zwitter, Andrej J. – Hadfield, Amelia (2014): Governing Big Data. *Politics and Governance*, Vol. 2, No. 1, pp. 1–3.

AUTHOR BIOGRAPHY

Žilvinas Švedkauskas is a PhD candidate at Eberhard-Karls-Universität Tübingen and a Bucerius Fellow of the "Trajectories of Change" programme at ZEIT-Stiftung Ebelin und Gerd Bucerius, specializing in comparative politics and democratization. His research focus lies in constitutional change and digital transformation in Africa, the Middle East, and the post-Soviet space. Žilvinas holds a joint MA degree in Comparative & Middle East Politics from Tübingen University and the American University in Cairo. Since 2021 he is also a board member at the Euromed Young Researchers Lab hosted by EuroMeSCo, the leading network of think tanks and research centres in the Euro-Mediterranean region.

Ahmed Maati is a PhD candidate, a research associate, and a junior lecturer at the department of Political Science at Eberhard-Karls-Universität Tübingen. His research foci include identity and comparative politics of the Middle East, theories of the state, and digital politics. Maati holds a Master's degree in "Comparative and Middle East Politics and Society" (CMEPS) from the joint program between the American University in Cairo and the Eberhard-Karls-University of Tübingen.