Crises, Creep, and the Surveillance State

*Michal Lavi**

COVID-19 started in December 2019 in China and spread rapidly and globally. This virus led to a public health emergency of international concern as a threat to the public's health and safety.

The speed of virus infections depended on various aspects of an individual's social network position. Individuals with more friends, or those who were more central in the network, caught the virus sooner. In the beginning of the outbreak, governments thought that tracking human networks and collecting information on the movements of individuals would allow governments to utilize the information for mitigating the spread of the virus. They believed that mass surveillance would help health authorities identify the contacts an infected person had and warn such contacts, thus reducing the likelihood for them to infect others. By gaining such data, governments believed they could focus their efforts to block the spread of the virus and even predict where the next cluster of infections would emerge.

In general, information and data-driven models have the potential to promote health. Data is knowledge; however, knowledge is power that can grant governments control over citizens, leading to a slippery slope that could creep beyond health considerations and undermine the infrastructure of civil rights. The result could be constant surveillance instead of privacy, self-censorship

* Ph.D. (Law). Research Fellow, Hadar Jabotinsky Center for Interdisciplinary research of Crises Financial Markets, and Technology. Special thanks are due to Luca Provenzano, Rachel Forman, Michael J. Giordano, Abigail Grise, Giuseppe Natale, Jr., Alexis E. Pinzon, Andrew Foltiny, Claire M. Midili, Colin Dennis, Elizabeth Vignuolo, Tsz Chung (Alec) Wong, Bobbi M. Taylor, Gineen K. Abuali, Haley Giaramita, James Finnegan, Andrew R. Simon, Thomas Kingeter, Joshua Murphy, Kevin A. Wrobel, Lance Fischer, Melanie Andreas, Lauren Rutkowski, Steven Fasciale, Jiyoung Won, and their colleagues on the *Seton Hall Law Review* staff for remarkable comments and feedback throughout the editing process and for outstanding editorial work that profoundly improved the quality of this Article. I dedicate this Article to the memory of my mother—Aviva Lavi—who died suddenly and unexpectedly. My mother taught me to love knowledge and gave me the strength to pursue it. She will always be loved, remembered, and dearly missed.

instead of freedom of expression, suspicion instead of trust, and the rise of the surveillance state instead of democracy.

This Article outlines a taxonomy of surveillance data-driven practices that were used to combat the virus. It describes the potential benefits of such models while addressing the dangers created by such mass surveillance. Additionally, this Article demonstrates that surveillance practices can compromise privacy, infringe on free expression and equality without safeguards or due process, and lead to abuse of power. Finally, it establishes how such practices can erode democracy and creep beyond combating a virus.

This Article argues that even in times of crisis, we can have both health and human rights. It warns against surveillance creep and advocates for a privacy-by-design approach in such models, including anonymization of personal information. This Article further proposes safeguards including transparency, impact assessments of data protections and algorithms, fiduciary duties, oversight, and due process. Finally, this Article addresses practices of long-term invasive surveillance that should be ruled out altogether and rejected at all costs. COVID-19 is a test case that demonstrates the consequences of mass surveillance without warrants or adequate regulatory prerequisites, and the misuse of personal data. Thus, this Article warns that the creep of mass surveillance can lead to the rise of the surveillance state.

I. INTRODUCTION

"We must be vigilant about our community's health—and rights as well." [1]

The COVID-19 virus that began in December 2019 spread rapidly worldwide.[2] This virus led to a global health emergency as it infected

---

[1] Kari Bode, *COVID-19 Could Provide Cover for Domestic Surveillance Expansion*, VICE: MOTHERBOARD (Mar. 16, 2020, 7:15 PM), https://www.vice.com/en/article/884ew5/covid-19-could-provide-cover-for-domestic-surveillance-expansion (quoting Telephone Interview with Gaurav Laroia, Senior Policy Counsel and Privacy Expert, Free Press).

[2] Khadijah Abid et al., *Progress of COVID-19 Epidemic in Pakistan*, 32 ASIA PAC. J. PUB. HEALTH 154, 154 (2020) ("The outbreak of coronavirus initiated as pneumonia of unknown cause in December 2019 in Wuhan, China, which has been now spreading rapidly out of Wuhan to other countries.").

millions of people, burdened healthcare facilities,[3] and governments perceived it as a threat to public health and safety.[4] Humankind faced a global crisis, as the steps taken to combat the virus affected every aspect of life. International borders closed, schools and universities shut down, governments prohibited public gatherings, airlines abolished flights, and economies crashed.[5] The approaches taken to combat the virus will likely influence healthcare systems, economies, and our cultures for years to come.[6]

Several governments and private companies used practices of mass collection of data,[7] as well as "health-system-supportive technology solutions, including smartphone apps and other digital tools."[8] "The proliferation of smart devices and the development in digital communication has led to sophisticated methods" of surveillance, gathering location data, and other health-related data.[9] Governments believed this data would allow them to target those who were suspected of having caught the virus and monitor adherence to

---

[3] *See* Alfonso J. Rodriguez-Morales et al., *Clinical, Laboratory and Imaging Features of COVID-19: A Systematic Review and Meta-Analysis*, 34 TRAVEL MED. & INFECTIOUS DISEASE 1–2 (2020).

[4] The World Health Organization (WHO) announced the virus to be a pandemic. *See* Philippa Roxby, *Coronavirus Confirmed as a Pandemic by World Health Organization*, BBC: WORLD (Mar. 11, 2020), https://www.bbc.com/news/world-51839944. Additionally, the United States declared it a state of emergency. Charlie Savage, *Trump Declared an Emergency Over Coronavirus. Here's What It Can Do*, N.Y. TIMES (Mar. 13, 2020), https://www.nytimes.com/2020/03/13/us/politics/coronavirus-national-emergency.html; Toni M. Massaro et al., *Pandemics and the Constitution*, 2022 U. ILL. L. REV. 229, 230 (2022).

[5] *See* Adam Chilton et al., *Support for Restricting Liberty for Safety: Evidence During the COVID-19 Pandemic from the United States, Japan, and Israel*; Hadar Y. Jabotinsky & Roee Sarel, *How Crisis Affects Crypto: Coronavirus as a Test Case*, 74 HASTINGS L.J. 2–3 (forthcoming 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557929.

[6] *See* Yuval Noah Harari, *The World After Coronavirus*, FIN. TIMES: LIFE & ARTS (Mar. 20, 2020), https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

[7] *See* Laura Bradford et al., *COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes*, 7 J.L. & BIOSCIENCES 1–2 (2020) (referring to Google and Apple recently announcing their intention to build interfaces to allow Bluetooth contact tracking using Android and iPhone devices); Press Release, Apple, Apple and Google Partner on COVID-19 Contact Tracing Technology (Apr. 10, 2020), https://www.apple.com/uk/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology.

[8] JEFFREY P. KAHN, DIGITAL CONTACT TRACING FOR PANDEMIC RESPONSE: ETHICS AND GOVERNANCE GUIDANCE 1 (2020).

[9] Antonio Clim et al., *Big Data in Home Healthcare: A New Frontier in Personalized Medicine. Medical Emergency Services and Prediction of Hypertension Risks*, 12 INT'L J. HEALTHCARE MGMT. 241, 241 (2019).

quarantine orders.[10] It was assumed that such data could be used to predict which urban areas were at risk.[11]

Governments and private companies believed that data about individuals and their connections could be used to predict risks of infection from specific individuals.[12] For example, "[o]n March 13, 2020, Alphabet's life sciences division, Verily, announced it was developing a website to screen people for symptoms" of the virus.[13] "After accessing the system, which required an active Google Account, each user [was] assigned a COVID-19 risk score."[14]

Mass surveillance and data-driven practices might make it possible to facilitate early detection of viruses, achieve better diagnoses, map the diffusion of the virus, and even predict areas of outbreak before they materialize. Thus, a small Canadian Artificial Intelligence (AI) startup, BlueDot, "spotted COVID-19 nine days before the [World Health Organization] alerted people to the emergence of [the virus]."[15] Data-driven practices also allowed governments to identify potential urban areas of outbreak. For instance, as part of a COVID-19 research project which analyzed the spread of the virus, Facebook asked users whether they had been infected with the virus in order to generate "heat maps" of the outbreak and make new categories of data available to scientists who specialize in studying epidemics through a new program called Disease Prevention Maps.[16] This initiative involved

---

[10] Urs Gasser et al., *Digital Tools Against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid*, 2 LANCET DIGIT. HEALTH e425 (2020) https://www.sciencedirect.com/science/article/pii/S2589750020301370 ("These technologies can provide a mechanism of ensuring that infected individuals are isolated from other individuals. Examples include Taiwan's Electronic Fence application that tracks quarantined overseas arrivals using mobile phone data.").

[11] Alexander Martin, *Coronavirus: Facebook to Produce 'Heat Maps' of COVID-19 Infections*, SKY NEWS: SCI. & TECH. (Apr. 7, 2020, 2:02 PM), https://news.sky.com/story/coronavirus-facebook-to-produce-heat-maps-of-covid-19-infections-11969776.

[12] *See, e.g.*, Refaella Goichman, *Israeli Defense Ministry Teaming Up With Spyware Firm NSO to Fight Coronavirus*, HAARETZ (Mar. 29, 2020), https://www.haaretz.com/israel-news/2020-03-29/ty-article/.premium/israeli-defense-chief-plans-to-employ-spyware-firm-nso-in-fight-against-coronavirus/0000017f-db5f-d856-a37f-ffdf06810000.

[13] Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence,* 11 U.C. IRVINE L. REV. 995, 1004 (2021).

[14] *Id.*

[15] *See* Anindya Ghose & D. Daniel Sokol, *Unlocking Platform Technology to Combat Health Pandemics*, YALE J. REGUL. (Mar. 18, 2020), https://www.yalejreg.com/nc/unlocking-platform-technology-to-combat-health-pandemics-by-anindya-ghose-and-d-daniel-sokol.

[16] Martin, *supra* note 11.

sharing aggregated location data with partners in forty countries.[17] Such a program would allow cooperation between countries.[18]

Data can be used to reduce the spread of the virus, and some believe it can break chains of infection.[19] As data suggests, a substantial proportion of transmission occurs between individuals before symptoms appear.[20] As such, it was proposed that people who had contact with carriers of the virus should be isolated from others.[21] But how will one know whether he had direct contact with an individual who was infected? Data from smartphones, digital platforms, and related technological ecosystems can be key to such knowledge.[22]

Mass surveillance and data-driven tools, however, infringe on human rights and civil liberties such as privacy and freedom of expression. Furthermore, individuals are not aware of the types of data that states collect on them without their consent, how such data transfers between authorities, and the ways authorities use it. These methods provide neither transparency nor due process, and oversight is insufficient. Without safeguards, a dangerous surveillance creep can take place.[23] States might collect and analyze personal information in situations that are not emergencies. Moreover, some states use national security agencies, instead of health agencies, to conduct surveillance. In a related context, the Court of Justice of the European Union in *La Quadrature du Net v. Premier Ministre* ruled that bulk data collection by European Union national agencies was illegal; however, the court allowed for an exception in cases of serious threat to national

---

[17] *Id.*

[18] *See id.*

[19] Sofia K. Mettler et. al, *Diagnostic Serial Interval as a Novel Indicator for Contact Tracing Effectiveness Exemplified with the SARS-CoV-2/COVID-19 Outbreak in South Korea*, 99 INT'L J. INFECTIOUS DISEASES 347 (2020) (claiming that "a well-functioning contact tracing system leads to shorter diagnostic serial intervals, which can, in turn, contribute to breaking chains of infections").

[20] KAHN, *supra* note 8, at 14.

[21] Chandini Raina MacIntyre, *Case Isolation, Contact Tracing, and Physical Distancing are Pillars of COVID-19* Pandemic Control, not Optional Choices, 20 LANCET: INFECTIOUS DISEASES 1105 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7834806/pdf/main.pdf.

[22] *See* Ghose & Sokol, *supra* note 15.

[23] *See* Matthew Tokson & Ari Ezra Waldman, *Social Norms in Fourth Amendment Law*, 120 MICH. L. REV. 265, 271 (2021) ("State and local governments [have recently] deployed industry-designed contact tracing apps to monitor COVID-19 outbreaks, with little infrastructure in place to guard against government use of the apps' data for surveillance purposes.").

security.[24] Recently, in the Grand Chamber of the European Court of Human Rights (ECtHR) case of *Big Brother Watch v. United Kingdom*, the court also ruled that mass data interception violated the right to privacy,[25] rejecting the regime of bulk collection and interception, and holding that the Regulation of Investigatory Powers Act 2000 (RIPA) was incompatible with Articles 8[26] and 10 of the European Convention on Human Rights.[27] "The ruling is particularly relevant now as national governments are increasingly relying on intrusive methods of data collection and contact tracing to prevent the spread of COVID-19."[28] It can be argued, however, that even though the ECtHR rejected this regime in the context of national security, the result might have been different in the context of health.

Moreover, governments around the world conduct mass surveillance on citizens and develop emergency regulations and exceptions in the public health context. The term "police state" is now becoming relevant not only to authoritarian regimes, but also to democracies.[29]

---

[24] *See generally* Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Ordre des Barreaux Francophones et Germanophone v. Premier Ministre, ECLI:EU:C:2020:791 (Oct. 6, 2020).

[25] *Big Brother Watch v. United Kingdom,* App Nos. 58170/13, 62322/14, 24960/15, ¶¶ 522, 528 (May 25, 2021), https://hudoc.echr.coe.int/eng?i=001-210077; *see also* David Heaton, *Grand Chamber Confirms UK Secret Surveillance Regime Unlawful in Big Brother Watch v United Kingdom*, BRICK CT. CHAMBERS: NEWS & EVENTS (May 26, 2021), https://www.brickcourt.co.uk/news/detail/grand-chamber-confirms-uk-secret-surveillance-regime-unlawful-in-big-brother-watch-v-united-kingdom; Asaf Lubin, Introductory Note, *Big Brother Watch v. United Kingdom (Eur, Ct, H.R.Grand Chamber)*, 61 INT'L LEGAL MATERIALS 605 (2022).

[26] *Big Brother Watch*, at ¶¶ 425–27.

[27] *Id.* at ¶¶ 456–58 ("[I]n view both of these weakness, and those identified by the Court in its consideration of the complaint under Article 8 of the Convention, it finds that there has also been a breach of Article 10 of the Convention by virtue of the operation of the section 8(4) regime.").

[28] Monika Zalnieriute, *Big Brother Watch and Others v. The United Kingdom*, 116 AM. J. INT'L L. 585, 586 (2022).

[29] Limor Shmerling Magazanik, *Use of Digital Means to Fight the Coronavirus*, ISR. TECH. POL'Y INST. (Mar. 16, 2020), https://techpolicy.org.il/blog/use-of-digital-means-to-fight-the-coronavirus ("In grappling with the COVID-19 pandemic, humanity has many more tools than it ever had. These may come in handy in overcoming the disease as a significantly lower loss of human lives. Nonetheless, we must be cautious, responsive, and proportionate in employing these measures. In the absence of independent checks and balances, we risk letting in one of the biggest threats to democracy: a Police State.").

"In the digital age, privacy against the state remains an essential part of political freedom."[30] The Fourth Amendment to the United States Constitution protects "against unreasonable searches and seizures," including cell phone site location data.[31] In most cases, reasonableness requires that the government have probable cause that justifies granting a warrant before conducting a search; however, "warrants are not required when 'exigent circumstances' make getting them unfeasible."[32] Any disease surveillance program is likely to be evaluated under the Fourth Amendment's "special needs doctrine"[33] (also called the "administrative search doctrine") by which courts sometimes permit warrantless surveillance with less than probable cause. Such a search might occur if getting a warrant would be impracticable, the search is aimed at something other than a traditional law enforcement purpose, or the search is altogether reasonable.[34] When courts broadly deem all types of state surveillance and data collection reasonable, or allow warrantless surveillance, under special needs programs, however, there may be grave consequences to civil liberties. Unfortunately, the virus was used to permit warrantless mass surveillance and "normalise the development of mass surveillance tools in countries that have so far rejected them."[35]

---

[30] NEIL RICHARDS, WHY PRIVACY MATTERS 133 (2022).

[31] Carpenter v. United States, 138 S. Ct. 2206, 2206–07 (2018); Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1792 (2022).

[32] Alan Z. Rozenshtein, *Disease Surveillance and the Fourth Amendment*, LAWFARE (Apr. 7, 2020, 1:54 PM), https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment; Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298 (1967).

[33] Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. (forthcoming 2022) (manuscript at 22) (on file at SSRN), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4111547 ("'[S]pecial needs' searches (where we conclude), courts find the government's conduct to be a 'search' governed by the Fourth Amendment, but require neither warrants or probable cause. Rather, government information collection simply requires regulatory prerequisites in place before collection occurs.").

[34] *See* Alan Z. Rozenshtein, *Digital Disease Surveillance*, 70 AM. U. L. REV. 1511, 1541 (2021) (referring to L.A. v. Patel, 576 U.S. 409, 420 (2015)); *see also* Amitai Etzioni, *iPhone vs. Trump: How Technology Companies Can Protect Both Customers and National Security*, NAT'L INT. (Jan. 19, 2020), https://nationalinterest.org/feature/iphone-vs-trump-how-technology-companies-can-protect-both-customers-and-national-security.

[35] Yuval Noah Harari, *The World After Coronavirus*, *supra* note 6; Linda Lew, *Homo Deus Author Yuval Harari Shares Pandemic Lessons From Past and Warnings for Future*, S. CHINA MORNING POST (Apr. 1, 2020), https://www.scmp.com/news/china/article/3077960/homo-deus-author-yuval-harari-shares-pandemic-lessons-past-and-warnings (stating the global pandemic might drive the development of mass surveillance). *See also* Christopher J. Coyne & Yuliya Yatsyshina, *Pandemic Police States* 2 (Geo. Mason

Moreover, even without exigent circumstances, it should be noted that "while technological developments continue at a meteoric pace, courts engage[d] in an [eighteenth] century version of common law decision-making" that did not provide tools for decision-making, and thus failed to prevent the use of mass surveillance.[36] Thus, governments are now engaged in mass collection of information, without warrants, that could result in a surveillance state.

This Article focuses on governments' widespread use of mass surveillance and data-driven tools during the COVID-19 pandemic. Part II will describe how governments used technologies, which were unimaginable even a short time ago, to engage in mass data collection in order to gain health information. Part III will conduct a taxonomy of data-driven practices that were used to protect the public's health. Next, Part IV explores the flip side of surveillance tools by examining how they infringe on privacy, considering that they are used without transparency, oversight, due process, or other safeguards. Part IV also addresses the infringement of privacy and its impact on trust, equality, and freedom of expression, as well as the potential erosion of democracy. In some contexts, it should be noted that this surveillance creep has already occurred.[37] Part V warns about the rise of the surveillance state in the shadow of a health emergency and argues that individuals should still enjoy both civil rights and health going forward, despite what the responses to COVID-19 have caused. It proposes adopting a privacy-by-design approach[38] that will limit the access of authorities to personally identifiable information and limit the use of information to specific ad hoc warnings without keeping it. This

---

Univ. Dep't of Econ., Working Paper No. 20-25, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598643 (noting state actions without legal authority "can be extended beyond surveillance to refer to the wide range of activities undertaken by states in the name of addressing the pandemic").

[36] Friedman, *supra* note 33, at 21 ("We live in an age of lawless surveillance, and when it comes to doing something about it, we're getting nowhere fast.").

[37] *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 98 (2015); Friedman, *supra* note 33, at 14 ("[T]he 'very serious threat to the future of democracy, human rights, and the rule of law around the world.'").

[38] Privacy by design is an approach that incorporates thinking about privacy protective features and implementing them as early as possible. *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 190–91 (2016); KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 32, 178 (2015); *Cf.* COURTNEY BOWMAN ET AL., THE ARCHITECTURE OF PRIVACY: ON ENGINEERING TECHNOLOGIES THAT CAN DELIVER TRUSTWORTHY SAFEGUARDS 13 (2015); ANN CAVOUKIAN, PRIVACY BY DESIGN: TAKE THE CHALLENGE 3 (2009).

Article further proposes anonymization techniques that would allow for beneficial uses of the information, including predictions and research of virus outbreaks. Next, this Article proposes safeguards against mass surveillance, including fiduciary duties, transparency, oversight, and due process in proceedings based on digital surveillance or automated decisions. Finally, this Article rejects altogether the practices of intrusive surveillance that can erode democracy with no way back.

II. SURVEILLANCE CAPITALISM AT THE SERVICE OF THE STATE OF SURVEILLANCE: AN OVERVIEW

The mass collection of information, the Internet of Things, big data, and artificial intelligence opens a new dimension for surveillance, data collections, and analysis by commercial corporations and governments.[39] Private lives of individuals are an open book to companies that have access to their data.[40] These companies can see the places a person visits every minute of the day and draw conclusions about him.[41] Surveillance capitalism marks the new economic order of the twenty-first century.[42] Constant private surveillance and documentation of the public's behavior is the "new oil" for commercial purposes.[43] Today, tracking technology is used nearly everywhere, far beyond the desktop of a computer.[44] These technologies are part of

---

[39] *See* Friedman, *supra* note 33, at 9.

[40] *See* Stuart A. Thompson & Charlie Warzel, Opinion, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[41] Friedman, *supra* note 33, at 9 ("Finally, there's the technology, largely AI driven, to pull all this information together into a remarkably complete picture of who you are, what you are doing, and what you might do next[,] . . . [including, for example,] the Department of Homeland Security's Fast Attribute Screening Technology (FAST), a set of 'behavior-based screening techniques' to ferret out who is safe to fly and who not.").

[42] *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) (coining the term "surveillance capitalism" and explaining its impact on commerce, free will, and society).

[43] *See* Jonathan Vanian, *Why Data Is the New Oil*, FORTUNE (July 11, 2016, 8:35 PM), https://fortune.com/2016/07/11/data-oil-brainstorm-tech.

[44] Paul Ohm & Nathaniel Kim, *Legacy Switches: A Proposal to Protect Privacy, Security, Competition, and the Environment from the Internet of Things*, OHIO ST. L.J. (forthcoming 2023) (manuscript at 5), https://ssrn.com/abstract=4149789 ("Almost all IoT devices embed tiny computers that wirelessly connect to the internet, our smartphones, and one another. Even when everything works as planned, these devices contribute to a

peoples' daily lives through smart connected devices and wearables, thereby producing incidental information—including biometric data—which leaves a digital trace that companies can exploit for marketing and financial gain.[45]

In times of crisis, the state can use the same methods of data collection analysis and prediction that private companies utilize to promote commerce and enhance their profits.[46] Thus, during the COVID-19 crisis, some states accessed "granular user data from CCTV surveillance footage, GPS tracking data from phones[,] . . . credit card transactions[,] and ATM records from financial service firms."[47] Governments gained smartphone location data and other personal information by tracking infected people and the people they were in contact with, thereby attempting to break the infection chain by ensuring those people stayed home.[48]

Such practices resemble the concerning mass surveillance of the KGB (the Committee for State Security). The KGB was established in 1954 as an outgrowth of several Soviet security organizations.[49] Its primary role was to protect the regime, gather and analize information that enhanced the government's understanding of its adversaries, and impose conformity on the population by placing everyone under

---

growing and pervasive surveillance society, creating a detailed record of what individuals and groups do, say, think, and feel.").

[45] *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 140 (2017) ("[N]ew techniques for customer tracking, immersive social design, and data analysis all promised new possibilities for profiting from targeted marketing in an increasingly fragmented media ecosystem."); Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 115 (2019).

[46] Bradford et al., *supra* note 7, at 11.

[47] *See The Use of Digital Enforcement in Light of COVID-19*, ALLOT 5 (2020), https://www.allot.com/resources/SB_Digital_Enforcement_After_COVID19.pdf ("Countries such as France, Germany, Israel, USA and the United Kingdom have unleashed their Intelligence and Law enforcement agencies with the hope that by controlling the crowd they may be able to control the virus. . . . The digital technologies used to fight COVID-19 were made possible by shifting the control and traffic of national networks from telecom providers to the Government itself. . . . Data from CCTV surveillance, credit card information, facial recognition, Internet surveillance, GSM and IP-based geolocation, and others are now rapidly and securely collected."). *See also* Ghose & Sokol, *supra* note 15, at 2–3.

[48] *See* Ghose & Sokol, note 15, at 2; KAHN, *supra* note 8, at 13; Shira Ovide, *Can Our Phones Stop a Pandemic?*, N.Y. TIMES: TECH. (Apr. 10, 2020), https://www.nytimes.com/2020/04/10/technology/coronavirus-smartphones-surveillance.html.

[49] Andrei Soldatov & Irina Borogan, *Russia's New Nobility – The Rise of the Security Services in Putin's Kremlin*, 89 FOREIGN AFFS. 80, 82, 86 (2010).

surveillance. To do so, the KGB used "a network of informers so dense that there was not a club, apartment building, or work brigade without one."[50] Fifty years ago, however, it was impossible for the KGB to follow all Soviet citizens twenty-four hours per day; as such, "[t]he KGB relied on human agents and analysts."[51] Technology changed that predicament because "now governments can rely on ubiquitous sensors and powerful algorithms instead of flesh-and-blood spooks."[52] The government can now use cell phones,[53] the Internet of Things,[54] CCTV,[55] automated license plate readers (ALPRs),[56] and even drones for surveillance.[57] Orwellian watchers observe our every move, infringing on privacy and other civil rights by making surveillance a part of life.[58]

The most notable example is China. By closely monitoring people's smartphones, making use of hundreds of millions of face-recognition cameras, and obliging people to check and report their body temperatures and medical conditions, the Chinese authorities attempted to identify suspected COVID-19 carriers, track their movements, and identify anyone who came into contact with the

---

[50] Aaron Bateman, *The KGB and Its Enduring Legacy*, 29 J. SLAVIC MIL. STUD. 23, 24 (2016).

[51] *See* Harari, *The World After Coronavirus*, *supra* note 6.

[52] *Id.*

[53] *See* Mark Surman, *Privacy Norms and the Pandemic*, MOZILLA BLOG (Apr. 22, 2020), https://blog.mozilla.org/blog/2020/04/22/privacy-norms-and-the-pandemic.

[54] *See generally* Ohm & Kim, *supra* note 44.

[55] CCTV can be utilized for facial recognition. *See* Coyne & Yatsyshina, *supra* note 35, at 7 ("The Chinese government has leveraged its extensive surveillance system to monitor and track citizens. It has also installed CCTV cameras outside the apartments of those quarantined in order to monitor their movements. In Moscow the police have used the government's existing camera system along with facial recognition technologies to monitor people who violate mandatory self-isolation.").

[56] For discussion on this technology, see Friedman, *supra* note 33, at 10 ("AI now allows ordinary low-cost cameras to become license plate readers.").

[57] Coyne & Yatsyshina, *supra* note 35, at 8 ("Governments in countries around the world, including the United Kingdom and the United States, are using drones to monitor citizens and enforce social distancing dictates."); *see, e.g.*, Rob Picheta, *UK Coronavirus Response Criticized as People Are Filmed by Drones and Stopped While Shopping*, CNN: WORLD (Mar. 31, 2020), https://www.cnn.com/2020/03/31/uk/uk-police-coronavirus-tactics-gbr-intl-scli/index.html.

[58] *See* Massaro et al., *supra* note 4, at 269 ("Strategies for virus containment may implicate equality in other ways that relate to privacy and policing. Take, for example, contact tracing. Tracking the movements of infected individuals and identifying those with whom they come into contact triggers liberty concems, because it implicates information about an individual's whereabouts that many would regard as private.").

suspected carriers.[59] A range of mobile applications ("apps") warned citizens about their proximity to infected patients, isolated people who returned from infected areas, and notified persons who had been in touch with infected individuals.[60]

"One of the leading Chinese monitoring apps, Alipay Health Code, use[d] a traffic light system, with a red light requiring mandatory hospital quarantine. Only those whose phone displays a green light are allowed to use facilities such as public transit."[61] Additionally, "Chinese surveillance went as far as forcibly installing cameras inside people's homes, or just outside their front doors, to make sure they complied with quarantine rules."[62]

China is not a democracy, and it has a tradition of tracking people even before COVID-19 started to spread. China's state surveillance practices include facial recognition software, CCTV monitoring, tracking of credit card purchases, and more.[63] The data allows the operation of China's governmental "social credit system."[64] "This system takes the idea of creditworthiness and exports it to all areas of life with the help of big data. Every piece of data on every citizen is used to rate that person on a scale of trustworthiness."[65] The social credit system "rewards and punishes citizens based on characteristics such as honesty, norm-following, and general courtesy, and it appears that biometric tracking is being used to further increase the system's accuracy."[66] China repurposed the infrastructure of its social-credit

---

[59] Joyce Huang, *China's Virus Tracking Technology Sparks Privacy Concerns*, CHINA NEWS (June 22, 2020) https://www.voanews.com/a/covid-19-pandemic_chinas-virus-tracking-technology-sparks-privacy-concerns/6191538.html.

[60] *See* Lucy Alexander, *In Asia, Contact Tracing Apps Have Helped Contain COVID-19. Now They May Be Coming to the U.S.*, ROBB REP. (Mar. 30, 2020), https://www.robbreport.com/gear/personal-technology/covid-19-big-tech-apps-2908811.

[61] *Id.*

[62] CARISSA VELIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA 61 (2020).

[63] *Facial Recognition and Beyond: Journalist Ventures Inside China's 'Surveillance State'*, NPR (Jan. 5, 2021), https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta.

[64] Katie Canales, *China's 'Social Credit' System Ranks Citizens and Punishes Them With Throttled Internet Speeds and Flight Bans if the Communist Party Deems Them Untrustworthy*, INSIDER (Dec. 24, 2021), https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

[65] VELIZ, *supra* note 62, at 60.

[66] Kugler, *supra* note 45, at 115; *see* Xin Dai, *Toward a Reputation State: The Social Credit System Project of China* (2018) (unpublished manuscript) (on file with Peking University Law School), https://papers.ssrn.com/sol3/papers.cfm?abstract

scoring for tracing COVID-19 efforts.[67] Local Chinese authorities have announced that if Chinese citizens fail to report symptoms of the virus, they could find themselves on social-credit blacklists.[68]

Tracking apps were used in many countries outside of China. In Singapore, the government also uses tracking apps.[69] In Singapore, people can give the app "access to Bluetooth, and it logs every phone you come into contact with".[70] "If you develop the virus, health authorities get a record of your phone data so they can contact owners of the other phones".[71] Data about others that the app collected, however, will be unavailable to the people in Singapore.[72]

This health crisis has increased the use of mass surveillance, even in states with long-term democratic traditions. In the United States, elements of the national security state—that is, the National Security Council (NSC), Pentagon, and intelligence—as opposed to civilian public health agencies, developed a response to the virus.[73] While the U.S. government's plans remained classified, reports revealed that the military and intelligence communities were working with the NSC to develop the government's COVID-19 response.[74] Subsequently, the United States government analyzed smartphone location data and reportedly planned to create a national surveillance system[75] by using

---

_id=3193577); FRANK PASQUALE, NEW LAWS OF ROBOTICS: DEFENDING HUMAN EXPERTISE IN THE AGE OF AI 136–39 (2020).

[67] *See generally* Isobel Asher Hamilton, *Chinese Citizens Who Conceal Any Coronavirus History Are Being Punished Using the Country's Dystopian Social Credit System*, BUS. INSIDER (Mar. 17, 2020) https://www.businessinsider.com/china-hiding-coronavirus-punishable-social-credit-system-2020-3.

[67] *Id.*

[68] *See* Shandong Rongcheng, *Social Credit Rewards and Punishments Help Win the Battle of Epidemic Prevention and Control*, ZHONGHONG (March 2, 2020, 11:08 AM), http://www.zhonghongwang.com/show-382-166675-1.html.

[69] Shira Ovide, *Can Our Phones Stop a Pandemic?*, N.Y. TIMES (Apr. 10, 2020), https://www.nytimes.com/2020/04/10/technology/coronavirus-smartphones-surveillance.html.

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *See* Whitney Webb, *US Intel Agencies Played Unsettling Role in Classified and "9/11-Like" Coronavirus Response Plan*, MINT PRESS NEWS (Mar. 13, 2020), https://www.mintpressnews.com/us-intelligence-unsettling-role-classified-9-11-like-coronavirus-response/265687.

[74] *Id.*

[75] *See* Chris Mills Rodrigo, *Senate Democrat Presses White House on Reported Coronavirus Surveillance System Efforts*, HILL (Apr. 8, 2020), https://thehill.com/policy/technology/491806-senate-democrat-presses-white-house-on-reported-coronavirus-surveillance.

this data.[76] Jared Kushner, a former Senior Advisor to President Trump, reached out to several health technology companies about creating a system to give the government real-time data on "where patients are seeking treatment and for what, and whether hospitals can accommodate them."[77] The White House operated in secret, without transparency or safeguards.[78] The White House also allegedly "ignored a Freedom of Information Act (FOIA)[79] request made by the Electronic Privacy Information Center and letters seeking details sent from several senators."[80] Additionally, digital contact tracing technology (DCTT) was proposed as part of a plan to reopen the country,[81] even though such apps are not precise—they work through proxies and cannot tell if someone actually caught the virus.[82]

In Israel, the government approved regulations permitting the Shin Bet (Israel Security Agency) to collect data by tracking cell phones of citizens without consent, using technology normally utilized in counterterrorism.[83] In approving the regulations, the government circumvented the Foreign Affairs and Defense Committee of the Israeli Parliament (part of the unicameral legislature of Israel, called

---

[76] *See* Casey Newton, *The US Government Should Disclose How It's Using Location Data to Fight the Coronavirus*, VERGE (Mar. 31, 2020, 6:00 AM), https://www.theverge.com/2020/3/31/21199654/location-data-coronavirus-us-response-covid-19-apple-google.

[77] Danielle Citron & Geng Ngarmboonanant, *Be Very Wary of Trump's Health Surveillance Plans*, WASH. POST (Apr. 16, 2020, 4:05 PM), https://www.washingtonpost.com/opinions/2020/04/16/be-very-wary-trumps-health-surveillance-plans.

[78] *Id.*

[79] 5 U.S.C. § 552(a)(3)(A); Tara Leigh Grove, *Standing as an Article II Nondelegation Doctrine*, 11 U. PA. J. CONST. L. 781, 828 n.205 (2009) ("FOIA permits any person to request any type of information . . . without demonstrating any distinct interest in or particular need for the material."); *see also* Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CALIF. L. REV. 917, 928 (2021).

[80] Citron & Ngarmboonanant, *supra* note 77. It should be noted that open-data requests and lawsuits for privacy violations that follow are useful in other contexts but are not likely to be useful in the context of the COVID-19 surveillance. On such open-data requests and lawsuits that follow, see Bloch-Wehba, *supra* note 79, at 957, 961–62, 970.

[81] KAHN, *supra* note 8, at 1.

[82] VELIZ, *supra* note 62, at 182.

[83] Judah Ari Gross, *Government Okays Mass Surveillance of Israelis' Phones to Curb Coronavirus*, TIMES ISR. (Mar. 15, 2020) https://www.timesofisrael.com/government-okays-mass-surveillance-of-israelis-phones-to-curb-coronavirus ("Government officials stressed that the use of these tools, usually reserved for counterterrorism operations, was meant to save lives.").

the Knesset) in the process.[84] Ministers authorized the move despite the Justice Ministry's commitment to have it go through the Israeli Parliament, excusing it in that there was no time to deliberate the matter.[85] The regulations also authorized Israeli Police to track cell phones of individuals who tested positive for the virus and subsequently collect data on their whereabouts two weeks prior to diagnosis.[86] Furthermore, the regulations allowed tracking of those who were suspected of having caught the virus and monitored adherence to quarantine orders.[87] Unlike the requirement for a warrant to track cell phone data in criminal cases,[88] no court order authorized collection of data in these instances, nor were there any regulatory prerequisites or other safeguards.[89] Such surveillance was not focused on a specific individual—rather, it was mass surveillance.[90] Everyone was a suspect of spreading the virus.

---

[84] *See* Noa Landau, *In Dead of Night, Israel Approves Harsher Coronavirus Tracking Methods Than Gov't Stated*, HAARETZ (Mar. 17, 2020), https://www.haaretz.com/israel-news/2020-03-17/ty-article/.premium/cellphone-tracking-authorized-by-israel-to-be-used-for-enforcing-quarantine-orders/0000017f-e6de-dc7e-adff-f6ff22150000.

[85] *Id.* ("Ministers authorized the move despite the Justice Ministry's commitment to have it go through the Israeli parliament, which did not have the time to deliberate on the matter.").

[86] *See* Amir Cahane, *The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers*, LAWFARE (Mar. 21, 2020, 12:45 PM), https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers.

[87] *Id.*

[88] Landau, *supra* note 84 (explaining that normally, a court order is required for cell phone tracking, as it is "a serious invasion of privacy if there is no basis for it"); *see* Ariane de Vogue & Clare Foran, *Supreme Court: Warrant Generally Needed to Track Cell Phone Location Data*, CNN (June 22, 2018), https://www.cnn.com/2018/06/22/politics/supreme-court-ruling-cell-phone (explaining that in the United States, after the Supreme Court's decision in *Carpenter*, mass cell phone location data generally requires a warrant); Carpenter v. United States, 138 S. Ct. 2206, 2220–21 (2018) (accessing historical records containing physical locations of cell phones necessitates a search warrant); *see generally* Tokson, *supra* note 31 (expanding on the tests of *Carpenter* for revealing information and how they were used in the aftermath of the decision).

[89] Bradford et al., *supra* note 7, at 14–15 ("Such non-consensual tracking, as well as default sharing of data with law enforcement and national security services, greatly increases the risks that agencies may abuse their authority and use public health data for illegitimate surveillance, law enforcement, or targeting purposes.").

[90] *See generally* Bloch-Wehba, *supra* note 79, at 949 ("[T]he Supreme Court in the recent cases of *Jones* and *Carpenter* ruled that pervasive, long-term location tracking is the subject of Fourth Amendment protection, it remains unclear how those decisions fit with the longstanding rule that searches of public information are not really 'searches' at all.").

The Israeli Ministry of Health used the data that was collected from cell phones to notify individuals of potential contact with someone infected with the virus and to enforce quarantine orders. The Ministry of Health was allowed to keep the data for the sake of an internal inquiry of activities they conducted.[91]

The regulations faced public criticism for allowing mass surveillance by using tools preserved for terrorists. Due to such infringement on human rights, lawyer Shachar Ben Meir, the Association of Civil Rights in Israel (ACRI), and others, petitioned the Israel High Court of Justice to challenge the Israeli government decision to authorize the national security agency and the police to conduct mass surveillance.[92] The Israeli High Court of Justice ordered the state to limit the Israel's Security Agency's (ISA) use of the powers under the emergency coronavirus regulations and forbade police use of such powers until further notice.[93] After the High Court's decision, the Israeli government temporarily extended the authority to track citizens for another period, and it was set to approve a motion that would enshrine the tracking of cell phones belonging to confirmed COVID-19 carriers in law.[94] The passage of this legislation, however, would allow mass surveillance to continue. After many public objections, the government froze the bill.[95] The government, however, eventually restored the bill and continued to track citizens, moving forward into a surveillance state.[96] Only in March 2021, after another

---

[91] Joshua Davidovich, *The Night is Dark and Full of Tracking: 6 Things to Know for March 17*, TIMES ISR. (Mar. 17, 2020), https://www.timesofisrael.com/the-night-is-dark-and-full-of-tracking-6-things-to-know-for-march-17 ("Furthermore, the Health Ministry is allowed to keep the data for another 60 days beyond the regulations' expiration for the sake of an 'internal inquiry of the activities conducted by the Health Ministry.'").

[92] *See* HCJ 2109/20 Ben Meir v. Prime Minister (2020) (Isr.); Netael Bandel, *Israel's Top Court: No Shin Bet Tracking of Coronavirus Patients Without Knesset Oversight*, HAARETZ (Mar. 19, 2020), https://www.haaretz.com/israel-news/2020-03-19/ty-article/.premium/israels-top-court-no-shin-bet-tracking-of-coronavirus-patients-without-knesset-ove/0000017f-e76c-dea7-adff-f7ffa1820000.

[93] *See* HCJ 2109/20 Ben Meir v. Prime Minister (2020) (Isr.).

[94] *See* Itamar Eichner, *Israel to Enshrine in Law Shin Bet's Coronavirus Tracking*, YNET NEWS (Apr. 5, 2020, 12:49 PM), https://www.ynetnews.com/article/rkLE6VpF8.

[95] *See* Noa Landau & Jonathan Lis, *Israel Freezes Bill Allowing Shin Bet Tracking of Coronavirus Patients Due to Agency's Objection*, HAARETZ (June 8, 2020), https://www.haaretz.com/israel-news/.premium-israel-freezes-law-allowing-shin-bet-tracking-of-coronavirus-patients-1.8905478.

[96] *See Coronavirus in Israel: Knesset Advances Shin Bet Monitoring Bill*, HAARETZ (June 25, 2020), www.haaretz.com/israel-news/coronavirus-live-government-agency-warns-against-events-in-closed-spaces-1.8936142; Jonathan Lis, *Knesset Passes Temporary Law Allowing Digital Tracking of Coronavirus Patients by Security Service,* HAARETZ (July 1, 2020),

High Court of Justice holding,[97] was the surveillance limited only to people that did not cooperate with an epidemiologic investigation.[98]

When governments around the world gain new abilities to trace, track, and control citizens, they find it hard to relinquish such power and tend to abuse it by taking more and more. Thus, on November 27, 2021, with the discovery of the Omicron variant in Israel, the COVID-19 cabinet approved the resumption of ISA digital tracking of confirmed COVID-19 carriers by the Shin Bet security agency.[99] Again, ACRI and others petitioned the Israel High Court of Justice and challenged the Israeli government decision to authorize such mass surveillance.[100] Only after a sweeping public outcry did the Israeli Government halt ISA's surveillance concerning COVID-19.[101]

In addition to compulsory government surveillance tools, the Ministry of Health in Israel launched "Hamagen" (The Shield), a new smartphone app users could download voluntarily. This app seemingly aimed to help prevent the spread of the virus "by enabling users to know if they crossed paths with someone who has been diagnosed with the virus" and telling users if they were in the presence of anyone who tested positive.[102] The app cross-checked the "GPS history of [a] mobile phone with historical geographic data of patients from the

---

https://www.haaretz.com/israel-news/2020-07-01/ty-article/.premium/knesset-passes-bill-allowing-digital-tracking-of-covid-19-patients-by-shin-bet/0000017f-dbfb-db5a-a57f-dbfb6da90000.

[97] *High Court Limits Shin Bet Coronavirus Surveillance to Those Who Won't Cooperate*, TIMES ISR. (Mar. 1, 2021, 12:34 PM), https://www.timesofisrael.com/high-court-limits-shin-bet-coronavirus-surveillance-to-those-who-wont-cooperate ("The High Court of Justice ruled on Monday that the Shin Bet security service's controversial phone tracking program, designed to detect coronavirus carriers and those who came in contact with them, can only be used for those who don't cooperate with epidemiological investigations.").

[98] *Id.*

[99] *See* Jonathan Lis & Ido Efrati, *Israel Imposes Travel Ban for Foreigners, Stricter Quarantine Over COVID Omicron Variant,* HAARETZ (Nov. 27, 2021), https://www.haaretz.com/israel-news/israel-s-covid-cabinet-weighs-travel-restrictions-digital-tracking-as-omicron-looms-1.10420085.

[100] HCJ 8196/21 ACRI v. Ministry of Health (2021) (Isr.). *See* Amir Cahane, *The Collapsed Bridge Loan: Israel's Shin Bet Location Tracking of Omicron Carriers*, LAWFARE (Dec. 16, 2021), https://www.lawfareblog.com/collapsed-bridge-loan-israels-shin-bet-location-tracking-omicron-carriers.

[101] *After Outcry, Government Scraps Shin Bet Phone Tracking of Omicron Carriers,* TIMES ISR. (Dec. 2, 2021, 9:19 PM), https://www.timesofisrael.com/government-scraps-shin-bet-phone-tracking-of-omicron-carriers-after-outcry.

[102] Stuart Winner, *Health Ministry Launches Phone App to Help Prevent Spread of Coronavirus*, TIMES ISR. (Mar. 23, 2020, 12:19 AM), https://www.timesofisrael.com/health-ministry-launches-phone-app-to-help-prevent-spread-of-coronavirus.

Ministry of Health."[103] A more advanced version, HaMagen 2.0, was based on both Bluetooth and GPS cell site location data.[104]

Israel took more surveillance and invasion measures beyond cell phone tracking. For example, Israeli police deployed drones to enforce quarantine orders and checked in on patients who were ordered to self-isolate.[105]

Israel's efforts to prevent the diffusion of the virus do not focus only on tracking infected people and others who were around them. Israel also tried to predict risks for individual infection. Accordingly, NSO developed a system ("a notorious Israeli cyber intelligence company for security"),[106] "in cooperation with the Ministry of Defense and the [Israel Defense Forces] . . . for handling information about the probability that Israelis will be infected by the []virus."[107] The government planned that every Israeli citizen would be assigned an "'infection rating' on a scale of 1 to 10."[108] Such ratings were intended to describe "the likelihood that that person is a coronavirus carrier."[109] The system was intended to be updated in real time. A "'rating could be 5.6 one day, and then jump to 9'—the rating is dynamic because it depends on a person's activities: for example, the rating can jump

---

[103] *See HaMagen 2.0*, MINISTRY OF HEATH, govextra.gov.il/ministry-of-health/hamagen-app/download-en (last visited Oct. 6, 2022).

[104] *See HaMagen 2 Application Was Launched*, MINISTRY OF HEATH (July 27, 2020), https://www.gov.il/en/departments/news/27072020_02 ("Currently, the application detects two types of overlap points simultaneously: 1. Geographic tracking based on GPS technology, which alerts of location-based points of proximity to COVID-19 patients. 2. Tracking based on Bluetooth technology, which allows us to detect points of proximity between cellular devices on which this application was installed."); *HaMagen 2.0 App Alerting Users Who Have Crossed Paths with a Coronavirus Patient Ready for Distribution Among Owners of Android Devices*, KNESSET (June 24, 2020), https://main.knesset.gov.il/EN/News/PressReleases/Pages/press24620x.aspx; Press Release, Ministry of Health, HaMagen 2 Application was Launched, (July 20, 2020), https://www.gov.il/en/departments/news/27072020_02.

[105] *See* Joseph Kraus, *Israeli Police use Drones to Enforce Virus Quarantines, Rising Privacy Concerns*, TIMES ISR. (Apr. 14, 2020, 10:43 PM), https://www.timesofisrael.com/israeli-police-using-drones-to-enforce-coronavirus-quarantines.

[106] NSO was later blacklisted by the US Commerce Department for providing spyware to foreign governments that "'used these tools to maliciously target' journalists, embassy workers and activists." Sean Lyngaas, *US Blacklists Israeli Firm NSO Group for Use of Spyware*, CNN BUS. (Nov. 8, 2021, 11:57 AM), https://edition.cnn.com/2021/11/03/tech/nso-group-us-blacklist/index.html.

[107] *See* Yasmin Yablonko, *Bennett Plans Using NSO to Rate Individual Virus Exposure*, GLOBES (Mar. 30, 2020, 2:19 PM), https://en.globes.co.il/en/article-bennett-plans-using-nso-to-rate-individual-virus-exposure-1001323878.

[108] *Id.*

[109] *Id.*

because a person 'visited a grocery store where two carriers visited in recent days.'"[110] This plan, which the Israeli government fortunately neglected, attempted to use the social network and connections of individuals to predict the risk that any person could infect others. In fact, such a plan adopts a credit score system like China has.

Many other countries tracked cell phone locations and used apps and data networks to keep tabs on the virus.[111] Some were compulsory, and some were voluntary. In the European Union (EU), "Vodafone, Deutsche Telekom, Orange and five other telecoms providers have agreed to shared mobile phone location data with the European Commission to track the spread of the []virus."[112] Yet, "the Commission planned to use anonymized data to protect privacy and aggregate mobile phone location data to coordinate measures tracking the spread of the virus."[113]

Nations of the EU launched different apps to track the diffusion of COVID-19.[114] For example, Germany launched a smartphone app to help trace infections. Because in Germany the use of individual smartphone location data to track the spread of the virus is illegal under national and EU privacy laws,[115] the app attempted to track only close-proximity Bluetooth "handshakes" between smartphones and record and encrypt recent history of such contacts on the smartphone device.[116] Only if the smartphone's owner tested positive for the virus

---

[110] *Id.*

[111] *Countries Are Using Apps and Data Networks to Keep Tabs on the Pandemic*, ECONOMIST (Mar. 26, 2020), https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic.

[112] Foo Yun Chee, *Vodafone, Deutsche Telekom, 6 Other Telcos to Help EU Track Virus*, REUTERS (Mar. 25, 2020, 3:06 PM), https://www.reuters.com/article/us-health-coronavirus-telecoms-eu/vodafone-deutsche-telekom-6-other-telcos-to-help-eu-track-virus-idUSKBN21C36G.

[113] *Id.*

[114] *See generally* Costica Dumbrava, *Lifting Coronavirus Restrictions: The Role of Therapeutics, Testing, and Contact-Tracing Apps*, EUR. PARLIAMENTARY RSCH. SERV. 22 (July 2020), https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/652016/EPRS_IDA(2020)652016_EN.pdf.

[115] Douglas Busvine, *Germany Aims to Launch Singapore-Style Coronavirus App in Weeks*, REUTERS (Mar. 30, 2020, 9:58 AM), https://www.reuters.com/article/us-health-coronavirus-germany-tech/germany-aims-to-launch-singapore-style-coronavirus-app-in-weeks-idUSKBN21H26Z.

[116] B. Sowmiya et. al, *A Survey on Security and Privacy Issues in Contact Tracing Application of COVID-19*, 136 SN COMPUT. SCI. 2, 4 (2021) ("Germany launched its application named 'Corona Warn App' which does not store the location of users by concerning the Privacy of every user and it works together with Apple and Google. The exposure Notifcation System on the device transmits a rolling proximity identifer,

could the data be downloaded and transferred to the health authorities to allow contact tracing teams to "get in touch with others at risk."[117]

The use of location data was also common to enforce quarantine. Taiwan was one of the first countries to use a mobile-phone-based "electronic fence" that used location tracking to ensure people who were quarantined stayed in their homes.[118] "The system monitor[ed] phone signals to alert police and local officials if those in home quarantine move[d] away from their address[es] or turn[ed] off their phones."[119]

In summary, countries and private companies used mass surveillance and data-driven models in an attempt to combat the virus. The following part will explore the use of such technologies and models during the COVID-19 outbreak.

III. TAXONOMY OF DATA USES AND BENEFITS FOR COMBATING DIFFUSION OF COVID-19

A. *Warning of Exposure*

Two years ago, "[t]he World Health Organization (WHO) . . . urged countries to trace and track every COVID-19 case."[120] Tracking each and every move of individuals through cell phone location data, CCTV, and credit card purchases, and more, might make it possible for governments to identify positive cases, isolate those individuals, and warn others of any potential contact risks.[121] When the virus started to spread, many believed that surveillance could be used to trace infected people, thereby breaking the infection chain.[122] People believed that mass surveillance would allow states to focus on people that were

---

while also regularly scanning for identifers of phones using Bluetooth technology and storing the identifers locally. Those identifers are only valid for 20 min and derived using Cryptography from dynamic keys which changes every 24 h.").

[117] *See* Busvine, *supra* note 115.

[118] *See* Yimou Lee, *Taiwan's New 'Electronic Fence' for Quarantines Leads Wave of Virus Monitoring*, REUTERS (Mar. 20, 2020, 3:44 AM), https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc/taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-idUSKBN2170SK.

[119] *Id.*

[120] Ghose & Sokol, *supra* note 15, at 2.

[121] *See* James G. Adams & Ron M. Walls, *Supporting the Health Care Workforce During the COVID-19 Global Epidemic*, 323 JAMA 1439, 1439 (2020) ("Those . . . with symptoms of suspected COVID-19 should be rapidly triaged and separated from the general population . . . .").

[122] Ghose & Sokol, *supra* note 15, at 2.

already infected, or at severe risk to be infected, in order to avoid an aggressive lockdown.[123] South Korea implemented such an approach by adopting robust surveillance and other measures to avoid announcing an overall state-wide lockdown.[124]

B. *Enforcement of Quarantine Orders*

Individuals that were infected or were near infected people might be a source of infection.[125] "Quarantines and travel bans are often the first response against new infectious diseases."[126] "In public health practice, 'quarantine' refers to the separation of persons (or communities) who have been exposed to an infectious disease."[127] "'Isolation,' in contrast, applies to the separation of persons who are known to be infected."[128] Yet, in the time of COVID-19, "'quarantine' [referred] to both types of interventions, as well as to limits on travel."[129]

This controversial strategy of quarantines and isolation measures[130] was criticized by many scientists,[131] including in The Great

---

[123] *See* Gyooho Lee, Legitimacy and Constitutionality of Contact Tracing in Pandemic in the Republic of Korea 3 (May 7, 2020) (unpublished manuscript) (on file with Chung-Ang University School of Law), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3594974.

[124] *Id.* ("[T]he ability to trace and treat infected people has allowed South Korea to avoid aggressive lockdowns."); *see also* Anurag Viswanath, *COVID-19 Lessons from South Korea: Between Trust and Surveillance*, FIN. EXPRESS (Apr. 1, 2020, 5:15 AM), https://www.financialexpress.com/opinion/covid-19-lessons-from-south-korea-between-trust-and-surveillance/1915089 ("Instead, the strategy was TRUST: Transparency, Robust Screening and quarantine, Unique but universally applicable testing, Strict control and Treatment.").

[125] *See* Massaro et al., *supra* note 4, at 236 (explaining that it was believed that people that had symptoms or contact with an infected individual could present heightened risk of infecting others).

[126] *See* Wendy E. Parmet & Michael S. Sinha, *COVID-19—The Law and Limits of Quarantine*, 382 NEW ENG. J. MED. e28(1) (2020).

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] Martin Kulldorff et al., *Our COVID-19 Plan Would Minimize Mortality and Lockdown-Induced Collateral Damage*, USA TODAY (Oct. 22, 2020, 8:27 PM), https://www.usatoday.com/story/opinion/todaysdebate/2020/10/22/covid-plan-would-minimize-mortality-lockdown-induced-damage-editorials-debates/3735800001 ("The 'Focused Protection' plan in the Great Barrington Declaration would minimize both COVID-19 mortality and lockdown-induced collateral damage on other health outcomes.").

[131] *See, e.g.*, @MartinKulldorff, TWITTER (Sept. 19, 2020, 1:55 PM), https://twitter.com/MartinKulldorff/status/1307377809619288065 ("Contact

Barrington Declaration.[132] According to this strategy, everyone that was exposed to an infected person should isolate himself.[133] Everyone should work to achieve the common objective of mitigating the crisis, but individuals may fail to work together to achieve common good, namely reducing the spread of COVID-19. While individuals in any given group may share common interests with every other, each also has conflicting interests on whether to stay isolated to mitigate the spread of COVID-19, and whether it is worthwhile to sacrifice their freedom for a potential benefit to the collective, even if isolation slows the spread of the virus. To solve this collective action problem,[134] and despite criticism,[135] states used and enforced quarantine orders. To do so, they used cell phone location data, or other apps,[136] and conducted surveillance by using drones, to make sure that people that might have

---

tracing, testing and isolation is important against many infectious disease outbreaks, such as Ebola and post-vaccine measles. It is ineffective, naïve, and counter-productive against COVID19."); @MartinKulldorff, TWITTER (Dec. 19, 2020, 12:45 PM), https://twitter.com/MartinKulldorff/status/1340352578341789699 ("While contact tracing and isolation is critically important for some infectious diseases, it is futile and counterproductive for common infections such as influenza and #COVID19."); Jay Bhattacharya & Mikko Packalen, *On the Futility of Contact Tracing*, 5 INFERENCE, Sept. 2020, at 2 (COVID-19 "is too widespread for contact tracing to limit disease spread; second, that errors in PCR tests substantially raise the human costs of contact tracing and render it less effective; and finally, that contact tracing creates strong incentives among the public to mislead public health authorities and avoid voluntary testing".).

[132] Many epidemiologists signed The Great Barrington Declaration and heavily criticized "damaging physical and mental health impacts of the prevailing COVID-19 policies." GREAT BARRINGTON DECLARATION, https://gbdeclaration.org (last visited Aug. 28, 2022).

[133] *If You've Been Exposed to the Coronavirus*, HARV. HEALTH PUBL'G (Aug. 25, 2022), https://www.health.harvard.edu/diseases-and-conditions/if-youve-been-exposed-to-the-coronavirus.

[134] *See Collective Action Problem*, BRITANNICA, https://www.britannica.com/topic/collective-action-problem-1917157 (last visited Aug. 28, 2022); *see also* Frederik Jørgensen et al., *Compliance Without Fear: Individual-Level Protective Behaviour During the First Wave of the COVID-19 Pandemic*, 26 BRIT. J. HEALTH PSYCH. 679, 681–82 (2021) (identifying compliance with coronavirus protective behavior as a collective action problem).

[135] *See* Bhattacharya & Packalen, *supra* note 131.

[136] For example, "[t]he Polish government has introduced a new ["Home Quarantine"] app that will require coronavirus patients to take selfies to prove they're quarantining properly" for 14 days. Individuals that download the app "register a selfie with the app, then periodically receive requests for geo-located selfies. If they fail to comply, the police will be alerted." Isobel Asher Hamilton, *Poland Made an App That Forces Coronavirus Patients to Take Regular Selfies to Prove They're Indoors or Face a Police Visit*, INSIDER (Mar. 23, 2020, 8:06 AM), https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3.

posed a risk for infection stayed at home.[137] Moreover, the police even visited suspected violators, stepping in the direction of "the police state."[138]

C. *From Individuals to Networks: General Mapping of Social Networks and Predictions*

Today, social networks seem to organize social life.[139] "They are always there, exerting both subtle influence over our choices, actions, thoughts, feelings, and even our desires."[140] "Social networks can affect the full spectrum of human experience."[141] The ties and connections formed within them are crucial to understanding dissemination of information and resulting behavior.[142] The prisms of social networks allow a new understanding of the spread of viruses because networks and connections affect health.[143] Mapping and identifying areas of outbreak on social networks and visualizing a spreading pattern of the virus might allow individuals to take more accurate measures to combat the virus.[144] Because charts and graphs are available for everyone's analysis, they can be used for measuring, calculating,

---

[137] *See* Coyne & Yatsyshina, *supra* note 35, at 8; *see also* Picheta, *supra* note 57.

[138] Michael D. Whitem & Henry F. Fradella, *Policing a Pandemic: Stay-at-Home Orders and What they Mean for the Police*, 45 AM. J. CRIM. JUSTICE 702(2020); Coyne & Yatsyshina, *supra* note 35, at 2 ("As the range of government responses illustrate, one implication of COVID-19 is the rise of police states which, in the name of protecting public health, limit the basic rights and freedoms of citizens and impose, often harsh, punishments on those who fail to obey state dictates.").

[139] MANUEL CASTELLS, NETWORK LOGIC: WHO GOVERNS IN AN INTERCONNECTED WORLD? 221 (2004).

[140] NICHOLAS A. CHRISTAKIS & JAMES FOWLER, CONNECTED: THE SURPRISING POWER OF OUR SOCIAL NETWORKS AND HOW THEY SHAPE OUR LIVES 7 (2009).

[141] *Id.*; Michal Lavi, *Content Providers' Secondary Liability: A Social Network Perspective*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 855,889 (2016).

[142] *See* CHRISTAKIS & FOWLER, *supra* note 140, at 7–9.

[143] CHRISTAKIS & FOWLER, *supra* note 140, at 95–134 (describing how social connections can influence health). *See also* Nicholas A. Christakis, THREAD READER (Mar. 5, 2020), threadreaderapp.com/thread/1235566497591742464.html ("The speed with which people acquired the flu during the epidemic depended on various aspects of their social network position. Those with more friends, those who were more central in the network, and those whose friends did *not* know each other got it sooner.").

[144] *See* Baoquan Chen et al., *Visual Data Analysis and Simulation Prediction for COVID-19*, 6 INT'L J. EDUC. EXCELLENCE 95, 95 (2020) (the researchers collected and visualized publicly available data and showed patterns and characteristics of the pandemic development. Such visualization allows for evaluating the effectiveness of some pandemic control measures, and more importantly, to offer better preventive measures).

modelling and interpreting. Policy makers and governments can plan a strategy for combating the virus based on insights available to them. For example, mapping and visualizing the spread of the virus through social networks allowed governments around the world to restrict lockdowns to urban areas, avoiding restrictions on freedom of movement in areas that were less risky.[145]

Data from *online* social networks, and data on networks collected through DCTT, in a de-identified form, might prove useful to professionals and researchers "to support population-level epidemiologic analysis."[146] Such an analysis might even forecast the spread of communicable viruses. Measuring the intensity of social connectedness between locations might allow professionals and researchers to draw conclusions on connectedness between areas. Such conclusions can be deduced based on information and activity on online social networks.[147] Utilizing data from social networks allowed professionals, researchers, and the tech industry to predict virus outbreaks and improve allocation of resources.[148] Of note, as part of a research project, Facebook asked users whether they had been infected with the virus and tried to generate "'heat maps' of the outbreak" and "mak[e] new categories of data available to scientists who specialise in studying [viruses] through a new program called Disease Prevention Maps,"[149] to model transmission of the virus.

Mapping and visualizing the outbreak allowed researchers to see the big picture of the impact of the virus, track it on a day-to-day basis, anticipate what may happen, and prepare for different outcomes.[150] Looking at the big picture increases the likelihood of mitigating the virus. "[S]ignificant transformation in the ability to collect massive datasets" allows further analysis of data on networks by harnessing AI

---

[145] *See* Lee, *supra* note 123 (explaining that mapping the spread of the pandemic in South Korea "made it easier for the health authorities to see the coronavirus, to see where it is located and where it may be lurking" and "to avoid aggressive lockdowns").

[146] KAHN, *supra* note 8, at 2.

[147] *See generally* Theresa Kuchler et al., *The Geographic Spread of COVID-19 Correlates with Structure of Social Networks as Measured by Facebook* (Cornell University, Working Paper No. 26990, 2020).

[148] *See* SINAL ARAL, THE HYPE MACHINE: HOW SOCIAL MEDIA DISRUPTS OUR ELECTIONS, OUR ECONOMY, AND OUR HEALTH—AND HOW WE MUST ADAPT 234 (2020).

[149] Martin, *supra* note 16.

[150] *See, e.g.*, Lucas Ropek, *Boston Turns to Data Analytics to Track COVID-19 for Residents*, GOV'T TECH. (Mar. 20, 2020), www.govtech.com/analytics/Boston-Turns-to-Data-Analytics-to-Track-COVID-19-for-Residents.html (describing how Boston tracks the spread of the pandemic by mapping it at the macrolevel).

algorithms.[151] Constant collection of "digital traces from large segments of the population" might allow AI to draw conclusions on the welfare of the population, as it can find hidden correlations stored in large databases.[152] AI algorithms can thereby monitor the spread of infectious diseases and viruses. For example, "[d]uring the 2020 outbreak of coronavirus in Wuhan, China, journalists reported that data mining algorithm of health information called BlueDot was the first to warn of its spread."[153] AI algorithms can thus identify areas at risk, predict how the virus will spread further, and direct resources to cities that are most likely to be affected.

D. *From Networks to Individuals*

Social network analysis could help to deal with a crisis like the outbreak of COVID-19. Mathematic graphs of networks can represent entities (each is assigned to a node) and their relationships (each relationship is represented by a line between two nodes). It was believed that understanding networks might allow authorities to cut the graph and quarantine all the close connections of an individual that had been infected.[154] For example, understanding networks can help authorities to quarantine only the co-workers of the infected individual, or only the individuals that were in his proximity. Additionally, utilizing network analysis might improve *Warning of Exposure* practices described in Part III.A.

Network analysis and big data could also be used to predict risks. For example, Alphabet's life sciences division, Verily, developed a website to screen people for symptoms of the virus. "[A]fter accessing the system, which require[d] an active Google Account, each user is assigned a risk score."[155] Risk scores can be assigned based on individuals' data, their location, and their networks.[156]

---

[151] Ghose & Sokol, *supra* note 15.

[152] *See* Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence,* 11 U.C. IRVINE L. REV. 995, 1020 (2021).

[153] *Id.*; Ghose & Sokol, *supra* note 15.

[154] *See* Ricardo Gonçalves, *Performing Social Network Analysis to Fight the Spread of COVID-19*, SISENSE, https://www.sisense.com/blog/performing-social-network-analysis-to-fight-the-spread-of-covid-19 (last visited Aug. 17, 2022).

[155] *See* Marks, *supra* note 152, at 1004.

[156] *See Health Disparities Intensified by the COVID-19 Pandemic and Efforts to Mitigate*, VERILY (Apr. 24, 2020), https://blog.verily.com/2020/04/health-disparities-covid-19-underserved-communities.html ("When it comes to health, location plays an important role. Even within the same city, a study by the National Institutes of Health found that life expectancy can vary widely from one neighborhood to the next. Black

The idea that networks can influence welfare and health is not new. More than a decade ago, Christakis and Fowler found that the happiness of an individual is affected by the happiness of his friends on social networks and even the happiness of friends of his friends.[157] Similarly, a person's network affects their risk of obesity.[158] A person with obese friends has a greater chance to become obese as well.[159] Similarly, many believed that these insights on the influence of social networks and relationships can be analogized to the risks of infection from the virus. Knowing who your friends are can tell you what your chances are of being infected. The speed with which people infect one another depends on various aspects of their social network position.[160] Those with more friends and those who are more central in their network could get the virus sooner.[161] Tracking human networks and utilizing the information generated could predict risks more accurately.

In Israel, the idea arose of utilizing human connections to predict and mitigate risks from individuals to spread COVID-19 based on their network. NSO, a notorious Israeli cyber intelligence company for security, and spyware,[162] cooperated with the Ministry of Defense and Israel Defence Forces and developed a system that planned to handle information about the probability of Israelis being infected by the virus.[163] According to this plan, every Israeli citizen was intended to

---

Americans are almost twice as likely to live in areas expected to be most affected by COVID-19.").

[157] James H. Fowler & Nicholas A. Christakis, *Dynamic Spread of Happiness in a Large Social Network Longitudinal Analysis Over 20 Years in the Framingham Heart Study*, BMJ 1, 7 (2008), https://www.bmj.com/content/bmj/337/bmj.a2338.full.pdf.

[158] *See* Nicholas A. Christakis & James H. Fowler, *The Spread of Obesity in a Large Social Network Over 32 Years*, 357 NEW ENG. J. MED. 370, 370 (2007).

[159] *See id.*

[160] Rasim Alguliyev et al., *Graph Modelling for Tracking the COVID-19 Pandemic Spread*, NAT'L LIB. MED. (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7753933 ("In case of pandemic, the speed of infection depends on average number of people one person can infect and the time needed for these people to become contagious."); Nicholas A. Christakis, THREAD READER (Mar. 5, 2020), threadreaderapp.com/thread /1235566497591742464.html.

[161] *See* Christakis, *supra* note 160.

[162] The U.S. Department of Commerce has now blacklisted NSO for providing spyware to foreign governments that "'used these tools to maliciously target' journalists, embassy workers and activists." Sean Lyngaas, *US Blacklists Israeli Firm NSO Group for Use of Spyware,* CNN BUS. (Nov. 4, 2021) (citation omitted), https://edition.cnn.com/2021/11/03/tech/nso-group-us-blacklist/index.html.

[163] *See* Gwen Ackerman & Yaacov Benmeleh, *Surveillance Firm NSO Supplying Data Analysis to Stop Virus,* BLOOMBERG L. (March 17, 2020), https://www.bloomberg.com

have "an 'infection rating' from 1 to 10 describing the likelihood that that person is a coronavirus carrier."[164] The plan also stated that "[t]he system is updated in real time."[165] A person's rating "could be 5.6 one day, and then jump to 9 because [he] visited a grocery store where two carriers visited in recent days."[166] Such a plan uses the social network and connections of an individual to predict the risk that he will infect others and triggers interventions that affect individual human rights and civil liberties, such as the quarantining of an individual suspected of being infected. Such an intrusive intervention can be performed based on correlation, without reasoning, explanation, due process, or transparency. Israel fortunately neglected this plan, and it was not applied. China, however, has implemented such a solution through using surveillance technologies to rate their citizens according to their risk of infection, conducting algorithmic analyses based on a citizen's locations and medical history.[167] The results of the algorithmic analysis provide every citizen a different-colored health code reflecting his risk.[168] A high-risk score results in limitations on a citizen's freedom of movement.

After reviewing the practices of mass surveillance and data-driven models that were used as an attempt to mitigate the spread of the virus, the next Part will address their infringement on privacy and civil rights, such as freedom of expression and procedural justice. Moreover, the next Part will address the problem of surveillance creep that can result from digital tracking and data collection, as well as the erosion of democracy and rise of the surveillance state that will occur without oversight and safeguards.

/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus#xj4y7vzkg; *see also* Yablonko, *supra* note 107.

[164] Yablonko, *supra* note 107.

[165] *Id.*

[166] *Id.*

[167] *See* VELIZ, *supra* note 62, at 63–68; Dong Huang et al., *A Novel Risk Score to Predict Diagnosis with Coronavirus Disease 2019 (COVID-19) in Suspected Patients: A Retrospective, Multicenter, and Observational Study*, 92 J. MED. VIROLOGY 2709, 2711 (2020) (expanding on risk factor and risk score).

[168] Helen Davidson, *China's Coronavirus Health Code Apps Raise Concerns Over Privacy*, GUARDIAN (Apr. 1, 2020), https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy ("The 'health code' service—run on the ubiquitous platforms Alipay and WeChat and developed for the Chinese government—give users color-coded designations based on their health status and travel history, and a QR code that can be scanned by authorities.").

IV. THE FLIP SIDE OF DIGITAL SURVEILLANCE

A. *The Invasion of Privacy*

Digital surveillance may allow governmental authorities and agencies around the world to know where a person has been, whether he was in proximity to another person, and whether he was at home or not. When government agencies use drones to enforce a quarantine, they can learn what a person's home looks like, who a person lives with, and other personal details about that individual.[169] In addition, governments can draw conclusions from network analyses on an individual based on correlations without a causal link or explanation.[170] Aggregation of separate pieces of information and their analysis can lead to more data—which can be deduced from the analysis of an individual's information—and concrete conclusions on an individual. When governments conduct digital surveillance without the consent of the tracked individuals or use individuals' information for purposes other than that which the data subjects consented to, governments violate those individuals' right to privacy. Such an invasion causes harm per se. It infringes on individual privacy to be free from intrusion and the freedom to exclude the public, which Warren and Brandeis defined as "the right to be let alone,"[171] and Gavison defined as the limited right of access of others to our private spaces.[172]

Beyond the infringement of the negative right to privacy, namely the freedom from intrusion and notions of individual "rights to be let alone," mass surveillance disrespects individuality and personhood.[173] The invasion of privacy hampers identity formation.[174] A person who

---

[169] On drones and privacy invasions, see Hadar Y. Jabotinsky & Michal Lavi, *The Eye in the Sky Delivers (and Influences) What You Buy*, 24 U. PENN. J. CONST. L. (forthcoming 2022) (manuscript at 1–2) (on file with author) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3849218.

[170] *See generally* Rebecca Williams, *Rethinking Administrative Law for Algorithmic Decision Making*, 42 OXFORD J. LEGAL STUD., 428 (2022) ("The increasing prevalence of algorithmic decision making (ADM) by public authorities raises a number of challenges for administrative law in the form of technical decisions about the necessary metrics for evaluating such systems, their opacity, the scalability of errors, their use of correlation as opposed to causation and so on.").

[171] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 15 (2008).

[172] *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 446–47 (1980); *see also* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 171, at 20.

[173] *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 171, at 30.

[174] *See* RICHARDS, *supra* note 30, at 115.

knows that he is constantly watched and that the government collects information on him feels like a tool in the government's hands, not a free individual with sensibilities, ends, and aspirations of his own.[175] Thus, surveillance infringes on his dignity, personal autonomy, and self-determination.[176] The infringement of dignity can encroach on freedoms, such as the freedom to choose and control one's information and make rational choices.[177]

The loss of control over personal information and the infringement of privacy can result in several reactions. First, there are reactions on the part of the data subject that would change his behavior as a consequence of the violations of his privacy rights and the violations of his trust. Second, governments and other data processors can misuse the information to gain more control over citizens and infringe on their civil rights and liberties. Privacy is not only important on its own; the lack of privacy impacts other rights as well.[178] Surveillance infringes on the right to privacy by allowing for conclusions on individuals health, which can reach the general public. Moreover, surveillance can result in conclusions even about the intimate parts of life, violating intimate privacy.[179] The consequences are beyond the violation of privacy in itself, as such information can lead to undesirable stigmas, discrimination, and allow for the manipulation of individuals.[180]

As the following subsections demonstrate, the outcomes of infringing privacy are concerning.

---

[175] *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1116–17 (2002).

[176] ARI EZRA WALDMAN, PRIVACY AS TRUST INFORMATION PRIVACY FOR AN INFORMATION AGE 26–27 (2018).

[177] *See id.* at 29 (referring to IMMANUEL KANT, GROUNDWORK OF THE METAPHYSICS OF MORALS 71–72 (Mary Gregor trans., 1998)).

[178] RICHARDS, *supra* note 30, at 68.

[179] On the concept of privacy as intimacy, see Scott Skinner Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 161–62 (2015); Danielle Keats Citron, *Presidential Privacy Violations*, ILL. L. REV. 1913, 1916 (forthcoming 2022).

[180] I will further address the problem of stigma and discrimination in the next subsections. For further information on the need for privacy for preventing stigmas, see WALDMAN, *supra* note 176, at 24 (referring to ERVING GOFFMAN, STIGMA: NOTES ON THE MANAGEMENT OF SPOILED IDENTITY 3, 31, 43, 78, 140 (1963)).

B. *Consequences of Invading Privacy*

1. Chilling Effects of Surveillance—Effects on Individuals

i. Chilling Social Behavior

Surveillance infringes on privacy as a right to form relationships in society.[181] Privacy allows people to share information, behave and interact in ways appropriate to their different roles, construct unique norms for every context they operate in, and develop their interaction in public places.[182] Invasions into privacy by surveillance disrupt relations in society. The problem increases in a digital world where data is aggregated, analyzed, and used to categorize data subjects.[183] Information is taken out of context and used to draw conclusions on data subjects.[184] If people knew that their government collected information on their public activities and used it to draw conclusions about them—and in turn limit their freedom—they might change their behavior ex ante, behave differently, and even reduce their interactions with others.[185] In so doing, they would reduce the risk that the government will take their behavior out of context. Thus, due to the fear of future harm because of governmental surveillance, individuals would self-chill their behavior and the flow of information they create altogether.[186] Even if there is any ambiguity regarding whether the government conducts surveillance in specific circumstances, individuals would likely "act the way they believe others

---

[181] *See, e.g.*, *id.* at 35 (describing how retail giant Target used a young woman's purchase history and other pieces of information to accurately guess that she was pregnant and send her targeted advertisements); *see* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/20112/02/19/magazine/shopping-habits.htm?pagewanted- &_r=l &hp.

[182] *See* RICHARDS, *supra* note 30, at 38 (referring to ERVING GOFFMAN, INTERACTION RITUALS: ESSAYS ON FACE TO FACE VIRTUAL (1967)).

[183] On aggregation of data and algorithmic analysis, see FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 165 (2015).

[184] On a theory of information flow in context, see HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 4 (2010).

[185] *See* Jonathon W. Penney, *Understanding Chilling Effects,* 106 MINN. L. REV. 1451, 1492–93 (2022) (explaining that people change their behavior while being watched. This phenomenon is known as the "Hawthorne Effect"); GUILLERMO RAMIREZ-PRADO ET AL., NON-INTRUSIVE BEHAVIOR AWARENESS FOR RESIDENTS OF A SMART HOUSE, 2019 IEEE INTERNATIONAL CONFERENCE ON BIG DATA 5269 (2019).

[186] *See* Woodrow Hartzog & Evan Selinger, *Surveillance As Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1376–77 (2015).

would act in the same circumstance."[187] In other words, they would follow the norm, and that would lead to conforming—acting in ways that are mainstream.[188]

ii. Chilling Intellectual Privacy and Freedom of Expression

Mass digital surveillance infringes on privacy. At first glance, privacy conflicts with free speech because if there is more privacy, there is less free speech. This view of the relationship of privacy and speech, however, is misleading. A meaningful amount of privacy, what Neil Richards calls "'intellectual privacy,' . . . is essential to a robust culture of free expression" and safeguards democratic freedom.[189] "[Intellectual Privacy] is the privacy necessary to produce speech," as opposed to privacy that protects against unwanted speech.[190] Intellectual privacy includes three rights and liberties: (1) freedom of thought;[191] (2) the right to read freely;[192] and (3) the right to communicate in confidence.[193] Mass digital surveillance infringes on these rights.

Legitimizing and normalizing the deployment of digital mass surveillance on citizens to combat the spread of the virus—by collecting and analyzing information on the location of citizens, their connections, and their social networks—is an infringement of intellectual privacy. Individuals' intellectual activities would be disrupted if they knew that governments tracked their movement, their data on their social networks and communications, and knew their thoughts.[194] This is because when individuals feel they are being watched, they act differently.[195] "[S]urveillance is permanent in its

---

[187] Penney, *supra* note 185, at 1488; *see also* VELIZ, *supra* note 62, at 85 (when people know they are being watched and that whatever they do could have bad consequences for them, they tend to self-censor).

[188] *See* RICHARDS, *supra* note 30, at 129; *see also* Penney, *supra* note 185, at 1459.

[189] NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 11 (2015); *see also* RICHARDS, *supra* note 30, at 7 (explaining that privacy promotes instrumental values: identity building, freedom, and protects us as situated consumers and members of society).

[190] RICHARDS, *supra* note 189, at 11.

[191] *See id.* at 109, 112.

[192] *See id.* at 123–24.

[193] *See id.* at 136, 138–39.

[194] *See id.* at 106.

[195] *See* Melissa Bateson et al., *Cues of Being Watched Enhance Cooperation in a Real-World Setting*, 2 BIOLOGY LETTER 412, 412 (2006) (describing how workers put more money in a break room honesty box as requested by a sign when the background of the sign had eyeballs on it).

effects, even if it is discontinuous in its action . . . ."[196] Government surveillance will chill intellectual experimentation and speech because it causes individuals "not to experiment with new, controversial, or deviant ideas."[197] Such surveillance infringes on freedom of expression.[198]

C. *Lack of Trust—Lack of Cooperation with Health Authorities*

Privacy builds trust in addition to shielding against invasion.[199] If states build trust in sharing information for combating COVID-19, people might cooperate in solidarity for the health of others, even if there is a price in their freedom. If, however, mass surveillance and uses of personal information are without meaningful consent and infringe on reasonable privacy expectations, trust is breached; concerned citizens will change their social behavior and avoid cooperating with the government.[200] Failing to build trust in information sharing, invading privacy, and misusing information leads to a decay of trust,[201] suspicion instead of solidarity. Consequently, individuals will avoid adopting contact tracing applications, or circumvent their operations. For example, they can put their smartphone on "flight mode" disabling all wireless signals, Bluetooth, and GPS location tracking,[202] or simply leave their smartphone at home.[203] They might also avoid cooperating with epidemiologic interrogations if they lose their trust in public health responses to the

---

[196] *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 201 (Alan Sheridan trans., Vintage Books 2d ed.1995) (1977).

[197] RICHARDS, *supra* note 30, at 134.

[198] *Id.* at 131–36. (expanding on privacy and freedom).

[199] *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV 431, 464 (2016).

[200] *See, e.g.*, WALDMAN, *supra* note 176, at 53–54 (expanding on the importance of trust between sharers of information).

[201] *See* Citron, *supra* note 179, at 1932 (referring to governmental privacy violations, such as abuses of private information for smear campaign that eroded the "faith in the government's commitment to protect the privacy of data that they have collected about us.").

[202] *What Does Flight Mode Mean on a Mobile Phone*, METROFONE (June 25, 2022), https://www.metrofone.co.uk/blog/what-does-flight-mode-mean-on-a-mobile-phone.

[203] KAHN, *supra* note 8, at 19.

virus.[204] Without trust, individuals will not disclose essential information[205] and will mislead health authorities.

1. The Direct Infringements of Mass Digital Surveillance on Human Rights and Civil Liberties

i. Stigma and Discrimination

"Privacy protects us from being misdefined and judged out of context . . . ."[206] Surveillance and tracking infringes the right to privacy and can result in stigmas, leading to discrimination.[207] Such physical or social labels deeply devalue and discredit an individual from gaining full social acceptance.[208] Stigma of infection was common regarding the virus. When the virus started to spread, individuals that were identified as testing positive for the virus, or a neighborhood that was identified as a "hotspot" of infection, could become victims of stigma. Society might associate them with illness, or treat them with hostility based on their nationality, race, or town.[209] In turn, society might exclude, discriminate against, and reject, or even blame, them. The blame directed towards Chinese people serves as a good example.[210] Such a stigma can exacerbate already existing inequality, as in many cases outbreaks occur in already marginalized population concentrations.[211] If data regarding positive test results, quarantine

---

[204] *See* Massaro et al., *supra* note 4, at 252 (explaining that individuals will cooperate only if they have confidence in the ability of institutions to protect safety, liberty, and equality).

[205] *See* WALDMAN, *supra* note 176, at 71.

[206] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000); WALDMAN, *supra* note 176, at 28.

[207] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 855–57 (2022) ("A key aspect of discrimination harms is the unequal frequency, extensiveness, and impact of privacy violations on marginalized people. People of color are disproportionately targeted by surveillance.").

[208] GOFFMAN, STIGMA, *supra* note 180, at 3.

[209] *See* UNAIDS, RIGHTS IN THE TIME OF COVID-19: LESSONS FROM HIV FOR AN EFFECTIVE, COMMUNITY-LED RESPONSE 8 (2020).

[210] KAHN, *supra* note 8, at 71.

[211] *See, e.g.*, Ali Farhoudian et al., *COVID-19 and Substance Use Disorders: Recommendations to a Comprehensive Healthcare Response*, 11 BASIC & CLINICAL NEURO SCI. 133, 141 (2020) (describing a "marginalized hard-to-reach population living in crowded groups with lower access to healthcare. They usually suffer from poorer health [and] weaker immune function . . . . Consequently, they have higher risk of contracting COVID-19 and its transmission and casualties."); Alan Z. Rozenshtein, *supra* note 34, at 1554 ("Marginalized groups may also be subject to secondary

orders, or areas of outbreak are made public for purposes outside of public health, then those individuals are likely to be stigmatized or discriminated against.[212] For example, an employer may avoid hiring an employee that lives in a "hot spot."[213] As mass surveillance technology advances and the market gains more information on the health of people, the use of such information without safeguards is likely to exacerbate stigma and discrimination.

ii. Lack of Transparency and Infringement of Procedural Justice

Mass surveillance has consequences to individual freedoms. In countries where there is mandatory surveillance by using smartphones for tracking, there are consequences for freedom of movement and freedom of occupation.[214] Exposure to an infected person restricted these freedoms.[215] If the information collected by surveillance showed that the person had been near an infected individual, the government could subject him to a quarantine order and isolate him. Such action, however, might be justified in cases of crisis when the state interest in public health permits that breach.[216] Yet, while governments have broad policing power in the area of public health[217] and "are generally allowed to enforce legislation not preempted by federal laws, even emergency and health-protective laws must be consistent with the US [sic] Constitution."[218]

---

oversurveillance, if the data that is collected under the guise of disease prevention is used more broadly.").

[212] *See* KAHN, *supra* note 8, at 71.

[213] *See id.* at 84.

[214] On surveillance and its implications on freedoms, see generally RICHARDS, *supra* note 30.

[215] *See* Charter of Fundamental Rights of the European Union, Dec. 8, 2000, art. 1, art. 16, 2000 O.J. (C 364) 12. This Charter articulates the universal values, such as dignity, solidarity, freedom, and equality, on which the EU was founded. In the United States, an individual's right to conduct a business or pursue an occupation is a property right. *See* Garrison v. Herbert J. Thomas Mem'l Hosp. Ass'n, 438 S.E.2d 6, 14 (W. Va. 1993); United States v. Santoni, 585 F.2d 667, 673 (4th Cir. 1978); United States v. Arena, 180 F.3d 380, 394 (2d Cir. 1999), *abrogated by* Scheidler v. Nat'l Org. for Women, Inc., 537 U.S. 393 (2003).

[216] *See, e.g.*, Rozenshtein, *supra* note 34.

[217] Jacobson v. Massachusetts, 197 U.S. 11, 24–25 (1905).

[218] KAHN, *supra* note 8, at 86–87; *see also Legal Authorities for Isolation and Quarantine*, CTRS. FOR DISEASE CONTROL & PREVENTION (Sept. 17, 2021), https://www.cdc.gov/quarantine/about lawsregulationsquarantineisolation.html; Friedman, *supra* note 33, at 22.

Mass surveillance, however, operates without transparency and due process, and the collection of information is not subject to judicial review.[219] A person can receive a quarantine order to isolate from others without proof that he was in the proximity of an infected person. For example, in Israel, the Shin Bet's (ISA) mass surveillance and quarantine orders led to chaos.[220] "Reports contain[ed] stories of tens of thousands of citizens receiving text messages warning them to quarantine because of their alleged close contact with someone with coronavirus, but many of the messages seem[ed] to be demonstrable mistakes."[221] A person can be quarantined—yet at the time of the claimed exposure to the infected person, he was alone at home[222]—because a neighbor in his building had been infected,[223] even if he was not exposed to him.[224] There were lots of false positives that were quarantined.[225] Furthermore, in states operating a risk scoring

---

[219] In a related context of police digital surveillance, see Bloch-Wehba, *supra* note 79, at 921 (explaining that as police start to use sophisticated technologies, "such as large DNA databases, social media monitoring, and facial recognition[,]" they often do so surreptitiously. The result is that law enforcement surveillance accomplished by means of sophisticated technologies is "often less visible to individual targets, the judicial branch, and the public than their physical counterparts.").

[220] Yonah Jeremy Bob, *Chaotic Start to Shin Bet Corona Surveillance*, JERUSALEM POST (July 5, 2020, 6:54 PM), www.jpost.com/breaking-news/shin-bet-surveillance-led-to-thousands-of-people-getting-covid-19-texts-633959.

[221] *Id.*

[222] *See id.* ("A large volume of citizens has given stories to the media indicating that at the time they were told they came into contact with someone with the virus (time of supposed contact is the only information they are given) they were either asleep at home or alone in their office.").

[223] *See id.* ("Some citizens who say they were misidentified speculated that the Shin Bet tool might have identified them as coming within two meters of someone in their office building who was on a different floor right below them, but that the tool cannot grasp such subtleties.").

[224] VELIZ, *supra* note 62, at 182 ("The app might identify two people being in contact who are in fact on different floors of the same building, or who are on the same floor but separated by a thin wall.").

[225] *See* Dov Greenbaum, *The Algorithm Behind the Jewish High Holidays Is More transparent than Israel's COVID-19 Fighting Tech*, CALCALIST (Sept. 18, 2020), https://www.calcalistech.com/ctech/articles/0,7340,L-3850238,00.html ("From the program's outset, it has been beset with reportedly thousands of false positives, sending healthy and unexposed people to mandatory quarantine and creating further distrust in the government and its various coronavirus fighting methods.").

system,[226] an individual's score can be degraded without justification.[227] As a result of false positives, or erroneous calculation of the scoring algorithm, individuals might be discriminated against and denied entry from shopping centers, public transportation, and other institutions.

Technologies of surveillance are opaque, and citizens have no efficient way to appeal a quarantine order.[228] Decisions on quarantine that denied people their freedom should have been subject to transparency.[229] Failing to provide individuals with a means to contest the factual basis for a decision to isolate them deprives them of due process.[230] Long-term data collectors, whether they belong to governmental agencies around the world or private companies that cooperate with governments, may use black box algorithms to analyze the data they collect from citizens. Their opacity means that individuals do not have any idea how they work and have no opportunity to inspect the data and correct errors. The problem is exacerbated when these algorithms determine too much about freedoms and how individuals will be treated in society; the algorithms can then be used to discriminate against individuals or marginalized groups.[231]

Lack of due process and opportunity to contest the information collected, and conclusions made based on that information, deprives individuals of their constitutional right to due process and procedural

---

[226] For example, see China and the plan to adopt a risk score in Israel that fortunately was not adopted. Regarding China, see Catelijne Muller & Virginia Dignum, *Why the World Should not Adopt Chian QR-Code System*, ALLAY (Nov. 25, 2020), https://allai.nl/op-ed-why-the-world-should-not-adopt-chinas-qr-code-system.

[227] For more information on the risk score to combat COVID-19, see Yablonko, *supra* note 107.

[228] For example, the Israeli Ministry of Health has "been inadequately staffed to field all of the calls from citizens to verify or dispute the text they received" that order them to be isolated. *See* Bob, *supra* note 220.

[229] Transparency ensures the checks on government actions and is consistent with the separation of powers. *See* Bloch-Wehba, *supra* note 79, at 922–23.

[230] On the lack of due process in a scored society based on opaque algorithms, see Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 7–8, 10–11 (2014).

[231] *See* PASQUALE, *supra* note 183, at 165; Citron & Solove, *Privacy Harms*, *supra* note 207, at 857 ("Algorithms that appear neutral often have disproportionate effects on minorities."); Cade Metz & Adam Satariano, *An Algorithm That Grants Freedom, or Takes It Away*, N.Y. TIMES (Feb. 6, 2020), https://www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html.

justice[232] and exposes them to an arbitrary denial of their freedoms.[233] Constitutional norms should not be suspended during the virus outbreak.[234] The public deserves to know what data on them is collected, used, and shared; for how long will it be kept; and whether the privacy invasion is necessary and proportionate to its benefits.[235] The public has the right to due process and procedural fairness. These norms do not dictate substantive outcomes, but rather provide guideposts for decision making.[236]

iii. Surveillance Creep, the Police State, Manipulation, and the Erosion of Democracy

Technology has made it possible for governments "to hoover up unfathomable amounts of information on people: their location, their habits, their expenditures[,] communications, [and] their preferences."[237] COVID-19 was a catalyst for mass surveillance. Public health priorities in quarantine enforcement and contact tracing led states all around the world to adopt exceptional measures.[238] Several governments, such as Israel, used surveillance tools designed for counterterrorism on all citizens.[239] Such surveillance practices pose a major problem for democracy. These practices normalize the deployment of mass surveillance "in countries that have so far rejected them[,]"[240] leading to a constitutional crisis and erosion of democracy.[241]

Data collection during surveillance can expand beyond the response to the virus. A tool designed for one purpose can end up

---

[232] *See* U.S. CONST. amend. V, cl. 4; *id.* amend. XIV, § 1. On the importance of the right to contest, see Margot E. Kaminski & Jennifer M. Urban, *The Right to Consent AI*, 121 COLUM. L. REV. 1957, 1957 (2021).

[233] *See, e.g.*, Massaro et al., *supra* note 4, at 258–59.

[234] *See id.* at 247–48.

[235] *See id.* at 242, 259.

[236] *Id.* at 240.

[237] Friedman, *supra* note 33, at 2.

[238] Arthur PB Laudrain, *Pand-Veillance: COVID-19 Is a Catalyst for Mass Surveillance, and a Wake-Up Call for Privacy & Transparency* 2 (2022) (unpublished manuscript) (on file with author).

[239] *Id.*

[240] *See* Lew, *supra* note 35.

[241] *See* Moshe Maor et al., *When COVID-19, Constitutional Crisis, and Political Deadlock Meet: The Israeli Case from a Disproportionate Policy Perspective*, 39 POL'Y & SOC'Y 442, 447–51 (2020); *see generally* Jacek Lewkowicz et al., *COVID-19 and Erosion of Democracy*, 106 ECON. MODELLING (2022).

being used for another one.[242] In other words, surveillance can creep into a larger toolbox[243] for future health prevention and control.[244] For example, it can be used for tracking individuals that caught seasonal flu[245] or individuals with unhealthy lifestyles.

The creep of surveillance already exists in the private sector. Knowledge is power, and knowledge on customers spells out a potential increase in sales. Governments can collect information and sell it to third parties, like insurance companies, that can misuse health information to discriminate against their clients and charge them differential premiums due to predictions of AI algorithms regarding their risk.[246] Private-sector companies can also misuse the information to interfere with the process of their decision making, as "[h]uman information allows control of human behavior by those who have the know-how to exploit it."[247] Because "surveillance changes [the] power dynamic between the watcher and the watched" and gives the watcher power, it can even create risk of blackmail, discrimination, and coercive persuasion.[248] Such information allows companies to nudge, influence, manipulate, and exploit the watched.[249]

Moreover, mass surveillance and tracking can become a default. Governmental agencies may abuse their authority and use the data collected for illegitimate targeting of individuals for purposes that have absolutely no connection with public health.[250] "The Calcalist" (an Israeli business daily newspaper) recently reported that Israeli police

---

[242] Explaining the term "creep" in the related context of censorship, see Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NORTE DAME L. REV. 1035, 1050 (2018) ("The term creep refers to 'the idea that a tool designed for one purpose ends up being used for another one.' Tools or programs designed to accomplish a particular end or to solve a specific problem are gradually extended to other uses or contexts.").

[243] Tokson & Waldman, *supra* note 23, at 302 ("[A] camera at a four-way intersection may have originally been installed to photograph the license plates of speeders or those who drive through red lights, but it also enables the government to monitor pedestrians using facial recognition technology.").

[244] *See, e.g.*, *id.*; KAHN, *supra* note 8, at 1.

[245] *See* Tokson & Waldman, *supra* note 23, at 302–03; KAHN, *supra* note 8, at 1.

[246] *See* Carmel Shachar et al., *AI Surveillance During Pandemics: Ethical Implementation Imperatives*, 50 HASTINGS CTR. REP. 18, 20–21 (2020).

[247] RICHARDS, *supra* note 30, at 76.

[248] *Id.* at 134.

[249] *Id.* at 153 ("Data-driven personalized political persuasion is already being deployed against voters. One of the ways campaigns use data to persuade is through 'microtargeting.'").

[250] Bradford et al., *supra* note 7, at 15.

used the notorious NSO spyware to spy on citizens, mayors, political leaders, and protesters against the government.[251] Investigations and a report by the deputy attorney general ("The Merari report") found the allegations to be largely false[252] and, recently, the Israeli government investigators found in the final report that there was no indication that the police *illegally* hacked the phones of Israelis mentioned in the media by using the Pegasus spyware of the Israeli company NSO Group.[253] The investigation, however, found that the police did use the spyware and gained access to information beyond the information that the police was allowed to have, such as calendar entries and phone contact lists.[254] Furthermore, the very use of the spyware is problematic. An order, in accordance with the Israeli Wiretapping Law,[255] does not solve this problem because such orders allowing for bugging of conversations are unfit to accommodate data that is not a part of a conversation; therefore, there is no clear legal basis for using spyware.[256] Beyond the NSO scandal, it should be noted that Israel advances mass collection of information through proposing a bill that would allow facial recognition cameras in public.[257]

---

[251] Tomer Ganon, *Israel Police Uses NSO's Pegasus to Spy on Citizens*, CALCALIST (Jan. 18, 2022), https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html.

[252] *Bill to Probe Police Spying Scandal Passes Preliminary Reading in Knesset*, ISR. HAYOM (May 12, 2022, 7:33 AM), https://www.israelhayom.com/2022/05/12/bill-to-probe-police-spying-passes-preliminary-reading-in-knesset.

[253] *See* Chen Maanit, *NSO Investigation: Israel Police Exceeded Authority, but Didn't Illegally Hack Phones*, HAARETZ (Aug 1, 2022) http://ty-article/.premium/nso-investigation-israel-police-exceeded-orders-but-didnt-illegally-hack-phones/00000182-52de-d438-aba7-52fed7ae0000.

[254] *Id.*

[255] § 10A, Wiretapping Law (Isr.).

[256] Yuval Shany, *Stay Calm and Proceed with Caution: The Merari Report on Israeli Police's Pegasus Scandal*, LAWFARE (Aug. 25, 2022), https://www.lawfareblog.com/stay-calm-and-proceed-caution-merari-report-israeli-polices-pegasus-scandal ("The Merari report explains that the Wiretapping Law only permits surveillance of communications in transit, and that permissible monitoring activity pursuant to it must take place in real time or near real time—namely, it permits interception through surveillance undertaken in close temporal proximity to the time of the communication in question and does not permit the tracing back of the historical record of communications of individuals under surveillance. . . . Indeed, prominent experts in Israeli privacy law have maintained that given the dramatic impact of such technology on the right to privacy, the police cannot justify the utilization of spyware on the basis of existing legislation developed with much less intrusive technology in mind.").

[257] Noa Shpigel, *Israel Advances Use of Face-Recognition Cameras in Public*, HAARETZ (May 9, 2022), https://www.haaretz.com/israel-news/.premium-israel-advances-use-of-face-recognition-cameras-in-public-1.10787476.

Mass surveillance, collection, and analysis of data already takes place and can infringe on freedom of speech and the right of association.[258] For example, they can be used for collecting information on political activists.[259] Such mass collection can be used to target political opponents and quarantine them at the time of anti-government protests. Governments can justify this action by reasoning that they had been exposed to a COVID-19 carrier and should be isolated for public health protection, regardless of whether they were actually exposed to an infected person. The use of facial recognition technology can also extend beyond combating the virus. Such technology can be used to stop resistance against governments, oppress protests, arrest people that participate in demonstrations, and infringe on human rights.[260] Such systems can even analyze faces and draw insight on emotional expressions and personality traits.[261] Further, the fact that Microsoft decided to limit the use of their facial-recognition systems by refusing to sell them to police departments until passage of a federal law regulating the technology proves the technology's risks.[262] Moreover, the EU's recently proposed regulation regarding the use of AI even bans real-time remote biometric identification in public places because such identification poses a high risk to liberties.[263] Data collection and analysis allows for accurate

---

[258] On mass surveillance and the right of association, see Friedman, *supra* note 33, at 31.

[259] *See, e.g.*, Eder Campuzano, *Homeland Security Characterizes Portland's Anti-Trump Riot as 'Terrorist Violence:' Report*, OREGONIAN (Mar. 3, 2017, 2:25 AM), https://www.oregonlive.com/portland/2017/03/homeland_security_calls_portland_trump_riot_domestic_terrorist_violence.html; Friedman, *supra* note 33, at 37.

[260] Eldar Haber, *Racial Recognition*, 43 CARDOZO L. REV. 71, 100 (2021) ("[B]oth Miami police and the NYPD used facial recognition to track down Black Lives Matter activists."); *see also* Kate Cox, *Cops in Miami, NYC Arrest Protesters from Facial Recognition Matches*, ARSTECHNICA (Aug. 19, 2020, 4:45 PM), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches.

[261] KATE CRAWFORD, ATLAS OF AI 154 (2021).

[262] *See* Jay Greene, *Following Amazon and IBM, Microsoft Won't Sell Police Its Facial-Recognition Tech*, SPOKESMAN-REV. (June 11, 2020), https://www.spokesman.com/stories/2020/jun/11/following-amazon-and-ibm-microsoft-wont-sell-polic.

[263] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, art. 5(1)(d), COM (2021) 206 final (Apr. 21, 2021). For further information, see Denise Almeida et al., *The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: a Comparative Analysis of US, EU, and UK Regulatory Frameworks*, 2 AI & ETHICS 377 (2022); Margot E. Kaminski, *Regulating the Risks of AI*, 103 B.U. L. REV. (forthcoming 2023) (at 49–54), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4195066.

targeting of individuals that are prone to supporting the government, influencing their consciousness, and manipulating them to advocate for a specific candidate on an election cycle and even volunteer in the campaign. Much like Cambridge Analytica, a company that developed the model for predicting the behavior of voters and targeting political messages,[264] governments can abuse surveillance to influence voters instead of preserving the public's health.

"Exceptional circumstances are political windows of opportunity for deploying new surveillance tools and practices . . . ."[265] "Governments that have acquired new powers to monitor and control their citizenry to meet a temporary need are loathed to give them up."[266] "For example, shortly after the 9/11 terrorist attacks in the [United States], its government passed the USA Patriot Act of 2001, giving it 'temporary surveillance powers.'"[267] Almost two decades later, "the [United States] government has retained most of these powers."[268] Moreover, the National Security Agency (NSA) has been gathering records of online sexual activities and visits to pornographic websites "as part of a proposed plan to harm the reputations of those whom the agency believes are radicalizing others through incendiary speeches."[269] The NSA wanted to surveil "radicalizers" who are not terrorists, "but merely radical critics of U.S. policy."[270] "It also raises troubling questions about the government's ability and willingness to blackmail its critics for nothing more than sincerely speaking on core matters of political speech protected by the First Amendment."[271]

"In the digital age, privacy against the state remains an essential part of political freedom."[272] As history can repeat itself, mass surveillance can continue on the axis of time even when the risk of

---

[264] *See* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[265] Laudrain, *supra* note 238, at 2.

[266] *See* Andrew Urbaczewski & Young Jin Lee, *Information Technology and the Pandemic: A Preliminary Multinational Analysis of the Impact of Mobile Tracking Technology on the COVID-19 Contagion Control*, 29 EUR. J. INFO. SYS. 405, 410 (2020).

[267] *See id.*

[268] *See id.*

[269] Glenn Greenwald & Ryan Grim, *Top-Secret Document Reveals NSA Spied on Porn Habits as Part of Plan to Discredit 'Radicalizers'*, HUFFPOST (Nov. 26, 2013, 11:20 PM), https://www.huffpost.com/entry/nsa-porn-muslims_n_4346128.

[270] RICHARDS, *supra* note 30, at 131.

[271] *Id.* at 132.

[272] *Id.* at 133.

health due to COVID-19 is over. The danger of such surveillance practices, in both democratic societies and others, is that they do not roll back once the emergency is over. In fact, the "pandemic industry" that magnifies the crisis can lead to permanent changes in the state-citizen relationship, as a strong state response requires new powers and resources that persist in the post-crisis period. "[T]he costs of government responses to health crises are often long lasting, variable, and unseen meaning that the overall costs of government responses will tend to be understated."[273]

The erosion of democracy is expected to become much worse with the possibilities of surveillance that can transit from "over the skin" and focus on what we do, where we go, who we meet to "under the skin" by using technologies that can reveal what happens inside our body—our body temperature, blood pressure, heart rate, and even how we feel.[274] This technology became a reality. In Sweden, thousands have already inserted microchips into their hands, aiming to use them "to speed up users' daily routines."[275] For example, microchips allow for fast access to the office building without using a badge, buying food at the cafeteria, or gaining secure access to the computer at work.[276] As microchips develop, they might be able to evaluate physical body measurements and not only store information.[277] Even before microchips, the growing use of the Internet of Things (IoT) technologies enabled unprecedented

---

[273] Christopher J. Coyne & Yuliya Yatsyshina, *Pandemic Police States*, 26 PEACE ECON., PEACE SCI. & PUB. POL'Y, Sept. 2020, at 4.

[274] *See* Anna Carthaus, *The Biggest Danger is not the Virus Itself*, DW (Apr. 22, 2020), https://www.dw.com/en/virus-itself-is-not-the-biggest-danger-says-yuval-noah-harari/a-53195552.

[275] *See* Ahmed Banafa, *Technology Under Your Skin: 3 Challenges of Microchip Implants*, BBVA: OPENMIND (Apr. 5, 2021), https://www.bbvaopenmind.com/en/technology/innovation/technology-under-your-skin; Mandi Heshmati, *COVID-19: In Sweden, a Vaccine Passport on a Microchip Implant*, FR. 24 (Dec. 21, 2021, 4:22 PM), https://www.france24.com/en/video/20211221-covid-19-in-sweden-a-vaccine-passport-on-a-microchip-implant.

[276] *See* Rachel Metz, *This Company Embeds Microchips In Its Employees, and They Love It*, MIT TECH. REV. (Aug 17, 2018) https://www.technologyreview.com/2018/08/17/140994/this-company-embeds-microchips-in-its-employees-and-they-love-it; A. Spender et. al, *Wearables and the Internet of Things: Considerations for the Life and Health Insurance Industry*, 24 BRIT. ACTUARIAL J. 1, 23 (2019) ("Sweden has already offered microchips to employees of the start-up companies based there, and people did volunteer. The chips allow employees to unlock doors, operate printers, open storage lockers and even buy smoothies with the wave of a hand.").

[277] Spender et. al, *supra* note 276 ("The ability of chip implants to start tracking and measuring health stats on a large scale is closer than we think.").

invasive surveillance on a scale like never before.[278] Biometric information, collected by sensors in such devices, can tell governments far more about individuals than ever before. Traditional technological surveillance focused on monitoring actions in the world—where an individual goes, who he meets, and so on. Governments, however, have become more interested in what is happening inside the body and brain.[279] By using our growing understanding of the human body and brain, combined with the immense powers of machine learning, governments in the future might be able to "hack" the human body and gain knowledge on citizens' authentic feelings and emotions. A person could smile and clap his hands mechanically, but if he is actually angry, the government will know.[280]

Every step of state surveillance to combat COVID-19 leads to another and can creep to other areas of life in a slippery slope, cascading into a significant negative effect that erodes democracy. Right now, going under the skin,[281] at the service of "the thought police"—the agency which knows everything about a person and punishes them for a thought crime—seems similar to the Orwellian dystopia.[282] The idea of microchips under the skin, however, is already a reality. Sweden has even employed microchips loaded with citizens' COVID-19 vaccination certificates.[283] Governments are starting to paddle towards such ideas of going under the skin in related contexts. For example, Benjamin Netanyahu, Israel's former Prime Minister, proposed to "microchip" children who returned to schools and kindergartens as the COVID-19 lockdown was lifted, in an effort to ensure social distancing.[284] Experts slammed this proposal as unenforceable, inefficient, and risky, citing the potential misuse of

---

[278] Marie-Helen Maras et al., *Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things*, 4 J. CYBER POL'Y 160 (2019) (explaining that the Internet of Things "facilitates perpetual surveillance of populations. This form of surveillance is made possible because IoT devices record and transmit a massive amount of data that is being shared and analysed in new and unique ways to enable the ubiquitous monitoring of individuals.").

[279] *See* Lew, *supra* note 35.

[280] *Id.*

[281] Harari, *The World After Coronavirus*, *supra* note 6 (referring to under-the-skin surveillance).

[282] GEORGE ORWELL, 1984 12 (1949); *see generally* Varun Chikale, *1984 – George Orwell*, 2 JUS CORPUS L.J. 29 (2022) (book review).

[283] *See* Heshmati, *supra* note 275.

[284] Leon Sverdlov, *Benjamin Netanyahu Suggests Microchipping Kids, Slammed by Experts*, JERUSALEM POST (May 8, 2020, 2:46 PM), https://www.jpost.com/israel-news/benjamin-netanyahu-suggests-to-microchip-kids-slammed-by-experts-627381.

children's personal information.[285] The fact that such an Orwellian idea was even proposed demonstrates that the dystopic future described in *1984*[286] may already be here.

During times of crisis, citizens are distracted, scared, and "more at the mercy of their leaders. Too often, that ends up being a bad combination for democracy."[287] Such exigent circumstances "are taken advantage of to impose new norms that would never have been tolerated by the citizenry in less exceptional times."[288]

V. ENJOYING HEALTH AND PREVENTING THE EROSION OF CIVIL RIGHTS AND LIBERTIES

Privacy is a fundamental right. In the EU Charter of Fundamental Human Rights (ECHR), Article 7 (entitled "Respect for Private and Family Life") proclaims that "[e]veryone has the right to respect for his or her private and family life, home and communications."[289] "Article 8 of the Charter (entitled 'Protection of Personal Data') introduced a new categorical recognition of the rights to data privacy by stating that 'Everyone has the right to the protection of personal data concerning him or her.'"[290]

Many EU Member States, however, introduced states of emergency to respond to the COVID-19 crisis, which allowed certain rights to be limited.[291] Several EU Member States additionally made new declarations of states of emergency, while others prolonged states

---

[285] *Id.*

[286] *See* ORWELL, *supra* note 282, at 5. For further information on the dystopia of surveillance, see Jon Miltimore, *The Origins of the Thought Police—and Why They Scare Us,* FOUND. FOR ECON. EDUC.: STORIES (Nov. 15, 2019), https://fee.org/articles/the-origins-of-the-thought-police-and-why-they-scare-us.

[287] VELIZ, *supra* note 62, at 202–10.

[288] *Id.* at 185.

[289] Charter of Fundamental Rights of the European Union, Oct. 26, 2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (last visited Oct. 6, 2022).

[290] Charter of Fundamental Rights of the European Union, art. 8; Federico Fabbrini, *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court, in* THE EU CHARTER OF FUNDAMENTAL RIGHTS AS A BINDING INSTRUMENT: FIVE YEARS OLD AND GROWING 261, 267 (Sybe de Vries, Ulf Bernitz, & Stephen Weatherill eds., 2015).

[291] EUR. PARL. RSCH. SERV., STATES OF EMERGENCY IN RESPONSE TO THE CORONAVIRUS CRISIS (2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/659385/EPRS_STU(2020)659385_EN.pdf (explaining such states of emergency ranges were "generally renewable. The legislation underpinning the declared states of emergency allowed governments to restrict fundamental rights").

of emergency that were declared earlier when the virus started to spread. "Around a third of EU Member States extended existing states of emergency" as the spread of the virus continued in early 2020.[292]

In resemblance to the EU, the United States protection against state surveillance is also a constitutional right. The Fourth Amendment protects people from warrantless searches.[293] Under exigent circumstances, however, a warrant is unfeasible.[294] Thus, for many public health purposes, strict adherence to a warrant regime may not be required. Any disease surveillance program is likely to be evaluated under the Fourth Amendment's special needs doctrine (also called the "administrative search doctrine"), by which courts sometimes permit warrantless surveillance.[295] This might happen if getting a warrant would be impracticable, the search is aimed at something other than a traditional law enforcement purpose, and the search is considered reasonable.[296] In their battle against the virus, however, governments collect information on individuals without suspicion that the individual has contracted the virus.[297] "A robust contact tracing program would thus raise constitutional concerns . . . ."[298] Yet even in the United States, courts tend to give the government much more leeway in emergencies.[299] A pandemic is likely to be treated similarly, especially at the beginning when there is less information and courts have little basis to question government representations about necessity or effectiveness. "On the other hand, emergency powers are not limitless."[300]

---

[292] EUR. UNION AGENCY FOR FUNDAMENTAL RTS., CORONAVIRUS PANDEMIC IN THE EU – FUNDAMENTAL RIGHTS IMPLICATIONS: WITH A FOCUS ON CONTACT-TRACING APPS 8 (2020), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf.

[293] U.S. CONST. amend. IV. *See also* United States v. Jones, 565 U.S. 400, 404 (2012); Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

[294] Rozenshtein, *supra* note, *supra* note 34.

[295] *See* Friedman, *supra* note 33, at 34–35

[296] Rozenshtein, *supra* note 34, at 1541 (2021); Friedman, *supra* note 33, at 34 & n.185 (referring to Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)); Geoffrey S. Corn, *Deterring Illegal Firearms in the Community: Special Needs, Special Problems, and Special Limitations*, 43 CARDOZO L. REV. 1515, 1530–31 (2022).

[297] Rozenshtein, *supra* note 34, at 1520.

[298] Rozenshtein, *supra* note 32.

[299] *Id.*

[300] *Id.* (expanding on the safeguards that can be built into emergency powers that might limit abuse, "courts may give the government more leeway when the action is taken pursuant to a formal invocation of emergency, especially the legislature ratifies it. Sunset clauses (as in the United Kingdom's recently enacted Coronavirus Act) can provide an assurance that emergency powers will not be permanent. Transparency as

So, must people choose between civil rights and health? This Part argues no. The legitimate end of protecting health should be pursued by using rational means. The means must be reasonably tailored to the legitimate end of protecting health while avoiding over- or under-inclusion and minimizing damage, such as chilling effect on speech, infringement of intellectual privacy, discrimination, and stigma.[301] With the right design, safeguards, transparency, due process, and oversight, both civil rights and public health may be served, thereby avoiding the erosion of democracy. The following subsections focus on measures to protect civil rights while also protecting health and preventing the rise of the surveillance state.

A. *Privacy (and Other Values)-By-Design*

In recent years, there has been an increasing use of technology-based solutions to prevent the infliction of privacy harm. Studies emphasize "the power of architecture to account for human values and technology user rights 'in a principled and comprehensive manner throughout the design process,"[302] for example, by implementing the approach of "Value Sensitive Design that identifies human needs and values and needs and takes them into account in the design process."[303] Engineers make decisions that can unleash new technologies that the legislature did not foresee, decisions that may affect fundamental rights. Scholarly work has already explored the influence of technological governance systems and their potential to protect

---

to how the program is operating can increase accountability to the general public and civil society watchdog groups. And, above all, the emergency response must be limited to what is necessary to deal with the emergency; courts will (or at least should) examine the government program for 'surveillance creep.'").

[301] Massaro et al., *supra* note 4, at 242, 246; *see also* Lee, *supra* note 123, at 23 (referring to "(i) the legitimacy of the purpose, (ii) the adequacy of the method for achieving the goal, (iii) the minimum of damage, and (iv) the balance of legal interests between the public interest to be protected by the legislation and the fundamental right to be infringed.").

[302] Michal Lavi, *Publish, Share, Re-Tweet, and Repeat*, 54 U. MICH. J.L. REFORM 441, 494 (2021) (quoting Deirdre K Mulligan & Jenifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 1019 (2012) (quoting Batya Friedman et al., DEP'T OF COMPUT. SCI. & ENG'G, UNIV. OF WASH., CSE TECHNICAL REPORT NO. 02-12-01, VALUE SENSITIVE DESIGN: THEORY AND METHODS (2002)).

[303] *Id.* at 494 n.351 (2021) (quoting Michal Lavi, *Do Platforms Kill?*, 43 HARV. J.L. & PUB. POL'Y 477, 553 n.504 (2020) (citing Noemi Manders-Huits & Jeroen van den Hove, *The Need for Value-Sensitive Design of Communication Infrastructures*, *in* EVALUATING NEW TECHNOLOGIES 51, 54–55 (Paul Sollie & Marcus Duwell eds., 2009); *see, e.g.*, Deirdre K Mulligan & Jenifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989 (2012).

privacy.[304] This concept of privacy-by-design was developed into a philosophy that focuses on ex ante regulation of the technological design instead of ex post remedies.[305] Researchers have described how to make privacy-protective features, a core part of functionality, and how to accommodate threats to privacy.[306] Regulators around the world have discovered the benefits of privacy-by-design. In discovering these benefits, the regulators have set forth guidelines and promoted legal regulations that include privacy-by-design and have made efforts to incentivize stakeholders to adopt this approach as part of their business models.[307]

A central example is Article 25 of the EU Data Protection Regulation ("GDPR") which addresses "[d]ata protection by design and default."[308] Article 25 advocates for building privacy-friendly

---

[304] *See, e.g.*, ANDY CRABTREE ET AL., PRIVACY BY DESIGN FOR THE INTERNET OF THINGS: BUILDING ACCOUNTABILITY AND SECURITY (2021). Eric Everson, *Privacy by Design: Taking Ctrl of Big Data*, 65 CLEV. ST. L. REV. 27 (2017), https://engagedscholarship.csuohio.edu/cgi /viewcontent.cgi?article=3933&context=clevstlrev; Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1419, 1422 (2011); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 418 (2013).

[305] Privacy by design is an approach that incorporates thinking about privacy protective features and implementing them as early as possible. *See* HOOFNAGLE, *supra* note 38, at 190–92 (2016); BAMBERGER & MULLIGAN, *supra* note 38, at 32, 178; CAVOUKIAN, *supra* note 38, at 3.

[306] *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1419, 1422 (2011); Hartzog & Stutzman, *Obscurity by Design*, *supra* note 304, at 418 (referring to a narrow approach to privacy (obscurity of data) and overview of strategies to protect privacy by design); Serge Egelman et al., *Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators, in* CHI '09: PROCS. OF THE SIGCHI CONF. ON HUMAN FACTORS IN COMPUTING SYS. 319, 319 (2009).

[307] *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 22–30 (2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf; HOOFNAGLE, *supra* note 38, at 191 ("[t]he FTC is embracing [privacy by design]"); *see also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 12, COM (2010) 609 final (Nov. 4, 2010); Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why A 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 77 (2017).

[308] Council Regulation 2016/679, art. 25, 2016 O.J. (L 119) 1, 48 (EU). The General Data Protection Regulation that came into force in 2018 subjects "controllers" to a broader right to erasure. *Id.* art. 17, at 43–44. *See also* Edwards & Veale, *supra* note 307, at 77; Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard,* 71 FLA. L. REV. 365, 419–20 (2019).

systems starting at the beginning of the design process.[309] Accordingly, controllers of data must implement "appropriate technical and organizational measures" to protect the rights of data subjects, both at the stage of system development as well as at the stage of actual processing. In particular, "data protection by default" is required so that only personal data necessary for processing are gathered. "Typical implementations of [privacy] by design and data protection by design are the anonymi[z]ation and pseudonymization of personal data, a data minimi[z]ation approach during processing and storing data, storage limitation, transparency regarding processing, and limited access to personal data."[310] The GDPR's "principle-based approach offers a functional blueprint for system design that is compatible with fundamental rights."[311]

By contrast, in the United States, sector-specific rules are much narrower. For example, the U.S. Health Insurance Portability and Accountability Act (HIPAA) "applies only to data collected by health providers themselves, or businesses hired by health providers to process their data."[312] "An individual's diagnosis from a diagnostic lab would, therefore, be subject to HIPAA[]. . . but a Bluetooth exposure proximity system falls completely outside HIPAA's parameters."[313] Moreover, in the battle against COVID-19, the Department of Health and Human Services ("HHS") is exercising discretion in how HIPAA "[a]llow[s] [u]ses and [d]isclosures of [p]rotected [h]ealth

---

[309] Edwards & Veale, *supra* note 307, at 77 (explaining that by doing so, it "recognize[s] that a regulator cannot do everything by top down control, but that controllers must themselves be involved in the design of" systems that minimize invasion of privacy).

[310] Oliver Vettermann, *Self-Made Data Protecton – Is it Enough? Prevention and After-care of Identity Theft*, 10 EUR. J.L. & TECH. 1, 9 (2019); *see* Edwards & Veale, *supra* note 307, at 77.

[311] Bradford et al., *supra* note 7, at 1.

[312] *Id.* at 9–10 (citing HIPAA § 262(a); Standards for Privacy of Individually Identifiable Health Information, 64 FED. REG. at 59,918); *see* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 1001–02 (2021) ("HIPAA's main problem is that it does not apply to a broad enough category of relationships. Thus, it does not protect disclosed data outside of 'covered entities' or their 'business associates.'").

[313] Bradford et al., *supra* note 7, at 1 (citing Carmel Shachar, *Protecting Privacy in Digital Contact Tracing for COVID-19: Avoiding a Regulatory Patchwork*, HEALTH AFFS. BLOG (May 19, 2020), https://www.healthaffairs.org/do/10.1377/hblog20200515.190582/full.

[i]nformation by [b]usiness [a]ssociates for [p]ublic [h]ealth," including transferring the information to third parties.[314]

Although HIPPA's protection of personal data is relatively narrower than the GDPR, the GDPR has a long-arm jurisdictional reach. The GDPR protects data of EU citizens, yet also applies to non-EU companies that offer goods or services to EU consumers. Thus, it can also affect data protection in the U.S. and throughout the world.[315] The GDPR also contains a threshold test for "international transfers of personal data" to non-member states and a legal basis for blocking data exports to states that do not meet this standard.[316] The threshold for extraterritorial transmissions is the "*adequacy*" of data protection in the foreign jurisdiction.[317] Instead of an adequacy determination, the EU and United States have reached an agreed called "Privacy Shield"— a voluntary private sector program—for transmissions to the United States.[318] This bilateral agreement presented a list of "substantive EU principles for American companies to follow voluntarily."[319] Yet, the

---

[314] *See* DEP'T OF HEALTH & HUMAN SERVS., *Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19*, www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf (last visited Oct. 10, 2022).

[315] Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 810 (2019) ("[The EU's] power in this regard first developed in response to issues that it faced internally. It needed to harmonize the data processing practices of EU member states. The inward-facing elements of EU data protection law then became an important factor in its adaptability to the rest of the world. Here is a global diffusion story that begins with a response to internal political considerations.").

[316] *See* Anupam Chander et al., *Catalyzing Privacy Law,* 105 MINN. L. REV. 1733, 1739 (2021); Schwartz, *supra* note 315, at 774.

[317] *See* Schwartz, *supra* note 315, at 785 ("In Article 45, the GDPR requires that the Commission consider a long list of factors in assessing the adequacy of protection, including 'the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, . . . as well as the implementation of such legislation, data protection rules, professional rules and security measures.'").

[318] The privacy shield replaced the safe haven agreement. In *Schrems v. Data Protection Commissioner*, the ECJ declared that this safe harbor was invalid. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:2015:650, ¶ 216 (June 10, 2015). Following this decision, the United States and the European Union reached a new arrangement called the Privacy Shield. It should be noted that the legal future remains uncertain and is dependent on the outcome of another ruling by the CJEU. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd., ECLI:EU:C:2019:1145, ¶ 44–45 (July 16, 2015); *The Schrems Saga Continues: Schrems II Case Heard Before the CJEU*, HUNTON PRIV. BLOG (July 10, 2019), https://www.huntonprivacyblog.com/2019/07/10/the-schrems-saga-continues-schrems-ii-case-heard-before-the-cjeu.

[319] Schwartz, *supra* note 315, at 795; *Schrems*, ECLI:EU:2015:650, at ¶ 17.

European Court of Justice (ECJ) in Luxembourg recently struck down the privacy shield in *Data Protection Commissioner v. Facebook Ireland*.[320] The court determined that the Privacy Shield agreement did not limit access to data by U.S. authorities "in a way that satisfies requirements that are essentially equivalent to those required under EU law."[321] The principles of the GDPR have global impact today, more than ever, and can influence the engineering of privacy outside of Europe.[322] Adopting the concept of privacy-by-design will allow the industry and policy makers to adhere to cross jurisdictional legal standards and prevent the relinquishing of the right to privacy.

Inserting privacy and security safeguards into the architecture of technology builds protection into the design rather than counting on responsible use alone. Focusing on the design maximizes public health while respecting and promoting other values[323] as well as reducing the arising harm ex ante.[324] Adopting the concept of privacy-by-design will not only protect the right to privacy, it will also promote civil rights and prevent the erosion of democracy. The following subsection will overview a few models of surveillance used to combat COVID-19. It will demonstrate how privacy-by-design could protect health, values of privacy, and make it difficult for the surveillance state to rise.

---

[320] *See Data Prot. Comm'r*, ECLI:EU:C:2020:559, at ¶342.

[321] *Id. See also* Victoria Neiazy, *Invalidation of the EU–US Privacy Shield: impact on Data Protection and Data Security Regarding the Transfer of Personal Data to the United States*, 2 INT. CYBERSECURITY L. REV. 27, 28 (2021) ("[T]he Privacy Shield is no longer a valid transfer basis. According to the CJEU companies can still base their transfer on standard contractual clauses (SCCs) or other transfer tools under Article 46 of the General Data Protection Regulation (GDPR), but will have to review in each case whether this is sufficient. If that is not the case, they need to apply additional supplementary measures.").

[322] *See* Beata A. Safari, *Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection*, 47 SETON HALL L. REV. 809, 816–20 (2017); Schwartz, *supra* note 315, at 777–78.

[323] Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance-By-Design*, 106 CALIF. L. REV. 697, 721 (2018); Ari Ezra Waldman, *Privacy's Law of Design*, U.C. IRVINE L. REV. 1239, 1242 (2019) ("Design's significant, yet invisible, capacity to manipulate those who exist inside its ecosystem requires us to consider the values we want design to promote.").

[324] ALI ET AL., *supra* note 8, at 50–53.

1. Smartphone Contact Surveillance

i. Compulsory Surveillance—No Privacy, No Trust

In their battle against COVID-19, states used cell phone location data to track population movement because when the outbreak of the virus started, governments believed it would reduce the infection rate. By doing so, they violated the right to privacy because surveillance can reveal information on a person's health, location, contacts, and allow for drawing conclusions on their interpersonal connections. When health information, as well as information of location and interactions, is transferred between a government and the respective department of health and human services without their consent, the infrastructure of the surveillance tool and architecture does not consider the value of privacy. A prominent example of this practice is the mandatory surveillance of the Shin Bet Israel's Security Agency (ISA) in Israel, which tracks location data from mobile phones that the Israeli government collected and used without consent.[325] Such a location-based tracking system collects huge amounts of information and keeps it without considering principles of data minimization[326] and privacy in the design. Thus, this model promotes the rise of the surveillance state.

ii. GPS Location-Based Surveillance—the Model of Israel Ministry of Health "HaMagen"—One Step Further in Privacy Protection

In addition to compulsory government surveillance tools, the Ministry of Health in Israel launched "HaMagen" ("The Shield").[327] Such a voluntary app was one step closer to privacy-by-design but is still inferior to Bluetooth-based contact tracing apps, to be discussed below. This app was based on GPS smartphone location. The app had

---

[325] *See* Bandel, *supra* note 92; KAHN, *supra* note 8, at 37 ("Israel also implemented a centralized involuntary data collection system for tracking COVID-19 cases and alerting those who may have been exposed."); *see generally* Shaul A. Duke, *Understanding the Apathy Towards the Israeli Security Agency's COVID-19 Surveillance*, 19 SURVEILLANCE & SOC'Y 114 (2021).

[326] For the obligation of data minimization under E.U. Law, see Regulation 2016 /679 of the European Parliament and of the Council of Apr. 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119) 1, art. 5 [hereinafter GDPR].

[327] Press Release, The Ministry of Health, The Ministry of Health Launches "HAMAGEN" - an App to Prevent the Spread of Coronavirus (Mar. 22, 2020), https://www.gov.il/en/departments/news/2203202004.

an open code, which enabled transparency and inspection for everyone to see that the declarations of the Ministry of Health regarding avoiding collection of information were kept.[328] HaMagen obtained and compared, but did not share, location data from users' phones with a central server that contained the location histories of confirmed cases—no data was shared before diagnosis. The diagnosed users, however, "will be notified and given the option of reporting their exposure to the Health Ministry by filling out a form; subsequently, their location trails are released to public."[329] Tracking location is dangerous for privacy purposes because a person's location can tell a lot about them. Although HaMagen only processed users' location data on their smartphone devices, the system relied on pushing the location data of all infected users within the Israeli government servers to all users in the system. Thus, there was a centralized element of stored information on the routes of infected people. Hence, the location data of infected people was not protected, as "it expose[d] infected individuals to re-identification risk by pushing their identifiers to all edge devices for local matching."[330]

iii. The Apple/Google Bluetooth Contact Tracing App: Applying Privacy-by-Design

A third model is contact tracing apps, which are based on Bluetooth proximity exposure notification. The best example is the planned Google/Apple Contact Tracing App for exposure notification services.[331] The Google/Apple app allowed iPhone or Android devices to detect other devices that had been within a certain distance for a significant duration. That "handshake" causes unique identifier codes to be stored, in an encrypted form, on both devices.[332] If someone subsequently tested positive for COVID-19, that person uploaded information centrally to an app server together with their unique

---

[328] Press Release, The Ministry of Health, Israel: Ministry of Health launches HaMagen 2 Contact Tracing App, (July 28, 2020), https://www.dataguidance.com/news/israel-ministry-health-launches-hamagen-2-contact.

[329] *See* RUOXI SUN ET AL., VETTING SECURITY AND PRIVACY OF GLOBAL COVID-19 CONTACT TRACING APPLICATIONS 3 (2020), arxiv.org/abs/2006.10933.

[330] *See* DAVID STURZENEGGER ET AL., CONFIDENTIAL COMPUTING FOR PRIVACY-PRESERVING CONTACT TRACING 2 (2020), arxiv.org/abs/2006.14235.

[331] *Privacy-Preserving Contact Tracing*, APPLE, www.apple.com/covid19/contacttracing (last visited Oct. 6, 2022).

[332] *See Exposure Notification*, APPLE/GOOGLE (Apr. 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf; KAHN , *supra* note 8, at 37–38.

identifier codes. The app "download[ed] positive diagnosis identifier codes daily and . . . match[ed] them with codes stored on individual devices."[333] A match generated an automatic notification from the app that appeared on any device that recorded the infected individual's device identifier(s) during the relevant time period. Information about exposure events largely stayed on each user's phone, while the central server processed only "de-identified" information about individuals with a positive diagnosis.[334] The decentralized architecture of the app ensured continued adherence to a high standard of privacy and security.[335] There was anonymization of information and no data retention on a central server, which safeguarded government abuses of the information.[336] Standards of privacy-by-design were also more likely to be in line with data protection laws.

In the United States, HIPAA[337] applies only to data collected by health providers themselves or businesses hired by health providers to process their data. Google and Apple's Bluetooth exposure proximity system fell outside of HIPAA's parameters.[338] A Google/Apple app, however, could not escape the long-arm limitations and restrictions posed by the EU's GDPR.[339] This regulation is relevant to the United States because it extends to non-EU companies that offer goods or services to EU consumers. It applies to personal data that has "any information relating to an identified or identifiable natural person."[340] GDPR limitations and restrictions apply to "personal data" that is "any

---

[333] Bradford et al., *supra* note 7, at 3; KAHN, *supra* note 8, at 38.

[334] Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33–35 (2010). (explaining that "deidentification means that personal information has been processed in some fashion to reduce the ability to identify the individuals to whom the data refer"); Bradford et al., *supra* note 7, at 3 ("Information about exposure events largely stays on each user's phone, while the central server and ENS process only 'de-identified' information about individuals with a positive diagnosis.").

[335] *See* Ronald L. Rivest et al., *PACT: Private Automated Contact Tracing*, MASS. INST. TECH. (May 19, 2020), pact.mit.edu/wp-content/uploads/2020/05/PACT-Mission-and-Approach-2020-05-19-.pdf.

[336] *See* Urbaczewski & Lee, *supra* note 266, at 406 (explaining that without safeguards "[i]t is also not clear if the data collected would be protected from other uses by other government agencies"). On data retention and privacy, see generally Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 602 (2019).

[337] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[338] Bradford et al., *supra* note 7, at 7.

[339] *See generally* sources cited *supra* note 308.

[340] GDPR art. 4(1).

information relating to an identified or identifiable natural person."[341] If, however, anonymization is fully achieved, the data does not relate to an identified person anymore.[342] "Apple and Google claim that user data broadcasted through their app has been 'anonymized' by virtue of deidentification and decentralization."[343] If the goal of full anonymization is achieved, the data subject is no longer identifiable, and Google/Apple apps are not subjected to data protection obligations under the GDPR. Data anonymization, however, "is a very high bar and data controllers often fall short of actually anonymizing data."[344] Information is considered anonymized, and outside of the reach of the GDPR, only if the information cannot be associated with a natural individual, taking into account the means reasonably likely to be used, including the available technology at the time of the processing and other technological developments.[345] Yet, as more technologies of de-anonymization develop, "users can never be confident that data shared 'anonymously' will not be associated with them in the future."[346]

"Data controllers equally cannot be sure that they will not be found liable for failing to protect de-identified data."[347] Therefore, although Google and Apple anonymize the data processed through the app, "they have still instituted multiple controls to prevent re-identification in their design, in keeping with the GDPR's data minimisation and security of processing principles."[348] "These controls result in data that is at least *pseudonymized*."[349] If the data is only pseudonymized, controllers of the data will be required to implement appropriate technical and organizational measures to ensure that processing is performed in accordance with the GDPR.[350] They can still benefit, however, from several relaxed standards under the

---

[341] *Id.*

[342] *See* GDPR Recital 26.

[343] Bradford et al., *supra* note 7, at 7 (referencing Zach Whitaker & Darrell Etherington, *Q&A: Apple and Google Discuss Their Coronavirus Tracing Efforts*, TECHCRUNCH (Apr. 13, 2020), https://techcrunch.com/2020/04/13/apple-google-coronavirus-tracing).

[344] *Id.*

[345] GDPR Recital 26.

[346] Bradford et al., *supra* note 7, at 7.

[347] *Id.*

[348] *Id.*

[349] *Id.*

[350] GDPR art. 5(1)(b) (expanding on Principles relating to processing of personal data); Hadar Y. Jabotinsky and Michal Lavi, *Speak Out: Verifying and Unmasking Cryptocurrency User Identity*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 518, 589 (2022).

GDPR[351] but will bear costs in complying with the GDPR standards as controllers of the information.

In summary, privacy by design makes the need to choose between health and privacy redundant. In the context of contact tracing apps, adhering to high standards of privacy allows app operators to avoid violations of privacy and data protection laws and promotion of the surveillance state.

2. Privacy by Design: From Individuals to Network-Tracking Diffusion of COVID-19

Mapping, identifying, and predicting areas of outbreak on the network, as well as visualizing the pattern of the spread of COVID-19, might allow for more accurate control measures.[352] As charts and graphs are open to everyone's analysis, everybody is able to measure, calculate, model, and interpret them. Such modeling might develop research on the spread of the virus, identifying trends and preparing adequate reaction. The information collected on individuals is used for understanding the diffusion of the virus in general.

Much like contact tracing apps, however, mapping, identifying, and predicting areas of outbreak should not be at the price of privacy and should not promote a surveillance state. Researchers can map the diffusion of the virus without using identifying information. A privacy-by-design approach might allow governments to take efficient steps to prevent damages to public health and preserve privacy. Anonymizing private information of specific infected people by virtue of de-identification could achieve the goals of both governments and citizens in regards to public health and privacy.[353] Indeed, there is always a risk of re-identification and abuse of information by governments and third parties, despite efforts to prevent it. Yet even though the risk still exists, efficient anonymization increases the price of re-identification and reduces the risk for it.[354] Engineers and

---

[351] GDPR art. 6(4)(e) (referring to processing for other compatible purposes that can be allowed for pseudonymized data.). Bradford et al., *supra* note 7, at 7. ("By implementing pseudonymization as a security of processing measure, data controllers can benefit from several relaxed standards under GDPR, including potentially processing for other compatible purposes pursuant to Art. 6(4)(e) GDPR.").

[352] *See supra* Part III.C.

[353] Bradford et al., *supra* note 7, at 6.

[354] *See* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 733, 737 (2016) (arguing that anonymization should focus on the process of minimizing risk of reidentification and sensitive attribute disclosure, not preventing harm).

designers can mitigate the risk of de-identification, and in some jurisdictions they are even obligated to take steps to prevent de-identification.[355] As I explained, full anonymity can allow scientists who research the diffusion of the virus to be absolved from other legal obligations of data protection laws.[356]

It should be noted that if the data is only pseudorandomized, scientists would be subjected to the GDPR but can still benefit from several relaxed standards in processing under it.[357] Scientific research on COVID-19 aims to benefit society by expanding knowledge on the spread of the virus. Thus, processing of such information can be lawful under Article 6 of the GDPR.[358]

B. *Consent, Fiduciary, and Loyalty Duties*

Contact tracing surveillance via smartphones should be voluntary. States must avoid treating all individuals as suspects and avoid conducting mass surveillance without citizens consenting to it. "Consent is a fundamental concept in healthcare ethics."[359] It is part of an individual's right to self-determination. "It transforms the moral landscape between people and makes the otherwise impossible possible,"[360] and it allows for solidarity with the community.[361] Consent should be informed and based on information in a "clear and

---

[355] *See, e.g.*, California Consumer Privacy Act (CCPA), CAL. CIV. CODE §§ 1798.140(h)(1)–(4) (2022); KAHN, *supra* note 8, at 82.

[356] *See supra* notes 340–342 and accompanying text (discussing personal data and "an identified or identifiable natural person").

[357] Bradford et al., *supra* note 7, at 7.

[358] Article 6 refers to the lawfulness of processing. Article 6(1)(e) can fit well with scientific research, as it states, "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." GDPR art. 6(1)(e). For further information on the lawfulness of processing and scientific research see Regina Becker et al., *COVID-19 Research: Navigating the European General Data Protection Regulation*, 22 J. MED. INTERNET RSCH. 1, 3 (2020) ("As scientific research on COVID-19 aims to benefit society as a whole, using the legal basis of a task performed in the public interest appears to be a natural choice. It is also the choice suggested by the EDPB as more appropriate than consent for research in clinical trials and is one of the potential legal grounds mentioned in the EDPB's guidelines on COVID-19 and research. The availability of the public interest legal basis, however, must be established by Union or Member State law (Article 6). Infectious disease or public health laws may provide the necessary legal basis as a task in the public interest.").

[359] *See* JACQUES TAMIN, OCCUPATIONAL HEALTH ETHICS 25 (2020).

[360] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1462 (2019).

[361] TAMIN, *supra* note 359, at 28.

understandable [language]. Only then can this part of the consenting process be truly *informed* consent."[362]

Without informed consent to contact tracing via smartphones, there will be suspicions instead of solidarity. Compulsory measures, such as the Shin Bet surveillance in Israel,[363] crowd out intrinsic motivation to cooperate with such measures. Thus, because surveillance measures were compulsory, many individuals likely left their smartphones at home.[364] Consent is important to promote solidarity and trust and prevent infringement of civil rights. Individuals might consent to surveillance in order to protect their community from possible infection because of social solidarity. An obligation of receiving consent will also allow app providers and authorities to keep up with the GDPR requirement of lawful processing.[365]

Indeed, in the digital age, practical conditions of informed consent fall very short of the gold standard of knowing and voluntary consent.[366] Indeed, individuals' ability to assess the risks of using the app might be limited.[367] Regarding infrequent requests for consent, however, reaching informed consent might be possible. It could be easier to imagine harm resulting from consent; noting correct incentives to choose consciously and seriously, individuals can reach informed consent.[368] The risks of consenting to use the app are clearer to the user—his decision to consent to the terms of use can be informed if the consent is limited to contact tracing and the information is stored only on his smartphone. Consent to a surveillance app is infrequent and might reduce overload to our mind's capacity to make rational choices because individuals usually upload the app only once.[369] If the app is built on privacy-by-design

---

[362] *Id.* at 30.

[363] *See* Bob, *supra* note 220.

[364] *See* Tamar Uriel Beeri, *Doctor: 'Leave Phone at Home, avoid quarantine' - Health Ministry outraged*, JERUSALEM POST (July 13,2020) https://www.jpost.com/health-science/doctor-leave-phone-at-home-avoid-quarantine-health-ministry-outraged-634810.

[365] For the definition of consent, see GDPR art. 4(11). For consent as one of the bases of lawful processing, see GDPR art. 6(1)(a).

[366] Richards & Hartzog, *supra* note 360, 1462–63.

[367] Citron & Solove, *supra* note 195, at 852 (explaining that individuals lack the ability to assess the risks of future harm from the collection, use, and disclosure of their data).

[368] *See id.* at 1492–98.

[369] *Id.* at 1492–94 (explaining that infrequent consent is more likely to be informed).

and data minimalization, the harm of consenting to surveillance can be more easily imagined because the information is stored only on the smartphones of the data subjects and there are less long-term implications beyond quarantine orders.

Indeed, consent "cannot do everything well all the time."[370] An individual's consent to the collection of their information is not always informed, and they cannot always predict long-term risks.[371] This is especially true if app providers fail to adhere to privacy-by-design standards, keep the information on their cloud and transfer it to third parties, and misuse their data in addition to requirements of consent.

Recently, scholars have proposed a concept of *information fiduciaries*, inter alia, because of the problems with consent.[372] This approach likens intermediaries' obligations toward user information to that of doctors and lawyers' fiduciary duties to their patients and clients.[373] Accordingly, much like doctors and lawyers' duties of care, confidentiality, and loyalty, the law should impose special duties on intermediaries—such as Facebook, Google, and Twitter—in relation to their users. Such duties would be "sensitive to the power disparities within information relationships"[374] and solve the problem of gaining informed consent in the digital age.[375] Because such duties focus on relations, they open the possibility of more robust enforcement rules[376] that consider the motives of data collectors.[377] Imposing duties of care,

---

[370] *Id.* at 1503.

[371] *See* Hadar Y. Jabotinsky & Michal Lavi, *The Eye in the Sky Delivers (and Influences) What You Buy*, 24 U. PA. J. CONST. L. (forthcoming, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3849218.

[372] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186–87 (2016); Jack M. Balkin, *Fixing Social Media's Grand Bargain*, *in* AEGIS PAPER SERIES 2018 11 (Hoover Inst., Aegis Series Paper No. 1814, 2018); Richards & Hartzog, *A Duty of Loyalty for Privacy Law*, *supra* note 312, 964–65, 988–89; *see generally* Neil Richards & Woodrow Hartzog, *Legislating Data Loyalty*, 97 NOTRE DAME L REV. REFLECTION 356 (2022).

[373] *See* Balkin, *Fixing Social Media's Grand Bargain*, *supra* note 372, at 12.

[374] Richards & Hartzog, *Legislating Data Loyalty*, *supra* note 372, at 360.

[375] *Id.* at 361 (such duties "allow trusting parties to enter into information relationships without accepting the risks of whatever harmful data practices and consequences lurk in the fine print, the business model, or the technology").

[376] *Id.*

[377] *Id.* at 366 ("Data loyalty would compel an examination of a company's motives and the potential adverse consequences to consumers in determining if more data than necessary was collected or if the use of data deviated too far from its original purpose.").

fiduciary, and loyalty on app providers will protect users from manipulative practices and misuses of their data.[378]

Just as the law imposes special duties of care, confidentiality, and loyalty on doctors and lawyers with regards to their patients and clients, it should impose special duties on app providers that collect information towards their users to act in the best interests of their digital users and constrain conflicted, self-dealing behavior by companies.[379] App providers resemble fiduciaries because, much like lawyers and doctors, they receive personal information and are trusted to treat it with care.[380] Thus, app providers should neither breach user trust nor take actions that users would reasonably consider unexpected or abusive. Companies should be obligated to be trustworthy regardless of whether an individual clicked to "agree" to the app's terms of service.[381] Such policy is currently missing under the existing U.S. privacy framework. Thus, implementing it would allow for addressing a broader scope of emergent dangers, including a betrayal of data collectors.[382]

Loyalty duties could be implemented on two levels that would allow for integrating them into practice and enforcing them: First, a general prohibition on substantial conflicts with the trusting party's best interests. Second, specific duties targeting particular actions,[383] such as minimization of collection and retention of data, loyal

---

[378] *Id.* at 363 ("The scope of protection that loyalty rules safeguard includes, but is broader than, recognized privacy harms like identity theft, emotional harms, breaches of confidence, and dangerous exposure. It also includes more subtle individual and collective costs to our identity, our ability to create relationships, our collectively held truths, and the obscurity that protects our ability to share and move about freely.").

[379] *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 15 (2020); Richards & Hartzog, *A Duty of Loyalty for Privacy Law*, *supra* note 312, at 966–67 ("[A] duty of loyalty framed in terms of the best interests of digital consumers . . . should become a basic element of U.S. data privacy law. Such a duty of loyalty would compel loyal acts and also constrain conflicted, self-dealing behavior by companies. It would shift the default legal presumptions surrounding a number of common design and data processing practices. It would also act as an interpretive guide for government actors and data collectors to resolve ambiguities inherent in other privacy rules.").

[380] In a related context of imposing information fiduciary duty on intermediaries that profit from their users and beneficiaries, see Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66 BUFF. L. REV. 979, 1006–09 (2018); Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 372, at 1229; Balkin, *The Fiduciary Model of Privacy*, *supra* note 372, at 14–15, 17 (expanding the fiduciary duties to data brokers).

[381] *See* Richards & Hartzog, *The Pathologies of Digital Consent*, *supra* note 360, at 1503.

[382] Richards& Hartzog, *Legislating Data Loyalty*, *supra* note 372, at 364, 369.

[383] *Id.* at 371.

personalization of data-loyal gatekeeping of third-party access to the information,[384] and restrictions on "malicious interfaces" which are "meant to influence a person's behavior against their intentions or best interests."[385] Such duties could provide clear rules to ensure accountability. Imposing such duties on app providers is one step further towards having individual privacy, civil rights, and health.

C. *Safeguards: Transparency, Oversight, and Due Process*

Even in circumstances when there might be a need for quarantine orders, such orders that are based on digital infrastructure should be subject to safeguards. Transparent governance, oversight, and due process obligations should be fostered to strengthen the protection of civil rights and liberties.[386]

1. Transparency

Transparency protects a balance of power between governments and the public.[387] The public has to know what personal data is collected on them, even in times of crises. They should know how this data is used and shared, how governments will ensure that it will not be misused for other purposes beyond combating the virus, and how long their data will be retained.[388] Transparency and disclosure regarding the nature and scope of surveillance practices and processing of personal identifying information is only the first step in preserving civil rights. Transparency obligations towards governments that use algorithmic decisions should extend to the level of code and algorithm of automated systems to allow efficient oversight, impact assessment, and evaluation of automated decisions. Apps should be based on open-source software, and users should be informed about the ways in which their personal data is collected, processed, and stored.[389]

---

[384] *Id.* at 380.

[385] *Id.* at 382.

[386] KAHN, *supra* note 8, at 3.

[387] *See* Bloch-Wehba, *supra* note 79, at 923–24.

[388] KAHN, *supra* note 8, at 72.

[389] *See* Press Release, Joint Civil Society, Joint Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights (Apr. 2, 2020), https://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf; Maria Pia Sacco et al., *Digital Contact Tracing for the Covid-19 Epidemic: A Business and Human Rights Perspective*, INT'L BAR ASS'N 2, 15–16 (2020), papers.ssrn.com/sol3/papers.cfm?abstract_id=3618958.

2. Oversight

An open-source approach allows programmers, experts outside the app, system development teams, and civil society organizations to review the code. Allowing such oversight can improve the code and foster trust in contact tracing apps because an open-source approach enhances trustworthiness.[390] Due to the availability of the code for public review, experts around the world can confirm it works the way the development team said it would.[391]

A second oversight safeguard is data protection impact assessment (DPIA) for processing information that is likely to result in a high risk to individuals. DPIA evaluates the risk of data processing in the context that it is processed, including its suitability, necessity, and appropriateness to succeed in fighting the virus. Processing of information must be carried out in a transparent, comprehensible way to the data subject.[392] Entities that process private information should take into account the nature, scope, circumstances, and purposes of the processing and the risks to individuals' rights and freedoms. They should adopt appropriate technical and organizational measures to ensure and provide proof that the processing is in compliance with data protection laws.[393] The DPIA's requirement is already anchored in the GDPR.[394]

The practice of impact assessment is not revolutionary; it is starting to gain weight in legislation in other contexts like algorithmic impact assessment against discrimination and promoting

---

[390] *See* COVID-19 CONTACT-TRACING MOBILE APPS: EVALUATION AND ASSESSMENT FOR DECISION MAKERS, COVID SAFE PATHS 11 (2020), https://arxiv.org/ftp/arxiv/papers/2006/2006.05812.pdf.

[391] *See id.*; KIRSTEN BOCK ET AL., DATA PROTECTION IMPACT ASSESSMENT FOR THE CORONA APP 8 (2020) ("Open source development of the server and app software including all components—for example, in the form of free software—is an essential prerequisite for transparency regarding the implementation of data protection principles.").

[392] BOCK ET AL., *supra* note 391, at 60.

[393] *Id.*

[394] Council Regulation 2016/679, art. 35, 2016 O.J. (L 119) 1 (EU) ("Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."); *see also Article 29 Data Protection Working Party* 8–13 (Eur. Comm'n, Working Paper No. 248 rev. 01, 2017).

accountability.[395] Such a practice extends beyond the design stage and requires technology companies to ensure that their algorithms and tools regularly undergo safety evaluations by independent auditors and technology experts. Giving engineers an opportunity to correct failures might mitigate the risk of failure in the design stage or prevent unexpected reactions of learning algorithms.[396] Evaluation tools and practices of transparency and oversight should be adopted more broadly, as such tools allow for the discovery of legal violations by entities that collect information and infringe on civil rights.

3. Due Process for Quarantine Orders

During the outbreak of the virus, in many countries a person could be ordered to quarantine, despite being alone at the time of the claimed exposure to the infected person.[397] Individuals that are ordered to quarantine are not criminals, they are just ordinary people that were more likely to acquire the virus and maybe infect others. By contrast, however, to criminal procedures that are subjected to procedural justice and fair trial principles, surveillance technologies rendered opaque quarantine orders. Citizens lacked an explanation for decisions made by technologies such as apps, software, and algorithms. Individuals that received quarantine orders had no

---

[395] Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019). For further analysis and criticism, see Margot E. Kaminski & Andrew D. Selbst, *The Legislation That Targets the Racist Impacts of Tech*, N.Y. TIMES (May 7, 2019), https://www.nytimes.com/2019/05/07/opinion/tech-racism-algorithms.html?smid=nytcore-ios-share. For further information on algorithmic impact assessment, see Neil Richards & Woodrow Hartzog, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1769 (2020) (referring to algorithmic impact assessment for "high-risk automated decision systems"); Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 75 VAND. L. REV. 1563, 1602–04 (2019); Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 126 (2019); Frank Pasquale, *The Second Wave of Algorithmic Accountability,* L. & POL. ECON. PROJECT (Nov. 25, 2019), bit.ly/2LArsD0.

[396] *See* Michal Lavi, *Do Platforms Kill?*, 43 HARV. J.L. PUB. POL'Y 477, 566 (2020) (giving an example of a recent bill of impact assessment against algorithmic discrimination. The proposed bill, the Algorithmic Accountability Act of 2019, "requires entities that use, store, or share personal information to conduct impact assessments for automated decision systems and data protection. These impact assessments are meant to monitor for discrimination and give entities a chance to correct discriminatory algorithms in a timely manner."); H.R. 2231.

[397] *See* Bob, *supra* note 220.

efficient way to appeal,[398] and they were deprived of procedural justice and due process rights that even suspects in crimes are entitled to under the law.[399]

In countries such as Israel, where the government ordered individuals to quarantine based on the conclusion of technological contact tracing apps, citizens should have been able to contest the system. Due process facilitates accountability and allows individuals the opportunity to challenge and contest the decisions that are delegated to technology. As Professor Citron proposed, there should be "technological due process."[400] Procedures designed to ensure that decisions that are delegated to technology and automation satisfy some standard of review and revision to confirm their fairness and accuracy. As explained above, transparency that extends to apps, software, and algorithms allows for more oversight.[401] Transparency and oversight could have made it possible to challenge decisions of quarantine orders based on contact tracing apps.

---

[398] *See, e.g.*, *id.* (stating Israel's "Health Ministry has not merely been inadequately staffed to field all of the calls from citizens to verify or dispute the text they received" that order them to be isolated).

[399] In Israel, suspects in crimes are entitled to rights of due process and a fair trial that are protected under the Israeli Human Dignity and Liberty Basic Law. Section 5 to this Basic Law states that "[t]here shall be no deprivation or restriction of the liberty of a person by imprisonment, arrest, extradition or otherwise." Basic Law: Human Dignity and Liberty § 5 (1992) 5752 (Isr.). Section 8 of the law states that "[t]here shall be no violation of rights under this Basic Law except by a Law befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required, or by regulation enacted by virtue of express authorization in such Law." *Id.* § 8. In addition, such rights are guarded in in the Criminal Procedures Act, the Law of Evidence, and the Penal Law. *See* Avigdor Feldman, *The Right to a Fair Trial In Israel*, http://hrlibrary.umn.edu/fairtrial/wrft-fel.htm (last visited Nov. 1, 2022). Moreover, there are plans to codify these basic rights explicitly in a specific Basic Law. *See* Chen Maanit & Netael Bandel, *Israel's Justice Minister Plans Bill Enshrining Suspects' Rights in Basic Law,* HAARETZ (Jul 13, 2021), https://www.haaretz.com/israel-news/2021-07-13/ty-article/.premium/israels-justice-minister-plans-bill-enshrining-suspects-rights-in-basic-law/0000017f-db84-d856-a37f-ffc456980000 ("The law is expected to include protection of the right of people to approach the courts; the presumption of innocence until proven guilty in a final judgment; the rights of detainees; and the principle that punishment cannot be imposed without warning that someone is committing an offense. It is also expected to include the right to a fair trial and the state's duty to respect the rights under the Basic Law.").

[400] Danielle Keats Citron, *Technological Due Process,* 85 WASH. U. L. REV. 1249, 1249–50 (2008); s*ee also* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 121 (2014).

[401] *See supra* Part V.C.1.

The idea of a right to contest processing of personal information is not revolutionary; scholars recently proposed the idea in the context of AI,[402] and one can find first signs of it in the EU GDPR. Article 22 of the GDPR addresses automated decision-making and stipulates that individuals "have the right not to be subject to a decision based solely on automated processing."[403] Article 22(3), which addresses safeguards against automated decision-making, directs that: "the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[404]

Transparency and oversight of technology are not enough. Individuals should have had a right to appeal and contest the quarantine that denied their freedom without due process based on an automated decision. "The right of appeal . . . is a fundamental element of procedural fairness as generally understood in [the United States],"[405] as well as in other countries.[406] Similar to appeal rights in courts, individuals should have appeal rights when they are subjected to decisions of automated systems.[407] As there were a lot of false positive quarantine orders that coerced people to stay at home,[408] individuals should have at least been able to present an alibi proving

---

[402] Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI,* 121 COLUM. L. REV. 1957, 1957 (2021).

[403] Council Regulation 2016/679, art. 22, 2016 O.J. (L 119) 1, 46 (EU). This prohibition applies only when the decision is "based solely" on algorithmic decision-making without a human in the loop. Once the process is not "solely" automated, this provision will not apply. *See* Meg Leta Jones, *Right to a Human in the Loop: Political Constructions of Computer Automation & Personhood from Data Banks to Algorithms*, 47 SOC. STUD. SCI. 216, 217 (2017); Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data,* 47 SETON HALL L. REV. 995, 1015–16 (2017); Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 190–91 (2019).

[404] GDPR art. 22(3).

[405] Harlon Leigh Dalton, *Taking the Right to Appeal (More or Less) Seriously*, 95 YALE L.J. 62, 66 (1985) (quoting ABA COMM. ON STANDARDS OF JUDICIAL ADMINISTRATION: STANDARDS RELATING TO APPELLATE COURTS § 3.10 commentary, at 12 (1977)).

[406] On fair trial in Israel, see *supra* note 399.

[407] In a related context, see Margot E. Kaminski & Jennifer M. Urban, *The Right to Consent AI*, 121 COLUM. L. REV. 1957, 1979 (2021) (referring to Article 22 of the GDPR which focuses on automated individual decisions, "[t]he GDPR's new wording compared to the Directive's 'points at . . . at least, an obligation to hear the merits of the appeal and to provide a justification for the decision.' This right 'obliges the data controller either to render automated decisions contestable or to cease [automated decision-making] at all.'").

[408] *See* Greenbaum, *supra* note 225.

their presence at home at the time of the claimed exposure. For instance, a government could allow people to present an affidavit from someone that had been at home with them. Alternatively, individuals could contest the conclusion of the contact tracing app through technological means, such as recordings from personal digital assistants that can contest the conclusion of the contact tracing app,[409] or CCTV outside their homes. Effective due process and the right to contest and appeal is likely to mitigate violations of human rights and civil liberties.

D. *Categories of States' Data-driven Surveillance that Should Be Forbidden: The Case of Risk Score*

The previous subsections explain that when COVID-19's risks were largely unknown, some steps may have been necessary to combat it. But the way of implementing them could have made a difference.

Governments should have avoided certain steps at all costs, such as utilizing either the notorious cyber intelligence company NSO's risk score system for handling information about the probability of infection depending on an individuals' network,[410] or the Chinese system of AI risk score.[411] Such systems moralize and normalize the social classification of people, causing injustice and inequality.[412] These systems involve constant surveillance of individuals and their network's movements, calculating many dimensions and contexts of everyday lives. Individuals cannot knowingly consent to such constant, frequent, and invasive surveillance.[413] Governments implementing such systems would normalize constant surveillance and promote the rise of the surveillance state.

A system of risk scoring, which depends on many parameters processed and scored algorithmically in the black box,[414] is less likely

---

[409] Amazon Alexa is an example of a personal digital assistant. *See* CLEMENS KRUEGER & SEAN MCKEOWN, IEEE INT'L CONF. ON CYBER INCIDENT RESPONSE, COORDINATION, CONTAINMENT & CONTROL, USING AMAZON ALEXA APIS AS A SOURCE OF DIGITAL EVIDENCE (2020), https://arxiv.org/ftp/arxiv/papers/2006/2006.08749.pdf.

[410] Ackerman & Benmeleh, *supra* note 163.

[411] *See* Huang et al., *supra* note 167 and accompanying text.

[412] KATE CRAWFORD, ATLAS OF AI 205–06 (2021) (criticizing the use of systems that were designed to combat terrorism for social credit scoring based on correlations, not on inherent precision).

[413] *See* Richards & Hartzog, *The Pathologies of Digital Consent*, *supra* note 360, at 1464 (expanding on the inefficiency of consent in cases of frequent surveillance and invasions of privacy).

[414] *See generally* PASQUALE: THE BLACK BOX, *supra* note 183.

to achieve sufficient transparency. Moreover, the system designers might avoid being transparent with the algorithm, out of concern for trade secrets.[415] Therefore, there are legal difficulties in imposing general transparency obligations that allow for public oversight.[416] In addition, system designers are likely to be disincentivized from revealing the parameters beyond the scoring systems. This is because declining to reveal the parameters beyond the system will reduce individuals' ability to artificially change their behavior, or alternatively, game the algorithm in other ways to prevent an increase in their risk scores.[417] Further, even with transparency regarding the parameters at the base of the algorithm, and an impact assessment being conducted, it would be difficult to achieve efficient public oversight and mitigate the biases of the system, as it depends on AI and learning algorithms.[418] Because AI systems learn to recognize patterns and similarities, their capabilities grow in evolving and continuing processes as they absorb more data.[419] Furthermore, oversight might not be entirely feasible when learning algorithms are involved in creating and updating risk

---

[415] *See* Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 481 (2020); Finale Doshi-Velez & Mason Kortz, *Accountability of AI Under the Law: The Role of Explanation* 2 (Berkman Klein Ctr. for Internet & Soc'y, Working Paper, 2017), https://dash.harvard.edu /handle/1/34372584 (explaining that "there exist concerns that the engineering challenges surrounding explanation from AI systems would stifle innovation; that explanations might force trade secrets to be revealed").

[416] *See* Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1540 (2013); Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1308 (2020) ("Faced with demands for more transparency, courts and litigants have sometimes reached an apparent compromise: protective orders, coupled with nondisclosure orders, that permit disclosure to the parties while preventing disclosure to the general public.").

[417] *See* Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1, 4–5 (2018) ("The algorithm game also has important yet unintuitive distributional consequences. Some populations will be less willing or able to engage in gaming, and therefore both gaming and countermoves can have disparate effects on different subgroups.").

[418] AI systems can produce biased outcomes that can inflict harm to minorities. For example, Amazon's AI facial recognition software wrongly identified twenty-eight members of Congress as individuals who had jail mugshots. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28.

[419] *See* Maayan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 FLA. L. REV. 181, 189–90 (2017).

scores because the systems are capable of "learning" and changing.[420] Finally, such automated agents lack legitimacy, thereby throwing away the expertise that justifies the administrative state.[421] Lack of significant oversight over automated decisions denies individuals their constitutional right to due process[422] and their right to appeal[423] decisions that have substantial effects on their civil rights.

Beyond infringing on privacy itself, social risk scores can exclude individuals with a high-risk score from society and deny them benefits. Social risk scores can also lead to their stigmatization because other people in these individuals' networks would want to avoid adverse effects on their scores. A scoring system that combats the virus can also creep and lead to the creation of other unrelated scores.[424] For instance, an obesity score used as a proxy for health could lead to other forms of discrimination that might relate directly to protected categories.

Continuing mass surveillance for creating a risk score, which can change with an individual's each and every action, normalizes surveillance.[425] Moreover, constant surveillance violates intellectual privacy.[426] "When the same powerful capacities are ranking and rating everyone all the time, they become oppressive."[427] These powerful capacities can also chill free speech.[428] As a result of constant surveillance, individuals will chill themselves, avoid asking questions, doubt facts, and refrain from looking for innovative answers to problems. Individuals might avoid experimenting with ideas, and thus constant surveillance hampers their freedom of expression.

---

[420] ADAM THIERER, ANDREA CASTILLO O'SULLIVAN & RAYMOND RUSSELL, ARTIFICIAL INTELLIGENCE AND PUBLIC POLICY, 19–20 (2017).

[421] *See* Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797 (2021) (explaining that reliance on automation and technology raise problems for the constitutional right of due process and due process problems of legitimacy for agencies that automate, thereby throwing away the expertise that justifies the administrative state).

[422] Citron & Pasquale, *The Scored Society*, *supra* note 230.

[423] On this right, see *supra* Part V.C.

[424] On censorship creep, see Tokson & Waldman, *supra* note 23.

[425] *See* Harari, *The World After Coronavirus*, *supra* note 6.

[426] On intellectual privacy and its connection to freedom of expression, see RICHARDS, INTELLECTUAL PRIVACY, *supra* note 189.

[427] *See* FRANK PASQUALE, NEW LAWS OF ROBOTICS: DEFENDING HUMAN EXPERTISE IN THE AGE OF AI 11 (2020).

[428] *See supra* Part IV.B.1.ii.

The deciding factors in avoiding risk scores altogether are the erosion of basic freedoms[429] and democracy, as well as the rise of the surveillance state.[430] Governments can misuse risk scores, which it assigns to each and every citizen to combat the virus, for other purposes unrelated to the public's health. The risk score system in itself creates an infrastructure for collecting information on citizens. Governments can use risk scores to gain control over citizens by punishing behavior that does not fit with the standards the government sets,[431] entrench governance, and eliminate democracy due to the opacity of the risk score system, lack of oversight, and lack of due process. For example, governments will have information on individuals that oppose the regime.[432] Governments can use the information to oppress protest and opposition to the regime[433] and justify this oppression on protest and free speech by assigning a high-risk score that does not allow protesters to demonstrate.[434] Constant surveillance allows governments to move beyond transparent limitations on opposition. Such information allows governments to know who opposes them, thus enabling governments to disrupt the communication and voices of such activists without providing any justification. For example, governments—using bots to enhance their

---

[429] Stacy Rudin, *Will You Choose Freedom?*, AIER (Sept. 1, 2020), https://www.aier.org/article/will-you-choose-freedom (describing freedom as giving up grasping control).

[430] In a related context of the Chinese system, see Lauren Yu-Hsin Lin & Curtis J. Milhaupt, *China's Corporate Social Credit System and the Dawn of Surveillance State Capitalism*, (Stanford Law School, Working Paper No. 560, 2021), https://ssrn.com/abstract=3933134 ("Chinese state capitalism is transitioning toward a panoptic, technology-assisted variant that we call 'surveillance state capitalism.' The mechanism driving the emergence of this variant is China's corporate social credit system (CSCS)––a big data project to evaluate the 'trustworthiness' of all business entities registered in the country.").

[431] For an example of the use of the social scoring system in China, see Lydia Barrios, Origins and Perceptions of the Chinese Social Credit System 5 (2020) (Honors Thesis, Duke University), https://sites.duke.edu/honorsthesis2020/files/2020/04/Final-FINAL-Draft-Lydia-Barrios.pdf ("Under the national SCS, the Chinese government will be scrutinizing citizens and closely monitoring their behaviors to calculate a social score. This score will be used as part of a rewards and punishments scheme that aims to control citizens' behavior to fit the standards set by the CCP.").

[432] *See, e.g.*, RICHARDS, *supra* note 30, at 145–153 (expanding on the ability of the NSA to collect information on citizens and gain power by using the information to blackmail or persuade citizens).

[433] *See Reports: Chinese Authorities Using COVID-Tracking App to Thwart Protesters*, CHINA NEWS (June 15, 2022), https://www.voanews.com/a/reports-chinese-authorities-using-covid-tracking-app-to-thwart-protesters-/6619689.html.

[434] *See* Friedman, *supra* note 33, at 15.

attacks—can disrupt protestors' internet infrastructure, thus preventing them from organizing. Governments can also post disinformation and conduct organized disruptions to opposition activity. Such algorithmic software programs, which operate according to instructions, can interact socially with users and manipulate the audience into distrusting activists that oppose the regime.[435] Moreover, such mass attacks can include "doxing," meaning it can include publishing personal details of individuals online, such as home address, work details, phone number, details on their parents, children, and more, thereby even creating a potential for physical violence against opponents to the government.[436] Mass attacks can silence protestors and chill their speech, thereby preventing criticism of government officials.[437]

Governments can use the infrastructure of the risk scoring system to gain control over citizens in non-transparent ways. The system can use the vast information it gathers to manipulate citizens towards the government's desired purposes. The government, having knowledge on individuals, holds the power to influence their behavior and lead them to act in certain ways. Modern technology in smart devices—coupled with the computational power used to decode "big data" and the ability to direct messages and advertisements back to a specific individual—can manipulate individuals' behavior.[438] Technologies

---

[435] Emilio Ferrara et al., *The Rise of Social Bots,* 59 COMMC'NS ACM 96, 96 (2016) (defining a social bot as "a computer algorithm that automatically produces content and interacts with humans on social media, trying to emulate and possibly alter their behavior"); WALDMAN, *supra* note 176, at 141 (expanding on the social communication of bots that motivate people to waive privacy protections, as a result of technological design); JARON LANIRE, TEN ARGUMENTS FOR DELETING YOUR SOCIAL MEDIA ACCOUNTS RIGHT NOW 55 (2018) ("If your extended peer group contains a lot of fake people calculated to manipulate you, you are likely to be influenced without even realizing it.").

[436] *See generally* Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARV. NAT'L SEC. J. 146, 149 (2018) (on doxing generally).

[437] *See generally* Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 U. CHI. LEGAL F. 45, 55 (2020) (explaining that attacks online can silence individuals).

[438] *See* YUVAL NOAH HARARI, 21 LESSONS FOR THE 21ST CENTURY 267–68 (2018) ("You might have heard that we are living in the era of hacking computers, but that's hardly half the truth. In fact, we live in the era of hacking humans. The algorithms are watching you right now. They are watching where you go, what you buy, who you meet. Soon they will monitor all your steps. All your breaths, all your heartbeats. They are relying on Big Data and machine learning to get to know you better and once these

can also process patterns of individual behavior. An analysis of the "Likes" that individuals hit on Facebook (Meta), which was conducted to evaluate risk scores, provides the government with an accurate evaluation on a wide range of personality traits, emotional states,[439] or psychographic traits,[440] even if individuals never meant to share that information with anyone.[441] Cambridge-Analytica's model for predicting behavior of voters and targeting political messages[442] is one prominent example of how data on voters can be used to manipulate votes and erode democracy. The more data a government collects, the more powerful its ability to manipulate citizens to advocate for a certain government policy, or vote for a specific political candidate, thereby entrenching the regime.

As explained above, a privacy-by-design approach, transparency, impact assessment, and due process could mitigate part of the concern regarding violations of civil rights in the struggle to combat the spread of the virus. But such measures are not likely to mitigate the prospective damage of risk scores; as such, surveillance is constant and includes every aspect of life. Using constant surveillance in the practice of risk scores for combating viruses that involves constant surveillance is unacceptable—it should be ruled out altogether and prevented at all costs. Otherwise, the United States, and any country that chooses to adopt risk scores, will become like the surveillance state and the Orwellian dystopia described in the novel *1984*.[443]

---

algorithms know you better than you know yourself, they could control and manipulate you and you won't be able to do much about it.").

[439] *See* Michal Kosinski et al., *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 PNAS 5802, 5805 (Apr. 9, 2013), https://www.pnas.org/doi/full/10.1073/pnas.1218772110; Wu Youyou et al., *Computer-Based Personality Judgments are More Accurate Than Those Made by Humans*, 112 PNAS 1036 (Jan. 27, 2015), https://www.pnas.org/doi/full/10.1073/pnas.1418680112.

[440] *See* Hannes Grassegger & Mikael Krogerus, *The Data That Turned the World Upside Down*, MOTHERBOARD (Jan. 28, 2017), https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win; *see also* Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 514 (2018).

[441] *See* Gregory Park et al., *Automatic Personality Assessment Through Social Media Language*, 108 J. PERSONALITY & SOC. PSYCH., 934, 934 (2015).

[442] *See* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[443] *See generally* ORWELL, *supra* note 282.

VI. CONCLUSION

"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." [444]

Given the uncertainty regarding the scope of risk and consequences of COVID-19, at the beginning of the outbreak of the virus, governments and private companies developed data-driven mass surveillance practices to combat the spread. Governments and private companies used such tools to track contacts with infected people and warn of exposure, enforce quarantine orders, identify and predict areas of urban outbreak to conduct social network analyses, and even to assign risk scores to citizens.

Much like the KGB, digital mass surveillance tracks individuals. But, with technological surveillance, there is no need for human agents: "Governments can rely on ubiquitous sensors and powerful algorithms,"[445] thereby infringing on civil rights and liberties without sufficient safeguards, eroding democracy, creeping beyond the health context, and leading to the surveillance state.

This Article first overviewed types of practices that were used during the COVID-19 outbreak. Next, it warned of the flip side of using such mass surveillance practices, including their infringement on human rights and civil liberties, the erosion of democracy in itself, and the creep of such practices into other contexts. The Article argued that the public should not allow infringements of their rights and the erosion of democracy, even in times of crisis. The public should not have to choose between civil rights and health; rather, the public should have both. Adopting the privacy-by-design approach and safeguards would have benefitted the public. Finally, this Article referred to the types of surveillance that should be ruled out at all costs.

This Article focused on a test case of surveillance. This example is, however, only one of many ways in which governments use crises to infringe on human rights and civil liberties. When COVID-19 started to spread, there might have been uncertainty regarding the scope of the virus's danger. Governments compromised civil rights and liberties for the sake of public health by instituting mass surveillance, quarantine orders, and even planning to apply risk scoring.

---

[444] Letter from Benjamin Franklin, to Robert Hunter Morris, Governor of Pennsylvania (Nov. 11, 1755), https://founders.archives.gov/documents/Franklin/01-06-02-0107#:~:text=Those%20who%20would%20give%20up,deserve%20neither%20Liberty%20nor%20Safety.

[445] Harari, *The World After Coronavirus*, *supra* note 6.

Many countries even imposed a "Green Passport" system order to encourage citizens to get vaccinated. "Green Passports," beyond causing people to make decisions related to their health for the wrong reasons,[446] had other potential uses: the government could have used them as a *surveillance tool* because the system was installed as a smartphone app or could have used them to create a general "credit score."[447]

The government brutally imposed aggressive steps and mandates on citizens without transparency. The recent leak of Anthony Fauci's emails reveals that in the United States some of the steps taken were inefficient, and the government should have known that from the beginning.[448] This demonstrates that without transparency and

---

[446] Simone M. Matthews, *Israel – Human Tragedy – Part 1*, SIMONE MATTHEWS, https://www.universallifetools.com/2021/03/israel-human-tragedy-is-this-the-global-template (last visited Oct. 11, 2022). I would like to note that I never believed that such limitations, that are beyond soft paternalism and exceed to coercion, would arrive in the United States. I thought that because of the deep commitment to constitutional values and autonomy, the United States would have adopted a policy of "your health is your responsibility," as adopted by some businesses. *See, e.g.*, @bluestarrfl, TWITTER (Dec. 11, 2021, 10:08 PM), https://twitter.com/bluestarrfl/status/1469866707376345097. But surprisingly, the Green Pass was applied in the United States. Stefania Milan et.al., *Promises Made to Be Broken: Performance and Performativity in Digital Vaccine and Immunity Certification,*12 EUR. J. RISK REG. 382, 383 (2021) ("This move mirrors other initiatives around the world to certify, at the very least, receipt of an authorised COVID-19 vaccine. These include Israel, whose 'Green Pass' was deployed in early 2022; Hungary and Iceland; and proposals in the UK *and the USA*.") (emphasis added). Moreover, President Joe Biden announced new mandates on workers in the United States. Twenty-six states filed suits against Biden's vaccine mandate. In response, the Biden Administration repealed federal vaccine mandates, a federal court in Missouri suspended the vaccine mandate for United States health workers, and a federal judge sided with Attorney General Wilson by blocking the Biden Administration's vaccine requirement for federal contractors. *See Federal Judge Sides with S.C., Other States, Blocks Vaccine Mandate for Federal Contract Workers*, WMBF NEWS (Dec. 7, 2021), https://www.wmbfnews.com/2021/12/07/federal-judge-sides-with-sc-other-states-blocks-vaccine-mandate-federal-contract-workers.

[447] Former Prime Minister Bennett talks about the "credit score" tech system that developed in Israel. This system was rolled out in Israel as the "new" vaccine pass system as of October 3, 2021. @efenigson, TWITTER (Sept. 28, 2021, 6:31 AM), https://twitter.com/efenigson/status/1442799033932816384; Elizabeth M. Renieris, *What's Really at Stake with Vaccine Passports*, CIGI (Apr. 5, 2021), https://www.cigionline.org/articles/whats-really-stake-vaccine-passports.

[448] Dr. Anthony Fauci, the Chief Medical Advisor to the President and the Director of the National Institute of Allergy and Infectious Diseases, knew that some mandates were inefficient, but he continued advocating for them. *See* Darragh Roche, *Fauci Said Masks 'Not Really Effective in Keeping Out Virus,' Email Reveals*, NEWSWEEK (June 2, 2021, 4:59 AM), https://www.newsweek.com/fauci-said-masks-not-really-effective-keeping-out-virus-email-reveals-1596703 (reporting that a leak of Fauci's emails shows that some

oversight, and with only partial constitutional protection due to "exigent circumstances," the government's ability to compromise human rights and civil liberties can be arbitrary.

Beyond the direct context of surveillance, living under emergency regulations also led to the general erosion of human rights, civil liberties, and, in particular, freedom of expression. This era legitimized the censorship of people that did not agree with infringement of human rights or civil liberties and enabled certain governmental bodies to block access to knowledge. For example, individuals expressed legitimate criticism on the policy of the Israeli Ministry of Health,[449] a public governmental authority. Despite being a governmental authority, the Ministry of Health blocked people who criticized its policy from accessing its Twitter account, thereby infringing upon the people's constitutional right to free speech,[450] including their right to receive information.[451] Censorship was pervasive in the private sector as well. Platforms relied solely on automated moderation at the beginning of the virus outbreak.[452] As a

---

were "not really effective in keeping out the [sic] virus, which is small enough to pass through material"). Despite this, Dr. Fauci continued to advocate mandating masks for everyone. *See also* Nicholas Jensen, *Bombshell Emails Over What Anthony Fauci Knew*, AUSTRALIAN (June 3, 2021, 6:30 PM), https://www.theaustralian.com.au/subscribe/news/1/?sourceCode=TAWEB_WRE170_a&dest=https%3A%2F%2Fwww.theaustralian.com.au%2Fscience%2Fbombshell-emails-over-what-anthony-fauci-knew%2Fnews-story%2F39c108c393a660b85dce452e4eb4a6b3&memtype=anonymous&mode=premium&v21=dynamic-groupb-control-noscore&V21spcbehaviour=append.

[449] The conduct of The Israeli Ministry of Health was controversial. For further information, see Guy Shinar, *How the Israeli Ministry of Health Became an Agent for Pfizer*, BROWNSTONE INST. (Oct. 18, 2022), https://brownstone.org/articles/how-the-israeli-ministry-of-health-became-an-agent-for-pfizer.

[450] The right to free speech is a basic right in Israel and is protected under the Human Dignity and Liberty Basic Law. Basic Law: Human Dignity and Liberty Amendments of 1994, SH 90; *see, e.g* Toy Staff, *Mandelblit Says Elected Officials Cannot Block Citizens on Social Media,* TIMES ISR. (Feb 2, 2022), https://www.timesofisrael.com/mandelblit-says-elected-officials-cannot-block-citizens-on-social-media.

[451] *See* Mordechai Sones, *Israel Health Ministry Blocks Dissenting Citizens on Twitter; Legal Experts: 'Definitely Illegal'*, AM.'S FRONTLINE DRS. (June 27,2021), https://www.globalresearch.ca/israel-health-ministry-blocks-dissenting-citizens-twitter-legal-experts-definitely-illegal/5749333?pdf=5749333 (Children's medical rights advocate Dr. Avshalom Carmel wrote: "The Ministry of Health is blocking citizens who criticize it? That's called McCarthyism, isn't it? Is it Corona fascism, or just the misuse of high-tech knowledge by an unknown programmer?").

[452] *See, e.g.*, Kang-Xing Jin, *Keeping Our People and Informed About the Coronavirus*, META (Dec. 18, 2020), https://about.fb.com/news/2020/12/coronavirus/#keeping-our-teams-safe; Vijaya Gadde & Matt Derella, *An Update on Our Continuity Strategy During COVID-19*, TWITTER BLOG, (Mar. 16, 2020), https://blog.twitter.com/en_us/topics

result, these platforms mistakenly removed, blocked access to, or made it difficult to share, high-quality content.[453] These practices applied even when the content was research that was published in one of the world's oldest and most influential general medical journals: the scientific BMJ.[454] The harm done to human rights and civil liberties will be difficult to fix, and such infringements can creep beyond the context of emergencies.

At this time (October 2022), when almost all COVID-19 restrictions have been lifted, we realize that many of the steps taken to combat the virus were misguided and caused more harm than good.[455] Even under a different scenario in which such steps might have been required, both implementing a privacy-by-design approach and safeguards, and forbidding the most dangerous and intrusive practices of surveillance are necessary to prevent the rise of the surveillance state. Liberal democracy is not a given, it is something we have to fight for every day.[456]

***

I would like to conclude with a personal take on the general topic of human rights, civil liberties, and health in general. About two years ago, my mother—Aviva Lavi—died. Her death was sudden and unexpected. She *did not* die due to the virus, but rather because of the lockdowns, the government's restrictions, and the idea that prioritization of curbing the spread of the virus over any other medical problem. If human rights and civil liberties were preserved, she probably would have still been living happily with us. Due to the

/company/2020/An-update-on-our-continuitystrategy-during-COVID-19.html (last updated Apr. 1, 2020).

[453] JASON A. GALLO & CLARE Y. CHO, SOCIAL MEDIA: MISINFORMATION AND CONTENT MODERATION ISSUES FOR CONGRESS 7 (2021), https://crsreports.congress.gov/product/pdf/R/R46662.

[454] Researchers blew the whistle on data integrity issues in Pfizer's vaccine trials and published their findings in the scientific BMJ, one of the world's oldest and most influential general medical journals. Shortly after, readers began reporting a variety of problems when trying to share this article on social media. "Some reported being unable to share it. Many others reported having their posts flagged with a warning about "[m]issing context . . . [i]ndependent fact-checkers say this information could mislead people," even though the article is a scientific high-quality source of information. *See* Fiona Godlee & Kamran Abbasi, *COVID-19: Researcher Blows the Whistle on Data Integrity Issues in Pfizer's Vaccine Trial*, BMJ (Dec. 17, 2021), https://www.bmj.com/content/375/bmj.n2635/rr-80.

[455] *See e.g.*, Sarah Knapton, *Lockdown Effects Feared to be Killing More People than Covid*, TELEGRAPH (Aug. 18, 2022) https://www.telegraph.co.uk/news/2022/08/18/lockdown-effects-feared-killing-people-covid.

[456] VELIZ, *supra* note 62, at 96.

aggressive lockdown in Israel between March and May, people were not allowed to travel beyond 0.06 (100M) miles from their homes.[457] Police officers were finding those that were just wanting to breathe outside air.[458] Moreover, everything was closed, and there was nowhere to go. Therefore, my mother barely came out of the house and did not walk much. My mother was not very afraid of the virus and would otherwise go out—not to crowded places, but she definitely would not have stayed at home.

After the first lockdown, something went wrong because of her lack of activity, and she started falling without a reason. So, we went to orthopedic doctors and neurologists, but they could not find the problem. Her Computed Tomography (CT) scan turned out fine, and we had appointments for Magnetic Resonance Imaging (MRI) tests and other medical tests, but she broke her foot before these appointments could happen. At the hospital, they did not bother to carry out any medical tests, even after asking them to do so, and disclaimed responsibility, even though they had the medical equipment to carry out the tests and find the reason why she was falling. But, they conducted four COVID-19 tests that turned out negative, as if COVID-19 was the only medical problem that existed. After a week or so, they sent her to a medical rehabilitation hospital, but there the staff also neglected to treat her properly. At the rehabilitation hospital, she received few physiotherapy sessions because they were understaffed due to quarantine. Moreover, due to the COVID-19 restrictions, they allowed only one family member to visit her for only one hour per day. When she arrived at the rehabilitation hospital, she was aided by a walker. When she came home, about a month later, she needed a wheelchair. We invited a private physiotherapist to our home and, after checking on my mother, he told us that she was likely to walk again with proper care. A day later, however, she suddenly had a heart failure and died. She was only

---

[457] Keren Kaplan Mintz et. al, *See or Be? Contact with Nature and Well-Being During COVID-19 Lockdown*, 78 J. ENV'T PSYCH. 1, 2 (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8555442/pdf/main.pdf ("During this lockdown, stay-at-home orders restricted people to remain within 100 m of home.").

[458] *See* Amir Kurtz, *Covid-19 Crisis Sidelined Individual Rights and Hurt Relations Between Police and the Public*, CALCALIST (May 17, 2020), https://www.calcalistech.com/ctech/articles/0,7340,L-3823670,00.html ("One of the most memorable moments of the coronavirus (Covid-19) era in Israel was the story of a surfer who came out of the sea to find a big group of police officers waiting to arrest him for violating the state-imposed lockdown."); *Watch: Police Swarm Tel Aviv Surfer Said to Refuse to Leave Water*, TIMES ISR. (Apr. 25, 2020), https://www.timesofisrael.com/watch-police-swarm-tel-aviv-surfers-who-allegedly-refused-to-leave-water.

seventy-five years old and had no other medical problems. I have no doubt that her heart failure was connected to the lack of treatment and a feeling of helplessness.

The health system neglected many other people that were not even infected by the virus, but had other medical issues. Others without medical problems also became ill. Elderly people cognitively deteriorated at nursing homes during the lockdowns because family members, who would have otherwise visited, were restricted from visiting and frontally communicating with them.[459]

The Israeli government, as well as other governments that took similar steps, by depriving citizens of their human rights and civil liberties and prioritizing COVID-19 over everything else, caused tremendous harm, not only to democracy but also to individuals' health. Such an infringement on rights and liberties has cost the life of my dearest of all.

I dedicate this Article to the memory of my mother—Aviva Lavi—who will always be remembered, loved, and dearly missed.

---

[459] *See* NAT'L CONSUMER VOICE FOR QUALITY LONG-TERM CARE, THE DEVASTATING EFFECT OF LOCKDOWNS ON RESIDENTS OF LONG TERM CARE FACILITIES DUE TO COVID-19 (Jan. 15, 2021), theconsumervoice.org/uploads/files/issues/Devasting_Effect_of_Lockdowns_on_Residents_of_LTC_Facilities.pdf.


SETON HALL UNIVERSITY
1856
HAZARD YET FORWARD