Article

Nontargets: Understanding the Apathy Towards the Israeli Security Agency's COVID-19 Surveillance

Shaul A. Duke

Independent Researcher
saduke@gmail.com

Abstract

This article tackles one of the latest—but nonetheless baffling—displays of public apathy towards surveillance: that of much of the Israeli public towards the decision to recruit the Israeli Security Agency (Shin Bet) to do COVID-19 contact tracing during the ongoing coronavirus pandemic. The case of a secretive state agency being authorized to do surveillance on its citizens for a strictly non-security-related matter seems to realize many of the dangers that surveillance/privacy scholars warn about with regards to surveillance expansion, function creep, and the creation of a surveillance state. I contribute to existing literature about apathy towards surveillance and the privacy paradox by offering the term “nontargets” as an explanation. This term suggests that, alongside social groups that are likely to be targeted by a given surveillance application, there are certain recognizable nontargets that most likely will not bear the brunt of the surveillance, at least not in the short- and medium-term, and thus do not fear it. In the case at hand, which is examined using a qualitative context-bound study, I suggest that Jewish-Israelis are such a nontarget group with regards to this novel Shin Bet surveillance, which explains a significant part of their apathy towards it.

Introduction

On March 17, 2020, the Israeli government issued an emergency ordinance directing the Shin Bet (also known as the Israeli Security Agency, Israel’s internal secret service) to undertake coronavirus contact tracing. That is, the Shin Bet (or Shabak in Hebrew) was authorized to utilize the data it collects through the continuous electronic tracking that it regularly performs in order to detect people who were in proximity with a COVID-19 carrier in the fourteen-day period prior to being positively identified as infected. The purpose of this tracking is to direct everyone who was in close proximity with the infected individual to enter quarantine and thus curb the spread of the pandemic. The Shin Bet’s coronavirus tracking, which was initially based on the government ordinance and later approved by the Knesset’s (Israeli parliament’s) Intelligence and Secret Services Sub-Committee, continued up until June 10, 2020, when the pandemic seemed to be winding down in Israel. It was later renewed on July 1, 2020, when infection rates spiked again, first based on a Knesset act that carried a temporary status, which was supposed to expire within twenty-one days, and later based on another Knesset act which is supposed to expire within six months, on January 21, 2021 (Birnhack, forthcoming).

Although the use of the internal secret service for a civilian matter, which has no parallel in any other global democracy coping with COVID-19, did encounter some opposition, this opposition was limited to a number of experts, political actors, NGOs, and concerned citizens. The majority of Israelis either supported this measure or were indifferent to it. Most remained indifferent even as warnings against the use of the Shin Bet were loudly voiced, precluding any notion of widespread ignorance (more on that ahead). Indeed, this

Duke, Shaul A. 2021. Nontargets: Understanding the Apathy towards the Israeli Security Agency's COVID-19 Surveillance. *Surveillance & Society* 19(1): 114-129.

<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2021 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#)

indifference to the use of secret service surveillance for a public health issue is indicated by the July 1 renewal of the tracking in the second wave of the coronavirus in Israel, by its continued use even after Israel's State Comptroller deemed it highly ineffective, and by its endurance throughout 2020 in its entirety.

Such apathy towards what many surveillance and privacy scholars consider the crossing of the Rubicon (e.g., Goichman 2020b) poses a dilemma. While scholars in the field are no strangers to public apathy, there are also recurrent research findings of public awareness, opposition, and resistance to surveillance processes (e.g., Hargittai and Marwick 2016; Budak and Rajh 2018). There is also the expectation and hope, among at least some scholars in the field, that when confronted with a clear and imminent danger from a new surveillance application, the public will not be passive and will offer active opposition.

This article argues that there is no contradiction between previous findings of a resistive public and the case at hand. I suggest the term “nontargets” as a way to understand surveillance apathy. I suggest that Jewish Israelis perceive themselves as nontargets of Shin Bet surveillance and that their apathy results from an accurate understanding of the short- and medium-term risks they face.

This research is based on a qualitative historic analysis of recent events. It was informed by a variety of primary and secondary sources, including court cases, laws, bills, reports, news articles, website material, correspondences, interviews, and academic papers. Interviews and correspondence were specifically sought on topics that were not covered by public records and remained in need of further clarification. The data sources were analyzed and pieced together in order to create a timeline of events and, when possible, determine causality. I believe the integration of a variety and an abundance of material is required in order to provide a relatively comprehensive account of the social context in which this new surveillance process has been implemented. Special emphasis is placed on differences in opinions and motivations within a single entity, such as “the Israeli public” and “those opposed to the Shin Bet’s surveillance.”

Apathy Towards Surveillance: Discovery, Rejection, and a Complex View

Since the intensification of surveillance practices with the online revolution of the mid-1990s, public apathy has become a popular scholastic topic. Surveillance and privacy scholars were surprised at the passive acceptance displayed by the public towards new surveillance technologies, by the ease with which people were willing to divulge personal information, and by what seemed to be an urge to share and self-expose online (e.g., Barnes 2006; Kim 2004). Moreover, as time passes, the number of texts and scholars dealing with this issue grows, making the mere existence of such apathy even less understandable (e.g., Best 2010). This dissonance is even greater considering that warnings about the dangers of top-down surveillance practices are sounded repeatedly, raising awareness and reaching a growing percentage of the population.

Apathy towards surveillance was also observed in the thread of research revolving around the “privacy paradox” (e.g., Carey and Burkell 2009; Lee, and Rha 2016; Pentina et al. 2016; Taddicken 2014). Research in this thread found that, despite declared attitudes and opinions that support the need for privacy and privacy-protection, people often do not take, or take insufficient, privacy-protection measures. That is, there is a gap between awareness and actions. This has become a prolific line of research, and while some have indeed found a privacy paradox, others have found none or have found that it disappears when inserting some mediating variables (e.g., Acquisti, Brandimarte, and Loewenstein 2015; Baek 2014; boyd and Hargittai 2010; Budak and Rajh 2018; Chalklen and Anderson 2017; Gerber, Gerber, and Volkamer 2018; Hargittai and Marwick 2016; Heravi, Mubarak, and Choo 2018; Kokolakis 2017; Romele et al. 2017).

Cumulatively, studies of apathy towards surveillance suggest that there is a significant behavioral apathy towards surveillance but that this apathy is selective and can be mostly explained by understanding the context in which people operate.

Secret Service Surveillance: A Surveillance Nightmare

Although the study of surveillance gained most of its popularity in the age of online data and proliferation of mobile devices, much of its origins, both scholarly and artistic, date back to the twentieth century. In these origins, it was not the current hybrid model of private-and-state surveillance that seemed most menacing but that of an all-encompassing state surveillance that spreads to varied facets of life. George Orwell's *1984* (1949) may be the perfect example of this, with its government ministries that try to know and control everything and from which one cannot escape.

This fear of state surveillance is no coincidence. The twentieth century saw a widespread use of low- and high-tech surveillance by secret agencies operating in the shadows. These uses of secret service surveillance facilitated notorious cases of citizen and human rights violations on a mass scale, for instance, in the Soviet Union, in Latin America, and even in the United States (against social activists and “subversives”). It is these historic cases, in which surveillance technology was paired with secrecy, that informed the ultimate surveillance nightmare for many. These cases show how extensive, obtrusive, arbitrary, and deadly an apparatus of surveillance that operates in the dark can be. Guilt was often determined within such dark-surveillance apparatuses based on association, proximity, or false information and, with no checks and balances, there was no possibility to correct the record and prevent the detrimental consequences. When surveillance scholars say that surveillance breeds distrust (e.g., Campbell 2004; Chan 2008; Starr et al. 2008; Murakami Wood et al. 2006), it might be speculated that those eras of secret surveillance regimes in which people constantly lived in fear lie in the back of their minds.

Surveillance Expansion and Slippery Slopes: COVID-19 as the Perfect Storm

The pervasiveness of surveillance and the idea that it is constantly expanding are at the heart of the surveillance studies discipline and are realized in key concepts such as surveillance creep and surveillance function creep¹ (Marx 1988; Murakami Wood et al. 2006; Nelkin and Andrews 1999) and the surveillance society² (Gandy 1989; Murakami Wood 2009). Opposing this expansion and sounding the alarm are part of the task that students of surveillance/privacy take upon themselves in what became known as “public sociology.”

There is a pronounced fear of a slippery slope in which a breach of certain boundaries will allow for a significant increase in surveillance practices with detrimental effect. This idea is supported by a progressive observation that governments may use extraordinary events to pass reactionary policies that could not pass otherwise (Klein 2007). In the field of surveillance, one such watershed event was the aftermath of the 9/11 terror attacks, which gave license for government agencies to electronically monitor en masse all citizens in every country on earth and to retain a permanent record of the data (Barnes 2006; Chan 2008; Davis and Silver 2004; Gandy 2002; Lyon 2004; Snowden 2019). It is in this light that we can understand the apprehension of surveillance scholars worldwide over the possibility that the COVID-19 pandemic will be used as another surveillance watershed event.

Nonetheless in Our Case: Apathy

The case of the COVID-19 pandemic in Israel seems to epitomize privacy and surveillance scholars' fears with regards to the dangers mentioned above. Israel's Security Agency's electronic surveillance data, which up until now was accessed almost exclusively to combat what was defined as security threats, has now been

¹ Surveillance creep refers to the way that the use of surveillance slowly expands into our surroundings and to different facets of life. Surveillance function creep refers to the process in which a tool of surveillance that was created for goal A is repurposed and then used for goal B as well (Marx 1988; Murakami Wood et al. 2006; Nelkin and Andrews 1999).

² Surveillance society refers to a state of affairs in which surveillance increasingly defines relationships and social settings (Gandy 1989; Murakami Wood 2009).

utilized to fight the spread of the pandemic. As mentioned repeatedly by Israeli experts, NGOs, and the media, Israel is the only democracy that chose to utilize its secret service to fight the coronavirus (Eiserbuch 2020; Goichman 2020b; Natour 2020). Moreover, we must recognize that Israel's internal secret service is not an average one but a very potent and robust security agency with many ongoing "projects" and strong capabilities (Barnea 2020), which means fears of abuse are in proportion to this potency. Fears also run high in light of the Shin Bet's known and well-recorded pattern of human rights violations (HCJ 5100/94; Sheleff 2002; State Comptroller of Israel 2000; Stroumsa 2020, telephone interview; The Public Committee against Torture in Israel 2020).

Yet despite all of this, and as will be further demonstrated in the empirical analysis, "Most of the citizens, so it seems, are reacting to this breach of privacy with relative apathy" (Goichman 2020b, my translation). Some considered this use of the Shin Bet a non-issue, and some even saw it as the natural solution to such a situation (Melman 2020). Moreover, although there are some limited indications of acts of evasion by Israeli citizens, such as leaving their cellphone at home or using a burner phone, these were non-declarative acts led by a personal wish to avoid quarantine (Leshem 2020). Most importantly, no significant protest or rally was carried out, despite an intensification of demonstrations and rallies in Israel during 2020 over COVID-19-related government policies and actions. Instead, the struggle that did take place against this move was carried out in court and in the Knesset, i.e., with tools that can be utilized even without considerable public support for a given cause. Fortunate for the opposition, both the Israeli Supreme Court and the Knesset do show some commitment to the privacy discourse.

Targeted vs. Universal Surveillance and the Concept of Nontargets

One of the major ongoing debates within the study of surveillance is the question of targeted versus universal surveillance. Is current surveillance universal and applicable to all and, consequently, risky to the population at large, or is it mostly targeted, posing special dangers to specific groups? Of course, the question is not a naïve dichotomy so much as it is a dilemma of how much of the risk that top-down surveillance entails is limited to some and which targeted groups run the most risk (Bigo 2004; Campbell 2004; Chan 2008; Earl 2011; Fiske 1998; Gandy 2011; Haggerty and Ericson 2000; Handel 2011; Henman 2004, 2005; Lyon 2004; Murakami Wood et al. 2006; Norris 2003; Speak and Graham 1999;).

This article suggests that the potential risk that most top-down surveillance produces is primarily relevant to certain groups and much less relevant (or hardly relevant at all) to others. Part of the perplexing apathy that students of privacy/surveillance encounter should be attributable to this differential risk. Specifically, I wish to suggest that there are "nontargets" that may be identified by understanding the social/political context of a given surveillance application. These nontargets lack fear of the surveillance process due to a realistic understanding that this monitoring body and its surveillance do not pose a significant danger to them in the short- to medium-term and that any limited harm may be curbed quite easily by applying pressure. While these nontargets, if asked in a survey, may say that privacy is important to them and that they are worried by surveillance—they do not effectively fear certain specific forms of surveillance and thus are very likely to present behavioral passivity towards them.

In the case at hand, I wish to suggest that Jewish Israeli citizens are the nontargets of Shin Bet operations at large, and of Shin Bet surveillance in particular, and thus are mostly apathetic to the latter's expansion to civil applications; that even if they take into account the unforeseen detrimental effects of such surveillance by a secretive semi-autonomous agency (and many of them do not), they, as Jewish citizens, can bank on their influence to stop or mitigate it and significantly lower the risk.

The Israeli Security Agency (Shin Bet)

The Israeli Security Agency was established a short time after the creation of the State of Israel in 1948. As with other internal security agencies (e.g., the British MI5), it has both intelligence functions (gathering the

information) and execution functions (acting upon it, either reactively or preemptively). In its early days, the mere existence of the Shin Bet was secretive, and this state of affairs lasted for an entire decade in which even mentioning the Shin Bet by name was prohibited (Pascovich 2015).

Throughout the decades, the Shin Bet was involved in several publicized incidents that exposed some of its more notorious methods of operation. Among them was the practice of killing terrorists after or during interrogation (e.g., Zamir 2019) and the practice of torture as part of the interrogation process (HCJ 5100/94; State Comptroller of Israel 2000). These revelations also exposed another anti-democratic practice: covering up unlawful practices under the guise of national security, including lying under oath in a court of law. Taken together, these practices revealed a tendency of the Shin Bet to operate outside the law with impunity (Pascovich 2015; Sheleff 2002; State Comptroller of Israel 2000).

Since the 1980s, we have been able to talk of the quasi-democratization of the Shin Bet in which its functions were defined and it was placed under the rule of law. The biggest step in this direction came as a result of a High Court ruling regarding the torture of detainees (HCJ 5100/94). Besides disallowing several forms of torture (unless in a “ticking bomb” situation), the Israeli High Court of Justice put much of the blame for human rights transgressions on the legislator, which refused to define the Shin Bet’s authority and framework of operation. This provoked a rapid process of legislation and, as early as 2002, the Knesset passed the General Security Service Act, which defined the Shin Bet’s functions and breadth of operation (Pascovich 2015; *The General Security Agency Act* 2002). As Pascovich (2015: 67) puts it: “Today, Shin Bet is much more regulated and supervised, at least theoretically, than it used to be.”

Despite this partial democratization, including its increase in transparency, the Shin Bet continues to be a major source of human rights violations. Among other things, torture—as human rights organizations define it—continues to be prevalent in some of the Shin Bet’s investigations, with people being physically and emotionally abused, sometimes to the point of being hospitalized in critical condition (Stroumsa 2020, telephone interview; The Public Committee against Torture in Israel 2020). Transparency was not extended to Shin Bet investigations, and this extremely high-tech organization refrains from recording videos of interrogations to this day. Moreover, in the last few years, the Shin Bet was implicated in questioning activists and in detaining activists at the airport in a way that is likely to create a chilling effect (The Association for Civil Rights in Israel 2018; Yakir 2018).

The Shin Bet as an Ethnic Organization

Israel’s nationality is defined ethnically as a Jewish state, although 21 percent of its population (excluding the Occupied Palestinian Territories) is Arab, as opposed to being defined by its jurisdiction within its borders as most nation-states are (Smootha 2010; Yiftachel 1999). This designation is not just a formality. Israel gives special privileges to all Jews of the world in the form of the right of return, which is the right to immigrate to Israel and receive automatic citizenship as well as aid in settling down (*Law of Return* 1950). Beyond the right of return, there are several other major laws (e.g., *Israeli Citizenship Law* 1952; *Foundations of Law* 1980; *Israel as the Nation-State of the Jewish People* 2018) that define Israel’s national interest by its Jewishness and that place the interests of its Jewish citizens above those of its Arab citizens (Benziman and Mansour 1992: 131–132; Lentin 2017). These special privileges, in addition to the many informal privileges, produce unofficial but consistent discrimination against Palestinians—citizens and noncitizens alike (Shafir and Peled 2002).

Indeed, when classifying Israel’s regime, some critical scholars call it an “ethnic democracy” (Smootha 2000) while others refer to it as an “ethnocracy” (Yiftachel 1999), but either way these scholars categorize it as a low-level democracy (Jamal 2000; Smootha 2010). Israel’s ethnic regime is realized in the operation of virtually every government agency but especially those that have to do with national security.

The Shin Bet, from this perspective, is an enlisted agency that is geared against Palestinians, citizens and noncitizens alike. Practically, this means that virtually no Palestinian is employed by the Shin Bet; that risks

to the state and the greater good are assessed and perceived from a Jewish national-chauvinistic stance, which renders Palestinians an inherent threat; and that Jews are treated significantly differently from Arabs.

Historically, this Palestinians-as-enemies policy was initially realized in the role that the Shin Bet played during the period of the Military Government (1948–1966). This regime, applied exclusively toward the Palestinian-Israeli population, was “a form of martial law which suspended many of the rights and legal protections that citizenship afforded” (Degani 2015). The Shin Bet used classic colonialist/imperialist forms of surveillance and domination in order to control Palestinians’ everyday lives. Among other things, it encouraged Arabs (through negative and positive incentives) to inform on their fellow-Palestinians’ “subversive behavior,” suspicions that would lead to backlisting (Benziman and Mansour 1992; Pedahzur 2009). Just around the time in which the Military Government was ending, the focus of the Shin Bet turned to another Palestinian population: that of the territories occupied in the 1967 war.

Throughout its existence, the Shin Bet has dedicated much of its energies to dealing with Arab terrorism while its record of locating and catching Jewish terrorists has been subpar at best (Pascovich 2017), even though Jewish terrorism has been in existence throughout Israel’s history, especially since the occupation of the Palestinian territories in 1967. This ethnic discrimination does not only apply to who is targeted but also to how suspects are treated. As far as it has been reported, the previously mentioned Shin Bet practice of severe torture and killing during/after interrogation was used exclusively against Arabs. While it seems that the practice of killing has stopped, the Shin Bet’s current severe interrogation tactics are still overwhelmingly geared towards Palestinians (Stroumsa 2020, telephone interview; Yellin 2020, email correspondence), and it seems that even in those rare occasions in which the Shin Bet does carry out a forceful interrogation of Jews, it does not use all of the tactics it uses against Palestinians (Stroumsa 2020, telephone interview).

Reactions to the COVID-19 Surveillance

As mentioned, the Shin Bet’s COVID-19 surveillance did not encounter much opposition among the Israeli public. Opposition was scarce even though the promoters of this tool have not, as of this writing, provided any robust indication that the Shin Bet’s coronavirus contact tracing is more effective than “regular” human epidemiologic investigation. Moreover, an independent examination carried out by Israel’s state comptroller, published in a report on October 26, 2020, has explicitly concluded that the Shin Bet’s contact tracing produces an extremely high rate of false-positives and that human epidemiologic investigations are significantly more accurate. Among other things, it found that out of the almost 500,000 contacts that the Shin Bet traced in the examined period, only between 3.5 and 4.6 percent were identified as positively infected (State Comptroller of Israel 2020). This means that a multitude of people were unnecessarily sent into isolation.

Early on, in order to justify the use of the Shin Bet tool, its promoters framed the problem as one of available personnel (e.g., HCJ 2109/20). Human epidemiologic investigation requires trained workers and, as complaints went, there was insufficient personnel for a full-blown outbreak. That said, even if the personnel explanation was a valid government justification during the first round of the pandemic in Israel (when there were only twenty-seven investigators; see Yanko 2020a), its validity in the last few months is dubious, since there are now around four-thousand investigators working towards this end (Goichman 2020c).

Technological alternatives—i.e., surveillance tools that, at the least, would not be run by the secret service and may also be less intrusive in other respects—were proposed but in a limited fashion. The government put forth the greatest effort into HaMagen, a voluntary, open-code smartphone app that performs COVID-19 contact tracing. This app, which at the peak of its popularity was installed by 1.5 million Israelis (roughly 17% of the citizen population) suffered from recurrent bugs (Bohbot 2020a, 2020b; Sokol 2020), which led around 700,000 Israelis to uninstall it (Goichman 2020b). While bugs in the initial implementation of a technology are to be expected, they nevertheless were not tolerated by the government. This reaction came even though some of the errors were supposed to be fixed in the next app version, which shifted from relying

just on GPS to a combination of GPS and Bluetooth, and despite the much better privacy offered by this app (in both early and late versions) and its basis in voluntary participation (Cohen 2020; Natour 2020). The government took a long time to relaunch the HaMagen app and was accordingly accused of neither making an earnest effort to encourage the use of this app nor seriously pursuing alternative technologies (Dolev 2020; HCJ 4762/20). The HaMagen 2 app was launched at the end of July 2020, this time accompanied by a media campaign, but public reception was lukewarm and the government declared it a failure, deciding to continue with Shin Bet tracking (Yanko et al. 2020).

It seems the Shin Bet's contact tracing has been given preference by the government due to, among other things, the fact that it is not voluntary and that it does not rely on possession of a smartphone. In Israel, although extremely popular, smartphones are not possessed universally, with Ultra-Orthodox Jews—which constitute around 10% of the population—being the major group that does not carry them. That said, even from a purely technical view, the Shin Bet tool has significant drawbacks as well. The primary one is that it relies on GPS location data, which produce many errors since their accuracy tends to vary and they ignore height (being on separate floors), the existence of walls (being in close proximity but separated by a wall or a door; Avriel 2020), and may even identify two persons as contacts if they were merely on the phone with each other (Arutz Sheva 2020). Indeed, in the time it has been operating, the Shin Bet's coronavirus surveillance has created thousands of Kafkaesque situations in which people who were not exposed to a coronavirus carrier were ordered to self-quarantine (Breiner and Peleg 2020; Goichman 2020a; Gontarz 2020; Linder 2020a, 2020b; Linder and Goichman 2020; Foreign Affairs and Defense Committee 2020).

The (Limited) Opposition

The opposition that the Shin Bet coronavirus surveillance did encounter came largely from three (somewhat overlapping) directions: experts, NGOs, and political actors.³ I will now discuss the case of each group.

Surveillance and Privacy Experts

The opposition posed by experts is a testament to the development of the privacy/surveillance fields in Israel, which are established enough to be part of the conversation about this tool, albeit with limited influence. At this stage of the evolution of the privacy/surveillance discourse, administrators, high-ranking officials, and politicians cannot ignore it. Similar to other types of “progressive” discourses (e.g., climate change and gender equality), such educated and media-aware personnel cannot afford to disregard it, but similar to these other discourses, these high-ranking policymakers often just pay lip service to it. That is, they do not seem to give it much importance when weighing it against other values/interests. For instance, throughout the COVID-19 pandemic, high-ranking officials in the Israeli Ministry of Health have been voicing repeated acknowledgments of the need to safeguard privacy (e.g., Binyamin 2020; HCJ 2109/20), yet they have pushed time and time again for intrusive surveillance measures (e.g., Appelberg 2020).

Surveillance and privacy experts have also had a significant chance to influence ordinary citizens through their access to the media, primarily through interviews and op-eds (e.g., Aschkenasy 2020; Goichman 2020b; Schwartz Altshuler and Levine 2020; Yablonko 2020). Media outlets, which seem to be drawn to the issue of surveillance, gave these experts an ample platform to sound their warnings, with some journalists, such as Refaella Goichman of the Israeli newspaper *TheMarker*, making coverage of this surveillance their pet project. Yet, it seems that these recurrent media appearances manage to strike a chord with just a narrow group and that their ability to provoke public action is limited. In the case at hand, there were two clear indications that their persuasion power is minimal. One had to do with the proposed law (which eventually passed) enabling the Shin Bet to carry out coronavirus surveillance with the backing of a

³ It is worthwhile to note that there were also minor and more sporadic oppositions posed by niche groups, prominent people, and certain government agencies. Among the opposers were former and current Shin Bet top brass, yet it should also be noted that, while these officials objected to using the Shin Bet for contact tracing, the agency as a whole cooperated fully with the surveillance and with various claims that it is more effective than what Israel's State Comptroller concluded.

Knesset act as opposed to a government decision. The public was given a week to comment online on the bill and approximately a thousand comments were posted almost exclusively opposing the law and repeating the talking points of privacy/surveillance experts (The Authorization 2020). The second was an online petition against the Shin Bet's contact tracking that managed to gather a few thousand signatures (Zazim Community Action 2020). While both are achievements in and of themselves, these figures (when taking into account that, excluding the Occupied Palestinian Territories, Israel has a population of nine million) are also indicative of the very limited appeal warnings against Shin Bet surveillance had.

Nevertheless, and primarily via their direct access to decision-making forums, surveillance/privacy experts seem to have had some success in imposing limitations and safeguards on the use of the Shin Bet tool and may have played a part in postponing its reuse before Israel plunged into the second coronavirus wave.

NGOs

NGO opposition came in the forms of court petitions, letters to government agencies, appearances in Knesset forums, issued reports, and media interviews and op-eds. NGOs share with the previous group (experts) the credit for the very limited success in combating public apathy and the credit for the modest-but-existing success in pushing policymakers to place checks and oversights over the Shin Bet's coronavirus tracking.

The centerpiece of NGO opposition to this particular surveillance is undoubtedly the petitions to Israel's High Court of Justice made in March 2020. These petitions were made almost immediately after the surveillance started and were given a final ruling just forty days later (HCJ 2109/20). Four petitions were filed and then merged into one case by the court: one by a lawyer-activist, one by the Union of Journalists in Israel, one by the Association for Civil Rights in Israel—an NGO that frequently deals with privacy issues—and one jointly by Adalah, an Arab-Israeli NGO, and the Joint Arab List, a coalition of three parties that cater to Palestinian-Israeli voters.

Although these petitions did not succeed in nullifying the expansion of secret service surveillance to the field of healthcare, they provoked a court ruling that placed significant limitations on this tracking. Among them: enacting immediate oversight of the surveillance by a Knesset sub-committee, imposing a debate on the necessity of the Shin Bet tool while considering possible alternatives, and ruling that any further extension of the tool's use (beyond a certain date) will be done via legislation. Further petitions that were issued by NGOs later in 2020 (e.g., HCJ 6732/20) seem, as of now, to have had similar results.

As mentioned above, courts are a possible avenue of influence that allow one to circumvent public apathy. Yet Israel's High Court of Justice seems reluctant to overrule the decisions made by the executive branch, and other than placing some limitations, it effectively passed the buck to parliament, where—in the face of public apathy—government can continue to use this Shin Bet tool for a public health application. It thus seems that it is very hard to actually circumvent public apathy towards surveillance.

Political Actors

Overall, political opposition to the Shin Bet's coronavirus tracking came from two directions: Arab representatives and anti-Netanyahu opposition. The latter group mostly claims that this surveillance is used to perpetuate Israel's current Prime Minister's hold on the government by giving power to an agency that is subordinate to him. According to them, Netanyahu's aims are both to prevent social protest and to promote a sense of emergency in Israel (Azulay and Yanko 2020; Eiserbuch 2020; Goichman and Amit 2020). While both of these goals can be easily categorized as undemocratic, there is no robust explanation given by these members of the opposition as to how exactly the Shin Bet's coronavirus tracking is used to achieve these ends. Interestingly, these opposition politicians refrained from making the historical connection to the Shin Bet's past, in which it was occasionally used for political purposes (Pascovich 2015).

The second source of political opposition came from the Arab Joint List, which together with Adalah—an NGO that works to defend the rights of Palestinians (both in Israel and the occupied territories)—petitioned against the Shin Bet's COVID-19 tracking. Their opposition to the use of the Shin Bet for coronavirus

surveillance seems to run much deeper than the anti-Netanyahu opposition and, while other actors seem to fear the misuse of the Shin Bet, both Adalah and the Joint Arab List seem to fear the use of it. That is, they fear that the Shin Bet's jurisdiction of operation is now expanding to non-security issues with the approval of the High Court and with grave repercussions (Adalah 2020; Jabareen, interview).

As mentioned above, the Shin Bet has a long and consistent history of targeting Israeli Palestinians, including in one period (1948–1966) in which they controlled every aspect of Arab life. Although not to the same degree, both the targeting and the branching out to civilian areas of operation continues in current times. For instance, the Shin Bet has been involved in hiring and promotion decisions in the Arab-section of the Israeli education system. In this involvement, which last occurred as recently as 2019 (Yanko 2020b), it strives to promote “loyal” and thwart “subversive” educators in a way that was deemed detrimental and unlawful (HCJ 8193/04). Another example, this time on the topic of free speech, revolved around the publication of a proposal for a “Democratic Constitution for Israel” by Palestinian-Israeli organizations. The Shin Bet intervened to prevent a public discussion on these papers, admitting that the risk here is not to Israel's security but to its national identity (Jabareen 2007; Jabareen 2020, telephone interview).

Adalah's (2020: 7) words seem to sum it up: “As history has proven, the Shin Bet has often intervened in civilian issues, particularly regarding Palestinians, whose individual, cultural and political lives have been a constant target of surveillance and repression.” Thus, as opposed to the more abstract and remote potential damage the Shin Bet poses to Jews in Israel, for Arabs the Shin Bet is a concrete threat, which means allowing it to legally branch out to any civilian function is a further risk.

Arabs and Jewish Israelis and the Shin Bet

Another more direct indication of each group's stance towards the Shin Bet's coronavirus tracking comes from two surveys, carried out five months apart, reporting on public sentiments towards the Shin Bet's role in the coronavirus crisis. The first survey, administered by the Israel Democracy Institute, was taken at the beginning of the pandemic—hence, before the NGOs' and surveillance experts' criticism was hashed out in the media—and clearly shows an Arab-Jewish divide in such support. When asked about their trust in the Shin Bet and in the governmental officials to make appropriate use of location data (e.g., use it solely for the prevention of infection in the current crisis), 63 percent of Jewish respondents said that they do trust the Shin Bet while only 38 percent of Arabs responded in the affirmative (Hermann and Anabi 2020).

The second survey was commissioned by the Ministry of Intelligence and carried out during August 2020. It found 67 percent support among Jews for continuing to use the Shin Bet's technological tools in order to fight coronavirus (i.e., contact tracing), compared with 41 percent support among Arabs (Komam 2020), virtually the same finding revealed in the first poll. Both polls taken together clarify that: (1) apathy towards Shin Bet's coronavirus surveillance is consistent and not diminishing and (2) objection to this surveillance is significantly higher among citizen-Palestinians than Israeli Jews, with no indication that the gap between them is closing.

The second survey also asked a more general question regarding the confidence respondents had in the Shin Bet. Here, the gap between Arabs and Jews was even greater, with 86.3 percent of Jews expressing confidence in this agency, compared with only 38 percent of Arabs (Komam 2020). This attitude is consistent with past attitudes towards the Shin Bet in prior surveys (e.g., Yuchtman-Yaar and Hermann 2016).

The finding that most Israeli Jews ultimately do not see the Shin Bet's surveillance as a threat to them is consistent with a surprising recurrent finding I encountered in my own interviews of Jewish human rights activists over a two-year period prior to the COVID-19 pandemic. These activists, who are dealing with issues of Palestinian human rights, who are operating well outside the Jewish consensus, whose organizations are targeted by laws aimed at weakening them, and who face an ongoing delegitimization campaign framing them as traitors and occasionally involving violence, did not report any fear of

government agency surveillance (Afek; Bar 2017, telephone interview; Barag 2017, personal interview; Dukhi 2017, personal interview; Gvanyahu 2019, telephone interview; Konforty 2017, telephone interview; Maor 2019, telephone interview; Montell 2019, telephone interview; Smith 2017, personal interview; Zohar 2017, personal interview). Moreover, when asked directly, interviewees explicitly said that they do not fear such surveillance (e.g., Doe 2017, personal interview; Smith 2017, personal interview).

This attitude cannot be considered complacency on the part of activists regarding the use of surveillance tools, since many activists did express very vivid fears regarding surveillance by the right wing (Afek; Bar 2017, telephone interview; Barag 2017, personal interview; Doe 2017, personal interview; Gvanyahu 2019, telephone interview; Konforty 2017, telephone interview; Maor 2019, telephone interview; Montell 2019, telephone interview; Smith 2017, personal interview) to the degree they adopted a variety of tactics in order to avoid such right-wing surveillance (Duke, forthcoming). Furthermore, this lack of fear comes despite human rights activists being occasionally harassed by the Shin Bet when entering the country and in other circumstances (The Association for Civil Rights in Israel 2018; HCJ 5277/13; Yakir 2018).

Indeed, this lack of fear of the Shin Bet within the Jewish population, even in the most extreme cases (human rights activists), is in sync with the history of this agency, which indicates that Jews are its ultimate nontargets and, therefore, the nontargets of its surveillance by extension. Thus, although utilizing the secret service to undertake coronavirus contact tracing is unproven (and, some would claim, invalidated) as a method, unorthodox in international comparison, and wholly undemocratic, the reaction was one of indifference.

Ultimately, the Shin Bet's contact tracing endured not because the Israeli government and state administration ignore its citizens but because they are responsive to them, specifically to the Jewish majority. This is indicated by the numerous shifts in and back-downs from major state policies aimed at fighting the COVID-19 pandemic. These politicians also routinely order public polls, just like the one the Minister of Intelligence commissioned regarding public support of the Shin Bet's contact tracing. In the words of the Minister of Intelligence: "The results of this poll prove that the Israeli public understands this [the effectiveness of the Shin Bet tool in fighting the coronavirus] and displays trust in the Shin Bet and its excellent work, which will continue as long as it is required" (Komam 2020, my translation).

The Future of the Shin Bet's COVID-19 Surveillance

Although this particular type of surveillance has a large group of nontargets (Jewish Israelis), their lackluster opposition to it is not set in stone. Aside from the significant risk that surveillance systems pose to social groups, there are more mundane and mild detrimental effects that surveillance systems usually produce. Errors and technological limitations create inconvenience to some people and may create Kafkaesque situations in which an automated false-output determines a person's fate for the next two weeks. It is conceivable that, if enough of these detrimental effects are felt, these nontargets will start to turn against such tools.

To a degree, this has already started to happen in Israel. As mentioned above, errors occurred, many of them due to the limitations of GPS technology: people who should not have been quarantined were sent into isolation (Breiner and Peleg 2020; Goichman 2020; Linder 2020a, 2020b; Linder and Goichman 2020; Liss 2020), and some people who knew they were not exposed at the alleged time and place could not appeal, either because there were no channels for appealing or, once channels were in place, because they did not work properly (Breiner and Peleg 2020; Goichman 2020a, 2020b; Gontarz 2020; Linder and Goichman 2020; Rubinstein 2020). There were even cases of hoaxes scaring people into thinking that they were infected or that the Shin Bet was coming to get them (Lukash 2020).

That said, up until now, both the Shin Bet and the Ministry of Health were responsive enough to public opinion to modify their procedures in order to address people's grievances, for instance, by establishing and improving the appeal system (Gontarz 2020; Linder 2020c; Linder and Goichman 2020; Liss 2020) and by

reducing false-positives (Yasur 2020). This adaptiveness in successfully reducing the disruption to everyday living that coronavirus surveillance creates ensures that public apathy will remain potent.

Barring unforeseen developments, it is hard to imagine that a significant part of the Jewish-Israeli population will snap out of its apathy and demand that this Shin Bet contact tracing be halted. What is more likely is that ongoing pressure from experts, NGOs, journalists, certain state agencies, and the courts, together with the waning of the pandemic, will compel government and the Ministry of Health to diminish and eventually end the use of this tool.⁴

Conclusion and Understanding Nontargets

This article offers an answer to a perplexing surveillance development: the relative apathy of Israeli citizens towards the use of its powerful internal intelligence agency's surveillance in the struggle against the COVID-19 outbreak. Using the term "nontargets," I showed that the differential reaction this step did provoke makes perfect sense and dissolves much of this alleged paradox.

Specifically, I suggested that, while Arabs are the Shin Bet's enduring targets, Jews are consistently its "nontargets," which also extends to the Shin Bet's surveillance and, consequently, to the attitudes towards such surveillance. Using the concept of nontargets, I am able to show that apathy towards surveillance, including to this particularly alarming form of it, does exist but that it is not irrational. That said, such apathy's rationality is limited to the short- and medium-term and does ignore potential future developments whereby the organization and/or the surveillance it carries out may change over time, or that some sequence of events may occur that place this passive public at the pointy end of the relationship.

The concept of nontargets takes the idea of surveillance targeting to the next level. Alongside "targets," groups affected by or likely to be affected by the surveillance, there are nontargets—that is, groups that are very unlikely to feel the brunt of the surveillance technology. The existence of nontargets helps explain why some people are so resistive to warnings about the dangers attached to certain types of surveillance: they do not believe they will actually be harmed by it. It also helps us understand statements, such as "I have nothing to hide," which express a belief that this technology does not pose a risk to them.

This type of "I am at no risk" stance is underpinned by an understanding of the organization doing the surveillance, its history, its pattern of operation, the general aim of the surveillance tool, and the access that the said individual may have to the organization. For instance, a white middle-class individual in the US who learns that the police are starting to implement a new surveillance technology for enforcing property crimes in their city can bank on all of the above in order to consider themselves a nontarget. It is not just because they know they will not commit the type of crimes this surveillance is after; it is also that they know that, as white middle-class people, they most likely will not be harassed or inconvenienced by the police. Similarly, when introducing a new biometric ID, individuals from globally-mobile groups, such as businesspeople and professionals, can also rely on all they know about the border agencies and the history of their operation to conclude that they are nontargets.

In those cases, warnings about the detrimental effects of such technologies are likely to fall on deaf ears. The fact that the equivalent organization in other places has been used to target the same group an individual belongs to does not seem to matter, which explains why Jewish Israelis do not seem to be influenced by negative experiences of people from the Soviet Block, authoritarian Latin America, or the US. Moreover, since people's perception of themselves as nontargets is based on the past, they may also miss new dynamics that may not have previously existed. In the case at hand, the Shin Bet was given a task within healthcare surveillance that it had never performed; this may make the technology risky towards the alleged nontargets.

⁴ The latest development being the government's decision to use the tool only to track individuals who refuse to cooperate with human epidemiological investigations (Zaken 2020).

Yet, this is where individuals rely on their access to the organization or the decision-maker regarding the surveillance technology and their ability to stop or reduce the detrimental effect on them.

Acknowledgments

I would like to thank Michael D. Birnhack, Sara Degli Esposti, Ariel Handel, Gary T. Marx, and the two anonymous reviewers for their helpful comments on an earlier draft of this article. Special thanks to Lauren Duke for her valuable insights and assistance.

References

- Acquisti, Alessandro, Laura Brandimarte, and George F. Loewenstein. 2015. Privacy and Human Behavior in the Age of Information. *Science* 347 (6221): 509–514.
- Adalah. 2020. *Adalah's Initial Analysis of the Shin Bet ("Shabak") Coronavirus Cellphone Surveillance Case*. Haifa, IL: Adalah.
- Appelberg, Shelly. 2020. The Head of the Ministry of Health in a Closed Meeting: Want to Open Shopping Malls? Track Visitors. [In Hebrew.] *TheMarker*, April 20. <https://www.themarker.com/coronavirus/1.8793390> [accessed May 26, 2020].
- Arutz Sheva. 2020. The Shin Bet Contact-Tracing Falsely Alerted of Exposure Between People in Phone Contact. [In Hebrew.] *Arutz Sheva*, November 24. <https://www.inn.co.il/news/458314> [accessed December 14, 2020].
- Aschkenasy, Bini. 2020. In Europe They Forbid Security Agencies Surveillance on Citizens—And What about Israel? [In Hebrew.] *TheMarker*, October 8. <https://www.themarker.com/law/.premium-1.9220799> [accessed October 9, 2020].
- Association for Civil Rights in Israel, The. 2018. Detaining Social Activists in Airports. <https://www.english.acri.org.il/post/33> [accessed June 18, 2020].
- Avriel, Eytan. 2020. The Shin Bet's Location System Doesn't Do the Job. This is What Will. [In Hebrew.] *TheMarker*, June 24. <https://www.themarker.com/podcasts/PODCAST-1.8945074> [accessed June 28, 2020].
- Azulay, Moran, and Adir Yanko. 2020. A Heated Debate in the Knesset: "The Epidemiological Investigations are a Hundred Times More Obtrusive Than the Shin Bet Tracking." [In Hebrew.] *Ynet*, June 24. <https://www.ynet.co.il/articles/0,7340,L-5753513,00.html> [accessed June 25, 2020].
- Baek, Young Min. 2014. Solving the Privacy Paradox: A Counter-Argument Experimental Approach. *Computers in Human Behavior* 38: 33–42.
- Barnea, Avner. 2020. The Shin Bet Coronavirus Surveillance. [In Hebrew.] Paper presented at the *Online Surveillance in the Age of Coronavirus and Beyond*, June 15.
- Barnes, Susan B. 2006. A Privacy Paradox: Social Networking in the United States. *First Monday* 11 (9): <https://doi.org/10.5210/fm.v11i9.1394>.
- Benziman, Uzi, and Atallah Mansour. 1992. *Subtenants: Israeli Arabs, Their Status, and the Policy Towards Them*. [In Hebrew.] Jerusalem, IL: Keter Publishing House.
- Best, Kirsty. 2010. Living in the Control Society: Surveillance, Users and Digital Screen Technologies. *International Journal of Cultural Studies* 13 (1): 5–24.
- Bigo, Didier. 2004. Globalized-In-Security: The Field and the Ban-Opticon. *Traces: A Multilingual Journal of Cultural Theory* 4: <https://doi.org/10.4324/9780203926765-7>.
- Binyamin, Idan. 2020. Due to a Delay Caused by the Ministry of Health: The Shin Bet Surveillance Might Come Back. [In Hebrew.] *Shakuf*, June 21. <https://shkifut.info/tag/%D7%9E%D7%A9%D7%A8%D7%93-%D7%94%D7%91%D7%A8%D7%99%D7%90%D7%95%D7%AA/> [accessed July 20, 2020].
- Birnhack, Michael D. Forthcoming. Privacy in Crisis: Constitutional Engineering and Privacy Engineering. [In Hebrew.] *Law and Government in Israel*.
- Bohbot, Hagar. 2020a. "You Have Been Exposed to the Coronavirus": A Malfunction in Hamagen App. [In Hebrew.] *Ynet*, March 28. <https://www.ynet.co.il/digital/technews/article/S1GKAonLU> [accessed May 26, 2020].
- . 2020b. Hamagen App Still Sends False Warnings to Users. [In Hebrew.] *Ynet*, April 5. <https://www.ynet.co.il/digital/technews/article/SJpiMXPvL> [accessed May 26, 2020].
- boyd, danah, and Eszter Hargittai. 2010. Facebook Privacy Settings: Who Cares? *First Monday* 15 (8): <https://doi.org/10.5210/fm.v15i8.3086>.
- Breiner, Josh, and Bar Peleg. 2020. 30 Thousand People Entered Quarantine Due to Shin Bet Coronavirus Tracking. [In Hebrew.] *Haaretz*, July 4. <https://www.haaretz.co.il/health/corona/.premium-1.8969925> [accessed July 5, 2020].
- Budak, Jelena, and Edo Rajh. 2018. Citizens' Online Surveillance Concerns in Croatia. *Surveillance & Society* 16 (3): 347–361.
- Campbell, Nancy D. 2004. Technologies of Suspicion: Coercion and Compassion in Post-Disciplinary Surveillance Regimes. *Surveillance & Society* 2 (1): 78–94.
- Carey, Robert, and Jacquelyn Ann Burkell. 2009. A Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments. In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock, 65–82. Oxford, UK: Oxford University Press.
- Chalklen, Charlotte, and Heather Anderson. 2017. Mothering on Facebook: Exploring the Privacy/Openness Paradox. *Social Media + Society* 3 (2): <https://doi-org.libproxy.lib.unc.edu/10.1177/2F2056305117707187>.

- Chan, Janet B. L. 2008. The New Lateral Surveillance and a Culture of Suspicion. *Surveillance and Governance: Crime Control and Beyond* 10: 223–239.
- Cohen, Sagi. 2020. Hamagen 2 App Won't Save Us as Either—And Apple and Google are to Blame. [In Hebrew.] *TheMarker*, June 24. <https://www.themarker.com/technation/.premium-1.8944903?v=31A030BE08F430A2DF1C7516F1E911F2> [accessed June 25, 2020].
- Davis, Darren W., and Brian D. Silver. 2004. Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America. *American Journal of Political Science* 48 (1): 28–46.
- Degani, Arnon Yehuda. 2015. The Decline and Fall of the Israeli Military Government, 1948–1966: A Case of Settler-Colonial Consolidation? *Settler Colonial Studies* 5 (1): 84–99.
- Dolev, Daniel. 2020. In a Limited Application: The Use of Shin Bet Tracking in the Struggle Against Corona Was Ratified. [In Hebrew.] *Walla*, May 26. <https://news.walla.co.il/item/3363103> [accessed June 2, 2020].
- Duke, Shaul A. Forthcoming. The Dynamics of Imposed Transparency and Its Role in Deep Social Conflicts. In *Trust and Transparency in an Age of Surveillance*, edited by Paweł Laidler and Lora Anne Viola, 1–20. London: Routledge.
- Earl, Jennifer. 2011. Political Repression: Iron Fists, Velvet Gloves, and Diffuse Control. *Annual Review of Sociology* 37: 261–284.
- Eiserbuch, Dafna. 2020. A Controversial Tool. [In Hebrew.] *Davar*, July 1. <https://www.davar1.co.il/233156/> [accessed July 5, 2020].
- Fiske, John. 1998. Surveilling the City: Whiteness, the Black Man and Democratic Totalitarianism. *Theory, Culture & Society* 15 (2): 67–88.
- Foreign Affairs and Defense Committee, The. 2020. *The 23rd Protocol of the Foreign Affairs and Defense Committee*. [In Hebrew.] Jerusalem, IL: The Knesset.
- Gandy, Oscar H., Jr. 1989. The Surveillance Society: Information Technology and Bureaucratic Social Control. *Journal of Communication* 39 (3): 61–76.
- . 2002. Data Mining and Surveillance in the Post-9/11 Environment. Paper presented at the *International Association for Media and Communication Research, Barcelona, Spain, July, 2002*, 1–18. IAMCR.
- . 2011. Consumer Protection in Cyberspace. *Triple C* 19 (2): 175–189.
- Gerber, Nina, Paul Gerber, and Melanie Volkamer. 2018. Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security* 77: 226–261.
- Goichman, Refaella. 2020a. Placement, Movement and Surprise Visits: The Full Map of Who Tracks Us Using the Coronavirus Excuse. [In Hebrew.] *TheMarker*, April 6. <https://www.themarker.com/technation/.premium-1.8742498?v=426E8C338E34706CE3407F44573E76D6> [accessed May 26, 2020].
- . 2020b. Why is the Government Insisting the Shin Bet Be the One to Track Us? [In Hebrew.] *TheMarker*, June 5. <https://www.themarker.com/technation/.premium-MAGAZINE-1.8896687> [accessed June 6, 2020].
- . 2020c. Tens of Meetings—And the Same Result: The State Approved the Shin Bet Tracking Again. [In Hebrew.] *TheMarker*, November 23. <https://www.themarker.com/technation/.premium-1.9323272?lts=1607950122169> [accessed December 14, 2020].
- Goichman, Refaella, and Hagai Amit. 2020. “Instead of Preventing Terrorism, the Shin Bet is Preventing Protest”: The Member of Knesset That is Sure That Netanyahu Enlisted the Coronavirus to the Coalition. [In Hebrew.] *TheMarker*, June 10. <https://www.themarker.com/technation/.premium-1.8908760> [accessed June 11, 2020].
- Gontarz, Nir. 2020. The Assumption That It Isn't Possible to Do Epidemiological Investigations Without the Shin Bet Isn't True. [In Hebrew.] *Haaretz*, July 7. <https://www.haaretz.co.il/magazine/.premium-1.8976594> [accessed July 8, 2020].
- Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–622.
- Handel, Ariel. 2011. Exclusionary Surveillance and Spatial Uncertainty in the Occupied Palestinian Territories. In *Surveillance and Control in Israel/Palestine: Population, Territory and Power*, edited by Elia T. Zureik, David Lyon, and Yasmeen Abu-Laban, 259–275. London: Routledge.
- Hargittai, Eszter, and Alice E. Marwick. 2016. “What Can I Really Do?” Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication* 10: 3737–3757.
- Henman, Paul. 2004. Targeted! *International Sociology* 19 (2): 173–191.
- . 2005. E-Government, Targeting and Data Profiling: Policy and Ethical Issues of Differential Treatment. *Journal of E-Government* 2 (1): 79–98.
- Heravi, Alireza, Sameera Mubarak, and Kim-Kwang Raymond Choo. 2018. Information Privacy in Online Social Networks: Uses and Gratification Perspective. *Computers in Human Behavior* 84: 441–459.
- Hermann, Tamar, and Or Anabi. 2020. *Israeli Voice Index: 76% of Israelis are Afraid of Getting Coronavirus*. Jerusalem, IL: The Israel Democracy Institute.
- Jabareen, Hassan. 2007. *The Unlawful Engagement of the Shin Bet*. [In Hebrew.] Haifa, IL: Adalah.
- Jamal, Amal A. 2000. Israel's Political Regime: Ethnic Democracy and the Critique of Reality. [In Hebrew.] *Israeli Sociology* 2 (2): 631–646.
- Kim, Mun-Cho. 2004. Surveillance Technology, Privacy and Social Control. *International Sociology* 19 (2): 193–213.
- Klein, Naomi. 2007. *The Shock Doctrine: The Rise of Disaster Capitalism*. New York: Metropolitan Books.
- Kokolakis, Spyros. 2017. Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Computers & Security* 64: 122–134.
- Komam, Nir. 2020. A Poll: How Much the Public Believes That the Shin Bet Contact-Tracing Support the Struggle Against the Coronavirus. [In Hebrew.] *Ice*, August 30. <http://www.ice.co.il/research/news/article/785113> [accessed December 16, 2020].
- Lee, Jin-Myong, and Jong-Youn Rha. 2016. Personalization-Privacy Paradox and Consumer Conflict with the Use of Location-Based Mobile Commerce. *Computers in Human Behavior* 63: 453–462.

- Lentin, Ronit. 2017. Race and Surveillance in the Settler Colony: The Case of Israeli Rule Over Palestine. *Palgrave Communications* 3: <https://doi.org/10.1057/palcomms.2017.56>.
- Leshem, Eitan. 2020. In Order to Avoid the Shin Bet Contact-Tracing Many Go Back to Using the “Dumb” Phones. [In Hebrew.] *Haaretz*, July 16. <https://www.haaretz.co.il/captain/premium-1.8998539> [accessed August 6, 2020].
- Linder, Ronny. 2020a. The Bizarre Story of Dr. Itamar Zilberman: “The Text Came Back Negative—But the Shin Bet Sent Everyone to Quarantine.” [In Hebrew.] *TheMarker*, March 22. <https://www.themarker.com/news/health/1.8698612> [accessed May 26, 2020].
- . 2020b. One of the Essential Workers for the Struggle Against the Coronavirus in Israel Was Placed in Isolation Because of the Shin Bet—And Doesn’t Understand Why. [In Hebrew.] *TheMarker*, March 24. <https://www.themarker.com/news/health/1.8705463> [accessed May 26, 2020].
- . 2020c. In Secret—The Health Ministry Recently Opened the Possibility to Appeal the Shin Bet’s Tracking Results. [In Hebrew.] *TheMarker*, April 17. <https://www.themarker.com/consumer/health/1.8776960> [accessed May 26, 2020].
- Linder, Ronny, and Refaella Goichman. 2020. “Damn Those Shin Bet Inspections. Shout Hard in Protest from Outside Because We are Breaking Down.” [In Hebrew.] *TheMarker*, July 5. <https://www.themarker.com/coronavirus/premium-1.8972215> [accessed July 7, 2020].
- Liss, Yonatan. 2020. About 60% of Appeals After Being Sent to Quarantine Based on the Shin Bet Contact Tracing Got an Approval to Exit It. [In Hebrew.] *Haaretz*, July 19. <https://www.haaretz.co.il/health/corona/premium-1.9004817> [accessed July 21, 2020].
- Lukash, Alexandra. 2020. Received a Fake Message That Her Daughter is Suspected of Being Infected in Coronavirus: “We Will Quarantine Her.” [In Hebrew.] *Ynet*, March 20. <https://www.ynet.co.il/articles/0,7340,L-5700155,00.html> [accessed May 26, 2020].
- Lyon, David. 2004. Globalizing Surveillance. *International Sociology* 19 (2): 135–149.
- Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. Berkeley, CA: University of California Press.
- Melman, Yossi. 2020. The Vulnerability of Locating Infected People: Exposure of Secret Methods and Leaks from the Ministry of Health. [In Hebrew.] *Haaretz*, March 19. <https://www.haaretz.co.il/blogs/yossimelman/BLOG-1.8690799> [accessed May 26, 2020].
- Murakami Wood, David. 2009. The “Surveillance Society.” *European Journal of Criminology* 6 (2): 179–194.
- Murakami Wood, David, Kirstie Ball, David Lyon, Clive Norris, and Charles Raab. 2006. *A Report on the Surveillance Society*. London: Surveillance Studies Network.
- Natour, Rajaa. 2020. No Democratic Country Used Its Secret Service in Its Struggle Against the Pandemic. [In Hebrew.] *Haaretz*, May 13. <https://www.haaretz.co.il/misc/article-print-page/MAGAZINE-1.8842363> [accessed June 2, 2020].
- Nelkin, Dorothy, and Lori Andrews. 1999. DNA Identification and Surveillance Creep. *Sociology of Health & Illness* 21 (5): 689–706.
- Norris, Clive. 2003. From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control. In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by David Lyon, 249–281. London: Routledge.
- Orwell, George. 1949. 1984. London: Harcourt Brace Jovanovich.
- Pascovich, Eyal. 2015. Not Above the Law: Shin Bet’s (Israel Security Agency) Democratization and Legalization Process. *Journal of Intelligence History* 14 (1): 54–69.
- . 2017. Shin Bet and the Challenge of Right-Wing Political Extremism in Israel. *International Journal of Intelligence and CounterIntelligence* 30 (2): 269–309.
- Pedahzur, Ami. 2009. *The Israeli Secret Services and the Struggle Against Terrorism*. New York: Columbia University Press.
- Pentina, Iryna, Lixuan Zhang, Hatem Bata, and Ying Chen. 2016. Exploring Privacy Paradox in Information-Sensitive Mobile App Adoption: A Cross-Cultural Comparison. *Computers in Human Behavior* 65: 409–419.
- Public Committee Against Torture in Israel, The. 2020. *Torture in Israel 2020: An Overview*. [In Hebrew.] Jerusalem, IL: The Public Committee against Torture in Israel.
- Romele, Alberto, Francesco Gallino, Camilla Emmenegger, and Daniele Gorgone. 2017. Panopticism is Not Enough: Social Media as Technologies of Voluntary Servitude. *Surveillance & Society* 15 (2): 204–221.
- Rubinstein, Roy. 2020. People Who Were Sent to Quarantine are Claiming False Detection: “It’s Frustrating, Everything is Messed Up.” [In Hebrew.] *Ynet*, July 5. <https://www.ynet.co.il/article/HJ2QQqy1P> [accessed July 7, 2020].
- Schwartz Altschuler, Tehilla, and Hagai Levine. 2020. Members of Israel’s Government—We Told You So! [In Hebrew.] *Haaretz*, July 21. <https://www.haaretz.co.il/opinions/premium-1.9009695> [accessed December 24, 2020].
- Shafir, Gershon, and Yoav Peled. 2002. *Being Israeli: The Dynamics of Multiple Citizenship*. Cambridge, UK: Cambridge University Press.
- Sheff, Leon. 2002. The Necessity of Defense of the Truth: On the Tortuous Deliberations about the Use of Torture. [In Hebrew.] *Bar-Ilan Law Studies* 17 (2): 459–493.
- Smootha, Sammy. 2000. The State of Israel’s Regime: A Civil Democracy, a Non-Democracy, or an Ethnic Democracy? [In Hebrew.] *Israeli Sociology* 2 (2): 565–623.
- . 2010. Israel Society: Like Other Societies or Exceptional Case? [In Hebrew.] *Israeli Sociology* 11 (2): 297–302.
- Snowden, Edward. 2019. *Permanent Record*. London: Pan Macmillan.
- Sokol, Sam. 2020. I Wasted 2 Days Holed Up in My Bedroom Thanks to Buggy Health Ministry Virus App. *Times of Israel*, April 27. <https://www.timesofisrael.com/i-wasted-2-days-holed-up-in-my-bedroom-thanks-to-buggy-health-ministry-virus-app/> [accessed May 27, 2020].
- Speak, Suzanne, and Stephen Graham. 1999. Service Not Included: Private Services Restructuring, Neighbourhoods, and Social Marginalisation. *Environment and Planning A* 31 (11): 1985–2001.

- Starr, Amory, Luis A. Fernandez, Randall Amster, Lesley J. Wood, and Manuel J. Caro. 2008. The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis. *Qualitative Sociology* 31 (3): 251–270.
- State Comptroller of Israel. 2000. *A Summary of a Report on the Investigation System in the Israeli Security Agency (Shin Bet) for the Years 1988-1992*. [In Hebrew.] Jerusalem, IL: State Comptroller of Israel.
- . 2020. *A Special Interim Report on the Topic of Israel's Coping with the Corona Crisis*. [In Hebrew.] Jerusalem, IL: State Comptroller of Israel.
- Taddicken, Monika. 2014. The “Privacy Paradox” in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication* 19 (2): 248–273.
- Yablonko, Yasmin. 2020. Not on Par with Europe's Pace: Why the Outdated Israeli Privacy Legislation Can Harm Its Economy. [In Hebrew.] *Globes*, July 20. <https://www.globes.co.il/news/article.aspx?did=1001336550> [accessed December 24, 2020].
- Yakir, Dan. 2018. No More “Administrative Mistakes”! Association for Civil Rights in Israel, August 17. https://www.english.acri.org.il/post/_24 [accessed June 18, 2020].
- Yanko, Adir. 2020a. Scarce Personnel, Impassable Conditions and Faulty Training: Epidemiological Investigations are on the Brink of Collapse. [In Hebrew.] *Ynet*, June 30. <https://www.ynet.co.il/articles/0,7340,L-5756712,00.html> [accessed June 30, 2020].
- . 2020b. The Calendar Was Exposed: A Meeting of Shin Bet Representatives with the Director of the Ministry of Education about Arab Students. [In Hebrew.] *Ynet*, February 13. <https://www.ynet.co.il/articles/0,7340,L-5676612,00.html> [accessed July 23, 2020].
- Yanko, Adir, Tova Zimuki, Itamar Eichner, and Gilad Morag. 2020. A Greater Number of Uninstalls Than of Installs: The “Hamagen 2” Campaign Was Stopped. [In Hebrew.] *Ynet*, August 9. <https://www.ynet.co.il/article/SJqLkKh11D> [accessed August 10, 2020].
- Yasur, Beit-Or, Maytal. 2020. The Shin Bet Tracked Half of the People Contracted in the Second Wave. [In Hebrew.] *Israel Hayom*, September 17. <https://www.israelhayom.co.il/article/802259> [accessed December 15, 2020].
- Yiftachel, Oren. 1999. Ethnocracy: The Politics of Judaizing Israel/Palestine. *Constellations* 6 (3): 364–390.
- Yuchtman-Yaar, Ephraim, and Tamar Hermann. 2016. *Peace Index—December 2015*. Jerusalem, IL: The Israel Democracy Institute.
- Zaken, Danny. 2020. Eli Cohen: The Shin Bet Contact-Tracing Will Be Terminated by January 21. [In Hebrew.] *Globes*, December 16. <https://www.globes.co.il/news/article.aspx?did=1001353436> [accessed December 28, 2020].
- Zamir, Yitzhak. 2019. *The Bus 300 Affair*. [In Hebrew.] Jerusalem, IL: Israel's Ministry of Justice.
- Zazim Community Action. 2020. Our Privacy is in Danger (Online Petition). [In Hebrew.] https://act.zazim.org.il/petition/stop_corona_surveillance_he [accessed July 17, 2020].

Interviews and Correspondences

- Afek, Rachel (activist, Machsom Watch). 2019. Interview by the author. Telephone interview. September 12.
- Bar, Shuli (activist, Machsom Watch; supervisor of the website's content aspects). 2017. Interview by the author. Telephone interview. November 16.
- Barag, Hanna (activist, Machsom Watch and Yesh Din). 2017. Interview by the author. Personal interview. Jerusalem, IL, November 14.
- Doe, John (former B'Tselem employee; anonymity maintained). 2017. Interview by the author. Personal interview. Tel-Aviv, IL, November 15.
- Dukhi, Khaled (labor law attorney; head of the Palestinian Workers Project at Kav LaOved). 2017. Interview by the author. Personal interview. Tel-Aviv, IL, November 15.
- Gvanyahu, Avner (director of Breaking the Silence). 2019. Interview by the author. Telephone interview. September 23. Jabareen, Hassan (director and founder of Adalah). 2020. Interview by the author. Telephone interview. July 15.
- Konforty, Aviva (activist, Machsom Watch; supervisor of the website's technical aspects). 2017. Interview by the author. Telephone interview. November 22.
- Maor, Idit (activist, Machsom Watch). 2019. Interview by the author. Telephone interview. September 16.
- Montell, Jessica (director of HaMoked: Center for the Defence of the Individual). 2019. Interview by the author. Telephone interview. September 12.
- Smith, John (former B'Tselem employee; anonymity maintained). 2017. Interview by the author. Personal interview. Tel-Aviv, IL, November 28.
- Stroumsa, Rachel (director of The Public Committee against Torture in Israel). 2020. Interview by the author. Telephone interview. July 9.
- Yellin, Roy (Director of Public Outreach at B'Tselem). 2020. Email correspondence with the author. June 24.
- Zohar, Hanna (former director of Kav LaOved; activist, Machsom Watch). 2017. Interview by the author. Personal interview. Tel-Aviv, IL, November 8.

Laws, Legal Documents, and Court Cases

- Foundations of Law*. 1980.
- General Security Agency Act 2002, The*. [In Hebrew]

HCJ 2109/20. *Shachar Ben-Meir v. Prime Minister* (Supreme Court 2020).
HCJ 4762/20. *The Association for Civil Rights in Israel v. The Knesset* (Supreme Court 2020).
HCJ 5100/94. *The Public Committee Against Torture in Israel v. Government of Israel* (Supreme Court 1999).
HCJ 5277/13. *The Association for Civil Rights in Israel v. Israel's Security Agency* (Supreme Court 2017).
HCJ 6732/20. *The Association for Civil Rights in Israel v. The Knesset* (Supreme Court 2020).
HCJ 8193/04. *Union of Parents of Arab Students in Israel v. The Ministry of Education* (Supreme Court 2004).
Israel as the Nation-State of the Jewish People. [In Hebrew.] 2018.
Israeli Citizenship Law. [In Hebrew.] 1952.
Law of Return. [In Hebrew.] 1950.