Coronavirus Surveillance and Palestinians

Elia Zureik and David Lyon

Abstract

Public health initiatives directed towards the mitigation of COVID-19 vary tremendously from country to country, depending on social-historical and political-economic factors. In the case of Israel/Palestine, already existing health disparities are reproduced more starkly in COVID-19 conditions. However, Israel's colonial project in Palestine also appears in sharp relief, seen most clearly in the controversial involvement of the Israeli Security Authority (Shin Bet) in mass surveillance, digital contact tracing, and related high-tech policing of quarantine orders.

Keywords

Surveillance; coronavirus; COVID-19; public health; biopolitics; settler colonialism; Israel; Palestine.

On 14 March 2020, Israel's then prime minister Benjamin Netanyahu announced that Israel would employ advanced digital monitoring tools, developed for counterterrorism, to track carriers of the coronavirus and to slow the spread of COVID-19. Within forty-eight hours, a legal framework was produced, permitting the Israeli Security Authority, or Shin Bet, and the police to use metadata in the service of public health.[1] A resolution relating to the Shin Bet's expanded use of data should have been presented for parliamentary approval but, due to disarray in the Knesset, the government enacted emergency regulations allowing the Shin Bet's use of metadata and police use of location to combat the coronavirus.

Serious criticism of this measure ensued, particularly of the permission it granted elements of the security apparatus to track down citizens in a manner previously used for counterterrorism, without proper privacy protections, oversight, or safeguards against misuse. Several NGOs objected and the Israeli High Court of Justice issued an interim order limiting the use of Shin Bet powers under the emergency regulations and forbidding their use by the police. By one measure, the efficacy of these measures did not justify their use: after securing the fifth extension of the contact-screening emergency regulation in early September of 2020, the success rate of contact tracing was reported to be a meagre 13.5 percent.[2] More generally, however, introducing the Shin Bet into the realm of public health meant treating Israeli Jews as "security threats" – as "terrorists" and, by extension, as Palestinians.

Despite this, the plan to link the Shin Bet and public health went ahead. Health officials passed details of those who tested positive for COVID-19 to the Shin Bet, which returned a list, derived from a hitherto secret national database, of every person with whom COVID-19-positive individuals had been in close contact over the preceding two weeks.[3] To be "in close contact" with another means to be within two meters of them for at least fifteen minutes. Those listed as "close contacts" received a text requesting that they go into isolation at home and remain there. Apparently, using geolocation data from mobile phones, the Shin Bet pinpointed about 4,600 people who subsequently tested positive, thus pioneering a dubious partnership between national security and public health.[4]

At the same time, the police were enabled to use phone location data to verify that those quarantined were complying with their instructions. Enforcement tactics included the use of drones to check that quarantined individuals were actually in their homes.[5] The Israeli police claimed to have made 403 arrests, but the Knesset committee that provides police oversight, the Foreign and Overseas Defense Committee, halted this work on the grounds of unnecessary violation of privacy.[6]

Yet information about how different groups in Israel have been affected by the Shin Bet–public health coronavirus collaboration is lacking. While some argue that low figures for infection and morbidity in Palestinian communities inside Israel is due to their diligence and community spirit, or to the relative youth of the Palestinian population in Israel, others have argued that the absence of testing in these communities is responsible for artificially low figures.[7] Meanwhile, Naftali Bennett, then defense minister and now prime minister, proposed a scoring method, based on data gathered by the Health Ministry and Shin Bet, to guide COVID-19 policies, with Orthodox Jews and Palestinians presumed to be the more prominent carriers of the virus and thus targeted for sealing off from others.

The racialization of the coronavirus is not unique to Israel. Recently, a group of researchers described political leaders' public responses to the pandemic as reinforcing "racial discrimination, doubling down, for example, on border policies and conflating public health restrictions with anti-immigrant rhetoric."[8] The researchers cited statements by Matteo Salvini, previously deputy prime minister of Italy, who blamed immigrants in Europe for the spread of COVID-19, and U.S. president Donald Trump,

who used anti-Asian rhetoric to attack China as the source of the virus and responsible for its spread.

Yet the nexus of securitization, racialization, and public health has taken on particular characteristics in Israel. In the coronavirus world, Palestinians in the West Bank, the Gaza Strip, and Israel have been regarded as sources of the outbreaks, to be treated as threats to the individual and collective security of Jewish Israelis and thus deserving of increased attention, but whose individual and communal health outcomes are relatively neglected by authorities.[9] In one example, Netanyahu blamed the spread of COVID-19 on Palestinian citizens of Israel, claiming that "instructions are not strictly adhered to in the Arab sector," and suggesting that without the "cooperation" of Palestinian citizens, "a lot of people will die."[10] Speaking to the BBC, the retired Shin Bet agent-handler Arik Brabbing claimed that the Shin Bet "saved lives from terror, but it saves lives also from the corona[virus]."[11] Further, he confirmed that the same methods are used for both purposes. Ahmad Tibi, a member of the Knesset, objected to using the coronavirus to justify the recruitment of former Shin Bet agents as analysts to collect data on Palestinians in Israel, describing the practice as "scandalous" and describing those who approved it as "stupid, arrogant, and racist. It is a decision based on the stereotype that Arabs always constitute a security threat to the country."[12]

This article is concerned with the implications for civil liberties and data privacy of measures taken to contain the spread of coronavirus in Israel-Palestine. Such measures include Israel's use of tracking technology through mobile phones to identify mobility, location, and contacts of citizens and non-citizens exposed to the coronavirus. The development of these technologies during the COVID-19 pandemic has implications not only for Palestinians in Israel and the occupied Palestinian territories today, but also for continued surveillance when the worst effects of the contagion are mitigated.

Militarization of Health Care

As noted, Israel, or more accurately its domestic intelligence agency the Shin Bet, has advocated access of mobile phone technology to gather metadata of individuals who have been in close contact with those who tested positive for COVID-19 and connect them with government offices, especially the Ministry of Health. Although the Shin Bet claimed that it would not collect the content of intercepted phone calls and messages, it will be able to collect any credit history that is stored on the phone.[13] There is no oversight in place regarding the use of such tracking technology. Moreover, according to the Israeli army, the information collected through contact tracing would not be limited to coronavirus containment efforts, but could be used for other purposes as Israel sees fit.

Thus, the government instructed Palestinian workers to use a mobile phone application to secure information pertaining to their time spent in Israel. This "would allow the army to track the Palestinians' cellphone location, as well as access notifications they receive, files they download and save, and the device's camera."[14]

The app, without which Palestinians would not be able to access work in Israel, requires them to agree "voluntarily" to the following statement:

> You agree and declare that you know that all the information you are asked to provide is not required by law or defense regulations, and it is provided of your own free will, so that we can make use of it as we see fit. In addition, you consent that we may store the information you have provided to us in our databases based on our considerations.[15]

The Shin Bet and Mossad, Israel's national intelligence agency, also recruited Israeli manufacturers of military cyberware, such as the NSO Group and Elbit Systems, to join efforts in supplying Israeli hospitals with hardware to combat the coronavirus.[16] Bennett, who headed the far-right religious alliance in the Knesset, was enthusiastic about involving the NSO Group, ignoring the highly controversial human rights background of the NSO Group and its involvement in criminal activity by peddling its Pegasus software to Middle Eastern and Latin American governments who are using it to track and eliminate dissidents, journalists, and others seen as challenges to their absolute authority.[17] The Mossad is similarly notorious: in a recent exposé, journalist Ronen Bergman acknowledged the connection between the Mossad and other unsavory regimes worldwide, noting that "the Mossad's efforts were easier in nondemocratic countries where intelligence agencies have more influence with the rulers."[18] Further, accounts of the Mossad's efforts to assist in the fight against the coronavirus are largely exaggerated, as journalist Yossi Melman noted: "Contrary to the flattering reports about the Mossad's cloak-and-dagger operations to acquire medical equipment, most of it was purchased officially in Europe and China, where the organization has no particular advantage."[19]

Joining the rush to combat coronavirus, Elbit Systems announced plans to manufacture ventilators that are in short supply in Israel (one per 2,500 Israeli citizens, compared to one per 1,655 in the United States), and boasted to have developed a "remote coronavirus testing system" that, according to press reports, uses radar to "measure the temperatures and heartbeats of patients without actually touching them."[20] Elbit Systems is a major Israeli exporter of arms that at the end of the third quarter of 2021 advertised a 20 percent growth in revenues from arms exports and a backlog of arms orders worth $13.6 billion.[21] Elbit System advertises its arms (which include cluster bombs and drones) as "battle proven," having supplied the Israeli army during its horrific 2014 Gaza offensive, which killed more than two thousand Palestinians, including more than five hundred children.[22] Elbit Systems also provided surveillance equipment for what Israel calls the "West Bank Barrier" and Palestinians call the Apartheid Wall, declared illegal by the International Court of Justice, and took part in other projects such as the U.S.–Mexico border wall.[23]

Privacy advocates warned against extending the military use of contact-tracing technologies and argued that the line between the military and the civilian sector is becoming increasingly blurred. Although this observation is made primarily regarding the Jewish Israeli sector, Palestinians have complained from the outset of the militarization of contact-

tracing technology and the state's use of social media to track Palestinian citizens' exposure to the pandemic. Observers drew attention to a possible slippery slope of expanding government surveillance, especially after Netanyahu asked the Shin Bet to collect additional information about individuals. The editorial board of the newspaper *Haaretz* warned that Netanyahu was using fake concerns about a "popular revolt" to expand government powers, and headlined its reaction: "Israeli government is invading our privacy under the guise of battling coronavirus … while riding roughshod over [the] right to privacy."[24] As one observer wrote:

> For years, Israel's intelligence community has gotten used to employing electronic surveillance methods – characterized by an ever-increasing sophistication and penetration – to track enemies and Palestinian populations under occupation. Now, as a new threat emerges and the world order is transformed in an instant, it has the perfect excuse to invade the lives of Israeli citizens.[25]

It did not take long for civil and human rights organizations to decry Israeli spy agencies' tactics as cynical, leading to violations of individual privacy and human dignity. The Arab Center in Israel for the Advancement of Social Media, for example, noted that "monitoring and tracking people 24 hours a day, 7 days a week – their location, calls, camera, and headsets – under the pretext of preventing the transmission and spread of infection, is a violation of people's right to privacy."[26] Lawyer Diana Buttu, a former advisor to the Palestinian Authority, expressed alarm about possible function creep, commenting: "My fear is that once this coronavirus threat passes, some measures will also be normalized this time: from racism in health care, to holding Palestinians and their health care system hostage, to surveillance, to home demolitions and blockades – all in the name of 'public security.'"[27]

Civil liberties organizations also petitioned the Israeli supreme court. The Association of Civil Rights in Israel explained: "The health of the public is of utmost importance, but these measures, born out of draconian emergency regulations, are bringing us to a slippery slope when it comes to the invasion of privacy and democracy."[28] Israel's supreme court, "citing grave dangers to privacy," ruled "that the government must bring its use of mobile phone tracking deployed in the battle against the new coronavirus under legislation."[29]

By May 2020, no fewer than twenty-seven countries worldwide were using data from cellphone companies to track the movement of individuals as part of their coronavirus contact tracing efforts.[30] Suspicions extended beyond privacy groups, as noted by a *Washington Post*–University of Maryland poll that reported that "3 in 5 Americans say they are unwilling or unable to use an infection-alert system being developed by Google and Apple."[31] Fueling these suspicions are reports that the employment of surveillance technology does not always deliver accurate information for public health purposes. Reliance on geolocation technology is seen as particular unreliable in high density patient areas: "Given the sharp rise in the number of coronavirus patients, contact tracing and geolocation are no longer effective at

finding all the people a given patient might have infected."[32] And a UK-based report in the *Lancet* shows that contact tracing requires a high proportion of cases to self-isolate and a high proportion of their contacts to be traced, combined with physical distancing, for the technique to make meaningful impact on containing the virus.[33] Indeed, Petra Molnar and Diego Naranjo criticized clandestine efforts to enlist spy firms to combat the coronavirus and efforts based around curtailment of movement and access to sites such as refugee camps as not only unethical but ineffective in addressing the coronavirus:

> The answer to stopping the virus is not increased surveillance through new technology or preventing access to the camps for medical personnel. Instead, we need to redistribute resources and ensure access to health care for all people, regardless of their immigration status.[34]

While we continue to witness the inefficacy and inequalities that such policies have produced in the realm of public health, the effects in the realm of surveillance and social control may be less visible but just as insidious.

Implications of Israel's COVID-19 Surveillance

A key concern raised by critics of the Shin Bet–Ministry of Public Health partnership has been the extent to which lives are needlessly affected by surveillance. People who are not likely to be affected by the virus – for example, because "contact" with an afflicted individual was fleeting or casual – may be unnecessarily disadvantaged. This parallels questions raised more generally about the global national security surge following 11 September 2001.[35] In this regard, COVID-19 represents the second major state of exception, after 9/11, within which legal and regulatory safeguards have been suspended to allow surveillance under the guise of safety.[36]

Further, it is typical of the "tech solutionism" of the current surveillance capitalist climate that data analytics would be seen to have obvious relevance for dealing with the effects of a global pandemic. Surveillance capitalism involves intensive partnerships and mutual reliance between public and private entities, so commercial considerations intrude all-too-easily into what should be public health-led initiatives.[37] This is especially true of Israel, which prides itself on its military-incubated, leading-edge technological prowess, especially in the fields of information and communication technology.[38] Technology is thus presented as holding solutions that are more effective or efficient than well-established public health practices such as manual contract-tracing. However, to the degree that technology offers potential public health benefits – although it is worth noting that even Singapore, an early adopter of digital contact tracing, warns against over-reliance on technology, insisting that contact tracing should be "human-fronted"[39] – it also raises new issues of data security and privacy.

Digital contact tracing raises major issues of human rights that should be publicly and democratically addressed. In the United Kingdom, for instance, a legal submission

to a parliamentary committee on the question of digital contact tracing pointed out that the risks of such systems require serious and sustained attention to human rights.[40] According to the submission, addressing such concerns would mandate an ethics advisory board, independent oversight, ongoing review, and remedies for violations.[41] At present Israel has no external and independent intelligence oversight body to oversee the implementing of emergency coronavirus regulations.[42]

The second important consideration is the confusion caused by the term "privacy." In Israel, as in many other countries, human rights and civil liberties abuses may continue despite legal adherence to privacy regulations. The problem is that data privacy issues are frequently seen as personal problems, not as a systemic fault-line of data-generated inequalities. Sharp questions have been raised about the privacy implications of large-scale use of personal data, originating primarily in widespread and commonplace platform use, and finding new uses in digital contact tracing and other technological "solutions" to the pandemic purveyed by governments.[43]

The issue arose in Israel when Bennett proposed that the controversial NSO Group – a spyware company – be involved in developing a coronavirus scoring system. Bennett argued that this system would in no way violate individual privacy: "The data required to operate the system by authorities and governments is statistical and aggregated, not personal data."[44] The same argument was made in the aftermath of the Edward Snowden revelations about the work of the U.S. National Security Authority in 2013. U.S. officials insisted that the "metadata" used by the NSA for their investigations was similarly "not personal." Yet those metadata actually revealed exactly the kinds of information that hiring a private detective might find – where a particular person was, when they were there, and what they were likely to have been doing.

It is not sufficient, however, to confront innovations such as digital contact tracing with privacy demands to mitigate the risks. Privacy is frequently considered to be a personal, individual concern, even if its protection is also seen to support more public values such as freedom of expression or freedom of movement. The risks of personal data ending up in the "wrong" hands or otherwise being misused are real, and privacy legislation is available to counteract such eventualities. But this is also a systemic problem, based on fundamental inequalities – in this case to healthcare – and unfair practices. These can all too easily translate into basic "automated inequality" in healthcare as in other areas.[45] In Israel, gross disparities in access to adequate health care obtain between the Jewish Israeli population and the Palestinian population of Israel, the West Bank, and Gaza. These disparities have been made particularly visible in the treatment of the outbreak of coronavirus. This is why issues of corona surveillance demand to be seen as ones of digital rights and, beyond that, data justice in Israel in particular, but elsewhere as well.[46]

A third implication – which again echoes concerns elsewhere in the world, but with particular relevance to Israel – is that measures put in place in a time of health crisis, a state of exception produced by the pandemic, will become routine. Further, there is justified fear that such measures will not only be applied in an increasing array of

circumstances ("function creep"), but will lead to the repurposing of whole systems in the goal of maximizing data collection ("mission creep").[47] This issue, seen writ large in the responses to 9/11, is now rearing its threatening head once again. In the case of the post-9/11 "global war on terror," despite efforts to insert "sunset clauses" in post-9/11 emergency measures, many supposedly exceptional practices remained in place indefinitely. Measures initially enacted to address an exceptional circumstance – marshalling personal data from the moment of booking an airplane flight, for example – quickly morphed into part of the unremarkable "normal" expectations. Here, the "exceptional circumstances" of a pandemic are the pretext for extraordinary measures that not only exacerbate inequalities today but also leave the door open for further data sharing with other government agencies in the future.

Today, many of Israel's initiatives to mitigate the impact of the coronavirus show evidence of what Rob Kitchin calls "control creep" – the progressive expansion of the social control apparatus.[48] As Kitchin writes: "The fine-grained mass tracking of movement, proximity to others, and knowledge of some form of status (beyond health, for example) will enable tighter forms of control and is likely to have a chilling effect on protest and democracy."[49] The fact that it might be anticipated does little to alleviate the concerns of those who provide evidence that today's COVID-19 containment initiatives are simply more of the same.[50] What began as a drive to collect phone-users' metadata – which Israeli authorities regard as "anything but content" – to influence and sell advertisements to those users, is now conscripted for an unproven form of contact tracing and for limiting the movements of citizens, especially Palestinians, whose mobility is already tightly restricted within Israel. If control creep is a fear even in fully democratic societies, how much more concerning is it in the case of Israel?

Conclusion

Michel Foucault captured the distinction between sovereignty and governmentality as that between "the right to *take* life and *let* live" and "the right to make live and to let die" – that is, biopolitics.[51] Of course biopolitics is not applied uniformly, to manage and enhance the well-being of the entire population; rather, racism is constitutive of the biopolitical process. As Patricia Ticineto Clough and Craig Willse argue, "Foucault argues that it is a form of racism that allows for death in biopolitics, the death of some populations that are marked as inferior and harmful to the larger body of the nation."[52] The coronavirus has made clear that which was already evident to observers of Israel's biopolitical regime: that Jewish Israelis are to be made to live, while Palestinians were to be left to die.[53]

Some politicians in Israel admitted publicly that the spread of coronavirus does not obey geographic or racial boundaries. Israel's president, Reuven Rivlin, seized on this point during his March 2020 telephone call to the Palestinian Authority president Mahmud Abbas: "The world is dealing with a crisis that does not distinguish between people or where they live. . . . The cooperation between us is vital to ensure

the health of both Israelis and Palestinians."[54] Yet Israel was unwilling at the outset to aid Palestinians during the coronavirus crisis. The then prime minister Benjamin Netanyahu personally incited Jewish Israelis against Palestinians, whom he invariably described as terrorists, and did little to assuage the fears of Palestinians in the West Bank and Gaza. To justify the expansion surveillance in response to the coronavirus, he invoked "technological means" also used in the "fight against terrorism."[55]

It is clear that strategies to contain COVID-19 are unevenly distributed on racialized lines in Israel/Palestine. Preexisting public healthcare disparities that disproportionately disadvantage Palestinians have become vividly visible in the time of coronavirus. Decisions about who may live and who is allowed to die may be obscured by bureaucratic regimes and contact-tracing algorithms, but their effects are all too physical. Meanwhile, in the process of dealing with COVID-19, the same forces of racialized biopolitics strengthen their hand by ensuring that emergency measures can become routinized, permitting even greater surveillance and thus control over populations. Only basic changes that result in equality of citizenship status will permit equal, fair, and just public health treatment in Israel/Palestine, whether in a pandemic or in "normal" circumstances. Instead, what we have seen over the course of the pandemic is the infiltration of the public health sector by the security sector, with implications that may outlast the pandemic itself.

Elia Zureik is Professor Emeritus of Sociology at Queen's University in Ontario, Canada. He is the author of Israel's Colonial Project in Palestine: Brutal Pursuit *(Routledge, 2016), co-editor with David Lyon of* Computers, Surveillance, and Privacy *(University of Minnesota Press, 1996), and co-editor with David Lyon and Yasmeen Abu-Laban of* Surveillance and Control in Israel/Palestine: Population, Territory, Power *(Taylor & Francis, 2010; Routledge, 2011).*

David Lyon is former director of the Surveillance Studies Center and Professor Emeritus of Sociology and of Law at Queen's University in Ontario, Canada. His newest book is Pandemic Surveillance *(Polity Press, 2022).*

Endnotes

1 Amir Cahane, "The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers," *Lawfare,* 11 June 2020, online at (lawfareblog.com) bit. ly/3tA4Gln (accessed 11 February 2022).

2 Refaella Goichman, "Israel Extends Digital Surveillance of Citizens, Despite Lack of Coronavirus Data," *Haaretz*, 13 October 2020, online at (haaretz.com) bit.ly/3qulZSS (accessed 11 February 2022).

3 "Israel's Coronavirus Surveillance Is an Example to Others – of What Not to Do," *Privacy International*, 1 May 2020, online at (privacyinternational.org) bit.ly/3izzmMY (accessed 11 February 2022); Richard Silverstein, "Israel Is Militarising and Monetising the COVID-19 Pandemic," *Wire*, 20 April 2020, online at (thewire.in) bit. ly/3ugFFdY (accessed 11 February 2020).

4 Benoit Dupont, "COVID-19: les dérives possibles de surveillance des donneés personnelles," *Conversaton*, 29 May 2020, online at (theconversation.com) bit. ly/3LaZc6C (accessed 11 February 2021).

5 Liza Lin and Timothy W. Martin, "How Coronavirus is Eroding Privacy," *Wall Street Journal*, 15 April 2020, online at (wsj.com) on.wsj.com/3NeUo1F (accessed 11 February 2022).

6 "Israel's Coronavirus Surveillance."

7 Tamar Shiloh Vidon, "Israel's Arabs Escaped the Worst, but COVID-19 Signals Economic Trouble Ahead," *France 24*, 22 May 2020, online at (france24.com) bit.ly/37Yr6o5 (accessed 11 February 2022); Nihaya Daoud, "The Reluctance to Test Israeli Arabs for COVID-19 Is a Ticking Time-bomb," *Haaretz*, 31 March 2020, online at (haaretz. com) bit.ly/3qqgR1R (accessed 11 February 2022).

8 Delan Devakumar, Geordan Shannon, Sunil S. Bhopal, and Ibrahim Abubakar, "Racism and Discrimination in COVID-19 Responses," *Lancet* 395, no. 10231 (2020): 1194.

9 Lana Tatour, "Palestinian Citizens of Israel: A Perfect Coronavirus Scapegoat," *Middle East Eye,* 8 April 2020, online at (middleeasteye. net) bit.ly/3iwcVsk (accessed 11 February 2022).

10 Tatour, "Palestinian Citizens of Israel."

11 Tom Bateman, "Coronavirus: Israel Turns Surveillance Tools on Itself," *BBC News*, 12 May 2020, online at www.bbc.com/news/world-middle-east-52579475 (accessed 18 January 2022).

12 Afif Abu Much, "Ex-Shin Bet Analysts Recruited to Fight Coronavirus within the Israeli-Arab Society," *al-Monitor*, 7 October 2020, online at (almonitor.com) bit. ly/3L8E9RX (accessed 11 February 2022).

13 Noa Landau, Yaniv Kubovich, and Josh Breiner, "Israeli Coronavirus Surveillance Explained: Who's Tracking You and What Happens with the Data," *Haaretz*, 18 March 2020, online at (haaretz.com) bit.ly/3wxbr9k (accessed 11 February 2022).

14 Nir Hasson, "Amid Coronavirus Crisis, Israel Tells Palestinians to Download App That Tracks Phones," *Haaretz*, 8 April 2020, online at (haaretz.com) bit.ly/3twhYit (accessed 11 February 2022).

15 Hasson, "Amid Coronavirus Crisis"; Joshua Shuman, "Pandemic Tracing in Israel Blurs Line between Military, Civilians," *Media Line*, 19 November 2020, online at (themedialine.org) bit.ly/3ujTGaM (accessed 11 February 2022).

16 David Cronin, "Has Israel's Weapons Industry Really Declared War on a Virus?" *Electronic Intifada*, 11 April 2020, online at (electronicintifada.net) bit.ly/3ukmMXt (accessed 11 February 2022); Elia Zureik, "Settler Colonialism, Neoliberalism, and Cyber Surveillance: The Case of Israel," *Middle East Critique* 29, no. 2 (2020): 219–35

17 Bill Marczak, John Scott-Railton, S. McCune, Bahr Abdul Razzak, and Ron Deibert, "Hide and Seek: Tracking NSO's Pegasus Spyware in 45 Countries," *Citizen Lab*, 28 September 2018, online at (citizenlab.ca) bit.ly/3Iz9XxB (accessed 11 February 2022); Zureik, "Settler Colonialism, Neoliberalism, and Cyber Surveillance."

18 Ronen Bergman, "Israel's Not-So-Secret Weapon in Coronavirus Fight: The Spies of Mossad," *New York Times*, 12 April 2020, online at (nytimes.com) nyti.ms/37NATgp (accessed 11 February 2022).

19 Yossi Melman, "The Mossad Is Flaunting Too Much during the Coronavirus Crisis," *Haaretz*, 19 April 2020, online at (haaretz. com) bit.ly/3qp1FlR (accessed 11 February 2022).

20 Cronin, "Has Israel's Weapons Industry"; "Israeli Defense Firm Elbit Systems to Produce Ventilators," *Reuters*, 13 April 2020, online at (reuters.com) reut.rs/3tvq0Z9 (accessed 11 February 2022).

21 Elbit Systems, "Elbit Systems Reports Third Quarter 2021 Results," 23 November 2021, online at (mayafiles.tase.co.il) bit.ly/3Ix7WCg (accessed 11 February 2022).

22 B'Tselem, "50 Days: More than 500 Children: Facts and Figures on Fatalities in Gaza, Summer 2014," 20 July 2016, online at (btselem.org) bit.ly/36HLcC3 (accessed 11 February 2022); Jonathan Cook, "If Coronavirus Overwhelms Gaza, Israel Alone Is to Blame," *Counterpunch*, 17 April 2020, online at (counterpunch.org) bit.ly/36gIQdR (accessed 11 February 2022).

23 Will Parrish, "The U.S. Border Patrol and an Israeli Military Contractor Are Putting a Native American Reservation under 'Persistent Surveillance'," *Intercept*, 25 August 2019, online at (theintercept.com) bit.ly/36JenVD (accessed 11 February 2022).

24 *Haaretz* Editorial, "Israeli Government Is Invading Our Privacy under the Guise of Battling Coronavirus," *Haaretz*, 27 April 2020, online at (haaretz.com) bit.ly/3qsZvSg (accessed 11 February 2022).

25 Amos Harel, "Israeli Army Can't Solve Coronavirus Crisis, Ex-security Official Says," *Haaretz*, 13 April 2020, online at (haaretz.com) bit.ly/3quyvS9 (accessed 11 February 2022).

26 7amleh – the Arab Center for the Advancement of Social Media, "Netanyahu Imposes Dangerous 'Big Brother' Surveillance under the Pretext of a Security Response to the Coronavirus," *Association for Progressive Communications*, 23 March 2020, online at (apc.org) bit.ly/3KZ11Ds (accessed 18 January 2022).

27 Diana Buttu, "Pandemic Lays Bare Israel's Systemic Racism," *Electronic Intifada*, 8 April 2020, online at (electronicintifada.net) bit.ly/37UIZUE (accessed 11 February 2022).

28 "We Won: HCJ Sides with ACRI Petition against Shin Bet Tracking Civilians," *Association for Civil Rights in Israel*, 26 April 2020, online at www.english.acri.org.il/post/__154 (accessed 11 February 2022).

29 Maayan Lubell, "Israel's Top Court Says Government Must Legislate COVID-19 Phone-Tracking," *Yahoo! News*, 26 April 2020, online at (yahoo.com) yhoo.it/3NhvGh2 (accessed 11 February 2022).

30 Kareem Fahim, Min Joo Kim, and Steve Hendrix, "Cellphone Monitoring Is Spreading with the Coronavirus. So Is an Uneasy Tolerance of Surveillance," *Washington Post*, 2 May 2020, online at (washingtonpost.com) wapo.st/3qsUR6J (accessed 11 February 2022).

31 Fahim, Kim, and Hendrix, "Cellphone Monitoring."

32 Refaella Goichman, "Israeli Defense Ministry Teaming Up with Spyware Firm NSO to Fight Coronavirus," *Haaretz*, 29 March 2020, online at (haaretz.com) bit.ly/3ww4PrN (accessed 11 February 2022).

33 Adam J. Kucharski, Petra Klepac, Andrew J. K. Conlan, Stephen M. Kissler, Maria L. Tang, Hannah Fry, Julia R. Gog, and W. John Edmunds, on behalf of the CMMID COVID-19 Working Group, "Effectiveness of Isolation, Testing, Contact Tracing, and Physical Distancing on Reducing Transmission of SARS-CoV-2 in Different Settings: A Mathematical Modelling Study," *Lancet*, 16 June 2020, online at doi.org/10.1016/S1473-3099(20)30457-6 (accessed 11 February 2022).

34 Petra Molnar and Diego Naranjo, "Surveillance Won't Stop the Coronavirus," *New York Times*, 15 April 2020, online at (nytimes.com) nyti.ms/3unwcle (accessed 11 February 2022).

35 Hina Shamsi and Alex Abdo, "Privacy and Surveillance Post-9/11," *Human Rights Magazine*, 1 January 2011, online at (americanbar.org) bit.ly/37VoUgX (accessed 18 January 2022).

36 Shohana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019); Sebastian Klovig Skeleton, "Surveillance Capitalism in the Age of COVID-19," *Computer Weekly*, 13 May 2020, online at (computerweekly.com) bit.ly/3JBTnP8 (accessed 11 February 2022).

37 Zuboff, *Age of Surveillance Capitalism*.

38 Priscilla Offenhauer, *Israel's Technology Sector* (Federal Research Division, Library of Congress, November 2008), online at (apps.dtic.mil) bit.ly/3Jygl9N (accessed 11 February 2022).

39 Mark Zastrow, "Coronavirus Contact-Tracing Apps: Can They Slow the Spread of COVID-19?" *Nature*, 19 May 2020, online at www.nature.com/articles/d41586-020-01514-2 (accessed 11 February 2022).

40 "Written Evidence from Professor Lorna McGregor et al (COV0090)," 1 May 2020, online at committees.parliament.uk/writtenevidence/3973/pdf (accessed 11 February 2022).

41 "Written Evidence from Professor Lorna McGregor."

42 Cahane, "Israeli Emergency Regulations."

43 David Meyer, "Privacy Could Be the Next Victim of the Coronavirus," *Fortune*, 21 March 2020, online at (fortune.com) bit. ly/3ILRqyt (accessed 11 February 2022).

44 Andrew Roth, Stephanie Kirchgaessner, Daniel Boffey, Oliver Holmes, and Helen Davidson, "Growth in Surveillance May Be Hard to Scale Back after Pandemic, Experts Say," *Guardian*, 14 April 2020, online at (theguardian.com) bit.ly/3iuK5IU (accessed 11 February 2022).

45 Virgina Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018).

46 David Lyon, "The Coronavirus Pandemic Highlights the Need for a Surveillance Debate beyond 'Privacy,'" *Conversation*, 24 May 2020, online at (theconversation.com) bit.ly/37NkHf3 (accessed 11 February 2022).

47 Natan Sachs and Kevin Huggard, "Technosurveillance Mission Creep in Israel's COVID-19 Response," *TechStream*, 9 June 2020, online at (brookings.edu) brook. gs/354X1SB (accessed 11 February 2022).

48 Rob Kitchin, "Civil Liberties *or* Public Health, or Civil Liberties *and* Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19," *Space and Polity* 24, no. 3 (2020): 362–81, online at (tandfonline.com) bit.ly/3D4p3Ki (accessed 11 February).

49 Kitchin, "Civil Liberties *or* Public Health."

50 Martin French and Torin Monahan, "Disease Surveillance: How Might Surveillance Studies Address COVID-19?" *Surveillance and Society* 18, no. 1 (2020): 1–11.

51 Michel Foucault, *"Society Must Be Defended": Lectures at the Collège de France 1975–1976* (New York: Picador, 2003), 241.

52 Patricia Ticineto Clough and Craig Willse, "Gendered Security/Natioanl Security: Political Branding and Population Racism," *Social Text* 28, no 4 (Winter 2010): 45–62, quote at 49.

53 See, for example: Ronit Lentin, "Palestine, Palestinians, and Israel's State Criminality," *State Crime Journal* 5, no. 1 (2016): 32–50; Nadera Shalhoub-Kevorkian, *Security Theology, Surveillance, and Politics of Fear* (Cambridge: Cambridge University Press, 2015).

54 Alan Baker and JCPA, "Israel, the Palestinians, Coronavirus, and Peace," *Israel Hayom*, 26 March 2020, online at (israelhayom.com) bit. ly/3IxSPbM (accessed 11 February 2022).

55 Edo Konrad, "Equating Coronavirus with Terror, Netanyahu Turns Surveillance Powers on Israelis," *+972 Magazine*, 15 March 2020, online at www.972mag.com/netanyahu-surveillance-coronavirus/ (accessed 11 February 2022).