International Journal of Communication 19(2025), 287–305 1932–8036/20250005

Privacy Activism: (Anti-)Surveillance Discourse in Pandemic Days

TAMAR ASHURI[1]
Tel-Aviv University, Israel

The current trend in which data-driven surveillance technologies are being appropriated by both commercial entities and state arms flies in the face of individuals' "right to privacy." This tendency gained momentum with the spread of coronavirus, when, in an effort to monitor the spread of the virus, governments authorized the deployment of surveillance tools and devices. In response to a growing body of research that overwhelmingly focuses on powerful entities that surveille individuals, this study emphasizes the agency of those being surveilled. It does so by analyzing the organic (anti-)surveillance discourse in Hebrew created and reflected on Facebook during COVID-19 days. The discourse is scrutinized through the analytical lens of 2 major approaches to privacy: the liberal-individualist and the social (Arendtian) frameworks. The analysis of the speech acts unveils people's perceptions about privacy and how they interpreted the impacts of surveillance measures on both individuals and society.

Keywords: privacy, surveillance, data-driven technologies, coronavirus (COVID-19), activism, protests, Facebook

The current tendency in which data-driven surveillance tools and devices are being appropriated by both commercial entities and state arms flies in the face of individuals' "right to privacy" (e.g., Cohen, 2013; Marwick, 2023; Turow, 2021). The controversy came to a head during the COVID-19 pandemic, when, in an effort to monitor the spread of the virus, governments authorized the deployment of novel networked technologies, which directly affected people's ability to control how data and information about them flow (e.g., Ferretti et al., 2020; Harari, 2020). Two technical approaches have dominated the deployment and rushed adoption (Newlands et al., 2020) of contact tracing technologies: GPS methods of colocalization tracing and Bluetooth-based methods of proximity tracing (Leslie, 2020; Madianou, 2020). The utilization of such surveillance tools and devices exposes citizens' powerlessness to command how their personal data and information spread through networks that they can never fully control. As Marwick (2023) recently observed, the surveillance (networked) technologies that states enact are the most invisible and powerful.

Tamar Ashuri: tashuri@tauex.tau.ac.il
Date submitted: 2023-09-01

[1] I wish to thank Yarden Sher for her contribution.

With the global spread of COVID-19 in March 2020, the Israeli government also resorted to tracking technologies. Yet, in contrast to liberal democracies—like those mentioned above—it decided to take an unprecedented step: to use digital surveillance technologies developed by the General Security Services (GSS) as tools to tackle coronavirus. Under orders of the Israeli prime minister, representatives of the GSS were required to identify individuals who had been in close proximity to confirmed patients, by location data on their cell phones. Using these technologies, state representatives were able to trace (and by implication, manage) people's social connections and behaviors (Marciano, 2021).

This study investigates the organic discourse about privacy in a world saturated with social media, state and corporate surveillance, and big data, as reflected in Israel's most popular social network, Facebook. Facebook pages provide individuals and groups with a means of framing what is going on in public life and engaging the mass citizenry. Thus, posts published in this public sphere express what John Austin (1962) termed "performative utterance," meaning, using words as a means of "doing things." According to this logic, those who write the posts, by doing so, do more than merely convey information: They act to perform a certain social function or enact an action through the act of posting itself. In the case examined here of (anti-)surveillance discourse, the "performative utterance" concept takes on a significant role as writers use language not only to communicate ideas but also to enact social change or signal alignment with a cause.

The motivation for investigating the organic (anti-)surveillance discourse in the Israeli context extends beyond the specifics of Israel. These discussions provide insight into how people feel about privacy issues, such as data breaches or the use of surveillance mechanisms during the pandemic, without the constraints of formal surveys or academic experiments and allow identification of critical moments in the evolution of privacy rights, and better understand how these movements influence broader societal norms and legal frameworks.

Theoretical Framework: Two Major Approaches to Privacy

The discourse about privacy in a world saturated with social media and state and corporate surveillance is investigated through the analytical lenses of two major approaches to privacy embedded in modern liberal thought.

The first approach to privacy—often called the "liberal-individualist tradition" (see discussion in Cohen, 2013; Solove, 2010)—focuses on the role of privacy in the lives of individuals. It involves both the conventional understanding of the individual (or self) that privacy is thought to protect, and the criteria that the defensible right to privacy ought to satisfy. This approach, which is rooted in Warren and Brandeis's (1890) influential definition of privacy as the right to be let alone is based on the conception of the individual as inherently autonomous. In its ideal form, the liberal self is capable of rational deliberation and of making rational choices independent of external influences. Privacy is thus understood as a necessary practice to forge subjectivities of self-determination. Importantly, the liberal-individualist approach to privacy, as per Warren and Brandeis's (1890) definition above, is strongly linked to the materiality and sociotechnology that emerged in an early bourgeois societal setting: Warren and Brandeis's (1890) legal endeavors were motivated by the development of instantaneous photography and the commercial yellow press.

A major argument set forth today by supporters of the liberal-individualist approach is that privacy preserves a space around a fully formed individual, protecting him or her from the negative influence of antidemocratic regimens in the surrounding cultural, economic, and technological contexts. These scholars claim that self-development requires a private space in which one can try out things and commit mistakes without too many detrimental consequences (Rössler, 2005). This conception is tightly related to scholarship in the social sciences concerned with identity management in which people are perceived as playing various roles in different social settings and contexts (see e.g., Goffman, 1959). These critics argue that a space protected from the influence of others through privacy facilitates the formation of self-identity, as it enables the autonomous individual to determine the information to be disclosed in any one context.

Such perceptions find reflection in legal studies, with scholars conceiving privacy as a mechanism that regulates public and private spaces. A notable proponent in this area is Gavison (1980), who suggests that the common denominator of privacy in all definitions is limited access to the individual:

> Our interest in privacy . . . is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. (p. 423).

In line with the liberal-individualist tradition about privacy, Gavison's (1980) definition of access to the individual agent restricts privacy to matters of withdrawal (solitude) and concealment (secrecy, anonymity).

Although the principles of the liberal-individualist tradition were articulated before the emergence of data-driven surveillance technologies, they still hold today, with scholars arguing that unrestricted access to one's private space by means of surveillance (digital) technologies jeopardizes individual autonomy, and by implication, threatens psychological well-being, subjectivity, self-development, and more.

Whereas the above-described liberal tradition stresses the importance of privacy for individualism, another approach focuses on its centrality for society. This line of argument is often associated with Arendt (1998), whose original conceptions of privacy serve as pillars for this agenda. For Arendt (1998), plurality is a key feature of humanism: People are human together, never alone. When people come together in a sphere that is public, the discourse resulting from this convergence establishes the possibility of freedom, which is necessary for the evolvement of politics—which Arendt saw as the highest form of human activity. According to Ardent, freedom is the possibility for one to change one's appearance through exposure to, and engagement with, plural perspectives. Arendt stresses that freedom is realized in public settings. That is, when people engage with others (in a public sphere), they generate conversations and, through exchange of ideas, create a common world and a shared understanding of that world. Yet, Arendt makes it clear that a public sphere—where politics occurs—depends on the existence of a private sphere where individuals are free from politics insofar as they hide themselves from others. Referring manly to the household as the ultimate private sphere, Arendt (1998) notes: "[We] return back from the outside world and withdraw into the security of private life within four walls . . . [that] enclose a secure place, without which no living thing can thrive" (p. 186). According to Arendt (and her many followers), privacy protects the plurality of standpoints in society and thus the possibility for subjects to change, to become someone else, and to create something new in the world.

State Surveillance During the Coronavirus (COVID-19) Period

The pandemic provided a unique context in which state surveillance practices expanded rapidly, raising critical questions about their effectiveness, ethical implications, and potential long-term impacts (e.g., Afroogh et al., 2022; French & Monahan, 2020).

Noting the unprecedented expansion of digital surveillance technologies, many highlighted how states used the pandemic to exert greater control over populations, leveraging public health as a rationale for increased surveillance (e.g., Kitchin, 2020). Studies demonstrated that the pandemic emphasized the datafication of health, where personal health information became a valuable resource for governments and companies. COVID-19, the argument goes, accelerated the normalization of surveillance, with practices that might have been considered intrusive before the pandemic becoming more widely accepted (e.g., Leslie, 2020; Lucivero et al., 2022; Lyon, 2021).

Scholars also raised concerns about the ways in which pandemic surveillance threatened individual privacy, arguing that the balance between public health and civil liberties tilted too far in favor of state control (Harari, 2020). Some scholars also criticized the reliance on surveillance, suggesting that resources might have been better spent on more traditional public health measures, such as testing, contact tracing by human agents, and public education (e.g., Gostin, Moon, & Meier, 2020).

Many studies about surveillance during COVID-19 examined public attitudes toward state surveillance during the pandemic (and how it evolved). Findings show that in some Asian countries, where collectivist values are more prevalent and there is a higher level of trust in government, surveillance measures were more widely accepted. Leung, Wu, and Leung (2021), for example, found that countries like South Korea and Taiwan, which had previous experiences with epidemics, saw higher public compliance and less resistance to surveillance. In contrast, in Western countries where individual privacy is highly valued, there was more resistance and debate about the balance between public health and personal freedoms). Studies conducted in the Global South found that attitudes were shaped by both trust in local governments and the level of technological infrastructure available (Zhou, Su, & Su, 2021). Studies show also that the urgency of the pandemic led to a significant shift in public acceptance of surveillance technologies, which were previously seen as invasive but became normalized under the guise of public health (Fuchs, 2021; Lyon, 2021; Newlands et al., 2020).

Surveillance in Israel During the Coronavirus (COVID-19) Period—Making Use of the Security Forces

As mentioned, with the global spread of the pandemic, the Israeli government also resorted to tracking technologies. Yet, in contrast to liberal democracies, it decided to take an unprecedented step: to use digital surveillance technologies developed by the General Security Services (GSS) as tools to tackle coronavirus. The government's unprecedented step to demand that the security forces surveil all the country's citizens was enabled by virtue of the General Security Service Law, 5762–2002, which lays out the activity of the GSS of Israel. The law empowers the GSS "to receive and gather information" among other means, by receiving communication data from the cellphone companies. A permanent supplementary

directive to the Communications Law (Bezeq and Broadcasting 5742–1982), obligates the telecommunications companies to help the GSS and pass on data in accordance with its request. At the same time, the Secret Monitoring Law, 5739–1979, sets down the secret monitoring that the GSS is authorized to carry out. This combination serves as the legal basis for the GSS operating the digital surveillance technologies, known as the "Tool."

The "Tool" enables any person to be tracked by location data of their cellphone. Intensive use of the Tool over time created (and continues to create) an impressive intelligence database for the GSS and the government. Until the coronavirus crisis, (as far as is known) such usage by the GSS was limited to security needs—identifying terrorists and thwarting terror attacks.

On March 17, 2020, the government instituted regulations that authorized the GSS to receive, collect, and process "technological data" so as to identify the location and movements of persons who had contracted coronavirus and those with whom they had been in contact. The authorization was extremely broad—the stated purpose was fast, effective, and the exact location of the contacts, and self-quarantine for the sick and potentially sick. The regulations for the GSS's operation were defined by the government as "Emergency Regulations," which allowed their implementation without the knowledge or authority of the members of the Israeli parliament.

On March 27, 2020, journalists Ronen Bergman and Ido Shvartztuch, in an investigative report to the popular newspaper *Yedioth Ahronoth*, exposed the characteristics of the surveillance Tool used by the GSS. The journalists also revealed that this Tool had already been in use for many years by the GSS and that the security forces methodically gather and collect data about all Israeli citizens. At the same time, the GSS's working methods and technologies were revealed to the public.

Following the exposure of the GSS surveillance—both by people in the government and also by journalists—several petitions were made to the High Court of Justice, in which it was argued that, by implementing these emergency regulations (which authorize the GSS to track contacts), the government had exceeded its authority, resulting in a severe infringement on the right to privacy and to human dignity, and that the regulations were therefore unconstitutional. The petitions were also against government monitoring of those requiring self-quarantine, which had been made possible because of data from the cellphone companies (Kan Hadashot, 2020). Following the petitions, on March 19, the High Court of Justice authorized the use of the Tool for several days, with an interim order, but demanded authorization by the Knesset (Israeli parliament). After a designated committee was established in the Knesset, the judicial permit was extended by several days. On March 24, in light of the court's remarks and following the swearing-in of the 23rd Knesset, the new government decided to obtain the Knesset's authorization for implementing the GSS surveillance.

Once the new Knesset was sworn in, the Knesset Subcommittee for Secret Services held several discussions, culminating on March 31, 2020, with the Knesset authorizing GSS surveillance for all residents, by tracking their cellphones. Consequently, the petitions that had been filed against the new government's resolution were amended. On April 16, a hearing was held in the High Court of Justice about the GSS's authority to track citizens (HCJ 2109/20 Ben Meir vs. Prime Minister). On April 26, the High Court of Justice

determined that the government is permitted to grant authority to the GSS to also operate in areas not concerning state security in its narrow sense (a security context). However, it made the continued help from the GSS conditional on the decision being anchored in primary legislation, leaving the continued authority in place for several days, conditional on the government advancing a formal legislative process. The court decided the authority was justified in exceptional cases in which there exists "a severe and immediate danger to the citizens and residents of the state"—a danger that was determined did indeed exist at the time of the verdict, but it was emphasized that the authorization must be reexamined.

Concurrent with the verdict and after a general lockdown had been imposed on all residents, a significant drop was documented in the number of persons infected with coronavirus. On May 3, the Privacy Protection Authority in the Ministry of Justice published a position paper which forcefully opposed the continued usage of the GSS and the technology which it had developed, arguing that "[the Tool] is unjustified at the present time, unreasonable, exceptional and not proportional" (Privacy Protection Authority, 2020, p. 1), and called to turn to alternatives with less damage to privacy.

Despite this, in May 2020, the government extended the surveillance authority given to the GSS and published a law memorandum on the subject. Thus, the government announced that it had begun the process of advancing a law on the issue.

Toward the end of June, there was a sharp increase in the number of people diagnosed with coronavirus. Even though the head of the GSS was opposed to using the GSS, the Israeli government advanced a designated law that permitted GSS surveillance for a period of three weeks. On July 1, a temporary law was passed. Concurrently, the Knesset discussed a permanent law about this issue. The law, named the Authorization of the General Security Service to Assist the National Effort to Reduce the Spread of the Novel Coronavirus (Amendment) 5780–2020, determined a line of arrangements relating to the continued GSS authorization to use the surveillance Tool for six months.

History of State Surveillance in Israel

From its early years, Israeli surveillance practices have evolved significantly, shaped by the ambition to address (perceived) external threats and internal dissent. Military and intelligence agencies, such as Mossad (external intelligence), GSS (internal security), and Aman (military intelligence), focused on gathering intelligence on neighboring countries, Palestinian organizations, and potential threats—surveillance policies that Handel and Dayan (2017) named "normalizing surveillance." The 1970s also saw the beginning of Israel's investment in technological advancements for surveillance, including signals intelligence (SIGINT) and early forms of electronic monitoring. The 1980s were characterized by Israel's continued focus on security, particularly in the context of its occupation of the West Bank and Gaza following the 1967 Six-Day War. After the war, Israel implemented extensive surveillance systems in the occupied Palestinian territories. Israel's Unit 8200, an elite military intelligence unit specializing in SIGINT, became increasingly influential. Unit 8200 intercepted communications from adversaries, and its role expanded significantly during this period, laying the groundwork for Israel's reputation as a global leader in cyber and electronic intelligence. The 1990s marked a shift toward digital surveillance, coinciding with the rise of the Internet and the First Intifada. With the advent of networked technologies, Israeli intelligence agencies

began developing more sophisticated methods for monitoring communications. During the 1990s, there was also increased surveillance of Israeli citizens, particularly those involved in left-wing activism, protests against the occupation, and opposition to the peace process. This included monitoring political organizations and activists within Israel (e.g., Zureik, Lyon, & Abu-Laban, 2010). The Second Intifada led to a significant escalation in Israeli surveillance of Palestinians. Israel deployed drones, biometric systems, and advanced data analytics to monitor Palestinian movements and communications. Thus, Palestinians were not deported, but as Handel and Dayan (2017) observed, "The rug is pulled from under their feet, leaving them within the controlled territory, yet excluded and with less and less rights" (p. 4). Throughout the 2020s, Israel continued to expand its surveillance capabilities, incorporating AI, facial recognition, and big data analytics. Israeli companies became renowned (and controversial) for developing sophisticated "zero click" spyware like Pegasus, which were used to infiltrate smartphones. These technologies were used for both counterterrorism and monitoring internal dissent, sparking ongoing debates about their impact on democracy and human rights.

Although surveillance measures have been central to Israel's security strategy, they have also raised significant concerns about civil liberties, the potential for abuse, and the impact on both Israeli and Palestinian societies. The balance between security and privacy remains a contentious issue, with ongoing debates about the role of surveillance in a democratic society (e.g., Birnhack & Zar, 2020; Handel & Dayan, 2017; Zureik et al., 2010).

The "Right to Privacy" in Israeli Law

The decision made by the Israeli movement to use GSS's surveillance tools during the COVID-19 pandemic infringes the right to privacy according to Israeli law (see e.g., Birnhack, 2020). Privacy, as a legal right in Israeli law, operates on three planes: between people, between a person (consumer) and a corporation, and between a person (citizen) and the state. What is common to all is the recognition that a person has the right to decide which information (if any) about him or her will be conveyed, to whom, the manner in which it will be conveyed, when, and under what conditions. Technologies to locate contact are based on enforced collection of information about citizens, and thereby using them encroaches on the right to privacy.

Israel's approach to privacy has been shaped by its unique history and security challenges. Founded in 1948 as a democracy with strong liberal foundations, the state was built to safeguard individual rights, including privacy. However, Israeli society reflects a blend of collectivist and individualist tendencies that influence attitudes toward privacy. On one hand, Israel's social fabric is deeply communal, with values of solidarity and collective responsibility often taking precedence, particularly during security crises. This collectivist orientation can sometimes make privacy concerns secondary to national interests or communal safety. On the other hand, Israel's liberal democratic framework emphasizes individual rights, including the right to privacy. Tensions between these two aspects are especially evident in areas where privacy is restricted because of military considerations, state surveillance, and counterterrorism measures.

Despite these tensions, Israeli law considers the right to privacy one of the most fundamental human rights. The right to privacy was already recognized in Israeli court rulings during the 1970s. In 1981,

it merited its own legislation in the form of the Protection of Privacy Law, and in 1992, it received constitutional status after having been anchored in the Basic Law: Human Dignity and Liberty.

The government surveillance policy in winter 2020, particularly the long-term authority given to the GSS to track all residents, is not commensurate with the legislation intended to protect the privacy of the state's residents. First, the GSS was authorized to receive medical information from the Ministry of Health and track the cellphones of people identified by the Ministry of Health as potentially or actually sick with coronavirus. Collecting the information and passing it on infringed on the right to privacy about medical information. This argument is based on the legislation about medical information, which is protected in Israel as part of the right to privacy in the Basic Law: Human Dignity and Liberty. Medical information is also arranged in the Protection of Privacy Law, 5741–1981, which defines health information as "sensitive information." The privacy of sick persons' medical information is also protected by the Patients' Rights Law, 5756–1996, which determines that those treating patients must respect the privacy and the obligation of secrecy. Evidence laws also determine immunity for medical information. There are also specific laws and regulations about additional aspects of secrecy of medical information. With pandemics, the right to privacy for medical information is not absolute. Particularly relevant in this context is the public health ordinance of 1940, which specifically refers to infectious diseases. This ordinance obligates notifying the Ministry of Health about a person having an infectious disease; meaning that, in these special cases, it is permitted to pass on information about a sick person to the health authorities.

Second, in the coronavirus context, the GSS was authorized to harvest individuals' location data and submit that information to the state authorities. Additionally, the police were authorized to receive cellphone data for purposes of enforcement and of monitoring those requiring self-quarantine. Privacy relating to information about location, or protection of data about location, are not noted as private information in the Basic Law or the Protection of Privacy Law, but emerge from Israeli legislation about communications data and from court decisions in these contexts (Birnhack, 2020; Birnhack & Zar, 2020). Data about place can be included as one of the definitions of "information" protected in the Protection of Privacy Law.

Third, during the coronavirus period, the GSS was required to gather and pass on information about individuals' connections and social meetings. The Basic Law and the Protection of Privacy Law do not openly refer to information about connections and social meetings. The only such mention is with reference to journalists and addressing the conditions in which the identity of parties in a conversation can reveal a journalistic source. However, as Birnhack (2020) showed, there is evidence that this information is protected by Israeli law, primarily as concerns the content of the conversation or communication, as opposed to details of the actual communication process—but the distinction between the two is unclear. Thus, for example, the identity of the parties to a conversation can reveal their social and interpersonal relationships, and thus testify or hint to the content of the conversation. Therefore, even though the details of the interactions and identity of those holding the discourse are seen as "less private" than the content of the conversation, they are personal information nonetheless, and as such is protected by privacy laws; and when the state authorities gather and/or use them, it is considered an infringement of personal information, ostensibly protected by law.

Thus far, no study has explored public attitudes toward privacy during the coronavirus outbreak, a period in which exceptional actions germane to privacy were taken that do not conform to Israeli law. The current study examines organic public discourse created and reflected on Facebook about exceptional actions carried out with surveillance technologies during the health crisis.

Methodology

With a view to characterizing organic public discourse on issues salient to activating the GSS tracking during the coronavirus period, posts written in Hebrew by Facebook users were analyzed. The primary purpose was to identify the resistance discourse to surveillance and infringement of privacy. Facebook was chosen as the largest social network in Israel, with 6 million registered users (approximately 75% of the population).

The analyzed posts were written from March 14, 2020—when the Israeli prime minister announced his intention to use the GSS services to track citizens so as to wipe out the virus and the beginning of the first national lockdown (the start of what was termed the "first wave" of COVID-19 in Israel)—until September 21, 2020, the height of the "second wave" and the return to a national lockdown.

The texts (posts) were selected by means of a search engine developed by Buzzilla—an Israeli company that combs Internet sites using keywords. The words used in this study are connected with the semantic field targeted—surveillance during the coronavirus period. Thus, the words searched for were "coronavirus" (including "COVID-19, COVID19, coronavirus, corona") and the different forms of one or more of the following words: "surveillance, listening, GSS, privacy, telephones (including cellphones)" and "police" (including "police officers, enforcement," and "Israel police").

In accordance with legal restrictions, Buzzilla does not scan posts on private profiles, and therefore all posts examined in this article were published in Facebook groups. Since some of these Facebook groups are open and public, whereas others are private, the researchers joined the groups (by sending a request to join and being approved by the group administrators). To preserve the posters' privacy, their personal details were not revealed.

The search was divided into four time periods during which the posts were published, two during the "first wave" of coronavirus and two during the "second wave": Period 1—the declaration that digital means would be used to track citizens as a way of dealing with coronavirus and the beginning of the first national lockdown (March 14–20); Period 2—the High Court of Justice deliberates on the legality of the state tracking its citizens and harm to the right to privacy, and that was broadcast live for the first time (April 16–22); Period 3—the beginning of the second wave, with a rise in morbidity that leads to reinstating the GSS tracking and strengthening the directives (June 22–July 4), and Period 4—the height of the second wave, returning to a general national lockdown and stringent restrictions during the period of the Jewish high holidays (September 15–21).

After removing posts that were repeated, completely irrelevant to the topic of the research, or those posted by organizations rather than individuals (such as posts published by news organizations), 122

posts were analyzed. Thus, the corpus includes all posts that are related to forced surveillance in the context of COVID-19.

The analysis of organic discourse on surveillance in Israel during the COVID-19 pandemic offers a valuable opportunity to deepen our understanding of how the individuals contributing to this discourse conceptualize privacy and how they assess the fundamental values that privacy safeguards—values that are essential for the functioning of a democratic and healthy society.

Findings

Resistance to State Surveillance: The Liberal-Individualist Tradition

On March 17, several days after the announcement of state-imposed surveillance, A.A. uploaded to Facebook the following post:

> I am not willing to allow a GSS member who is suspicious about his wife to be able to track her unlimitedly. I am not willing that the government should know where I was, when I pooped, and who I was horny with. (personal communication, March 17, 2020)

This short post, which grotesquely describes forced state surveillance, is a clear manifestation of privacy conventions rooted in the liberal-individualist tradition discussed above. One of the hallmarks of this discourse is the use of first-person singular pronouns, which appear five times in these three sentences. The word "I" refers to the individual and grammatically places him or her at the forefront of the proposition. By using the first-person mode and detailing intimate personal information that hypothetically might be publicized under the new rules, the author makes it clear that state-imposed surveillance victimizes first and foremost the individual who is the subject of such tracking. This conception—highlighted in the growing body of literature on state surveillance during COVID-19 (e.g., Harari, 2020; Kitchin, 2020)—derives from the liberal-individualist approach to privacy, which underscores the importance of privacy for the individual's well-being, and by implication the harms that may result from violation of privacy (see discussion in Solove, 2010).

The post invokes another important convention that aligns with liberal individualism: emphasis on individuals' free will and their rights to exercise it. This echoes the argument expressed in the literature on state surveillance (particularly during COVID-19 days) that although it is sometimes necessary to reconcile conflicts between privacy and security, privacy protections remain necessary to protect freedom against the power of the state. In the words of Neil Richards (2022): "In fact, not only does mass surveillance make us less free, but it can actually make us less safe as well" (p. 7). The author opens the post with a declaration: "I am *not willing* to allow a GSS member who is suspicious about his wife to be able to track her unlimitedly" (Richards, 2022, p. 7; emphasis added). This statement manifests a convention deeply embedded in the liberal-individualist tradition, whereby it is the individual who should (and can) decide who gets access to information about him or her, and under what terms. This echoes Gavison's (1980) idea of one's right to control access to one's personal information. According to Gavison (1980), the right to privacy first and

foremost entails that every person is able to limit other people's access to them—to information about them, their consciences, and their bodies.

This view about one's right to control access to one's person is also expressed in a short text posted by Y.R. on June 25, in opposition to forced surveillance: "We need to say 'no' to forced surveillance. People who want to be tracked should download a voluntary app" (personal communication, June 25, 2020).

This post also highlights the notion of the individual's free will by suggesting that one should be able to choose whether one wishes to be surveilled by the state. This author does not condemn state surveillance in the context of coronavirus, but—in accordance with liberal individualism—suggests that individuals (i.e., the subjects of state surveillance) should have the liberty to either allow or forbid this practice for themselves. This aligns with the critiques put forth by scholars who have demonstrated that the rapid deployment of surveillance technologies during the pandemic often occurred without adequate oversight, transparency, or clear guidelines about data usage and storage (e.g., Lucivero et al., 2022).

This claim is also voiced in a post written by A.A. on September 9: "In a normal world, without foreign considerations, there would not have been brutal force but rather freedom of choice" (personal communication, September 9, 2020). This viewpoint, too, is compatible with the liberal-individualist tradition. As mentioned above, a key tenet of this approach highlighted by leading scholars is the individual's right to be let alone (Warren & Brandeis, 1890). At issue is the right that first and foremost involves one's ability, if one so wishes, to isolate oneself from others and create for oneself a private and independent space free of external annoyances and harassments. The authors of the post cited above view forced surveillance—through which the state forcibly invades one's private space—as negating one's fundamental right to be let alone.

These perceptions resonate with the concept of "privacy as control" coined by legal scholar Alan Westin (1984). Westin (1984) argued that forced collection of information neutralizes one's ability to control the information in one's possession as well as information concerning one's person, and thereby harms one's right to privacy. This idea is described astutely by M.M. in a June 25 post:

> If someone would follow you in the street, go after you at every corner you turned, at the same time looking at your mobile phone, photograph what you are writing to the people closest to you, you would have already gone to the police. But what is happening now is exactly the reverse. (personal communication, June 25, 2020)

Another notable theme yielded by the analysis of the posts, and one that corresponds with liberal-individualist conventions, is the opposition to forced surveillance by the security forces. An example is A.C.'s post on June 23, which reads: "The GSS wishes to operate spying tools developed against terrorists, on citizens. To know where you [the citizens] are. So they will be able to read what you are saying and to whom" (personal communication, June 23, 2020).

The premise here is that the GSS surveillance is intended for tracking enemies of the state, and therefore recruiting this organization to track law-abiding citizens is symbolically injurious. In liberal

democracies, citizens enjoy basic rights (like the right to be let alone and to exercise control over who get access to personal information), while terrorists are not entitled to such privileges. Accordingly, forced surveillance using technology developed to combat terrorism constitutes a violation of individuals' rights that liberal countries ought to uphold (Handel & Dayan, 2017). This position is expressed in additional posts, such as the one published on July 3 by A.A.:

> Hotels [for Corona patients] have become jails. Israel has become a concentration camp. The prime minister has become a dictator. We have lost our freedom, privacy, and rights, under the cover of coronavirus. The country is in a state of emergency. The GSS tracking the citizens. Everyone has become terror suspects!!!! (personal communication, July 3, 2020)

In this case, too, the author views the tracking of citizens, carried out by an intelligence agency that uses surveillance as a tool to eliminate enemies, as an event signaling a change in the status quo: The government of a liberal democracy views citizens as its enemies and thus denies them basic individual rights (in the case in point, the right to privacy).

Related sentiments are evidenced in posts objecting to the *process* of allowing surveillance by the security forces, such as the one published on March 20 by G.B.:

> The cabinet meeting unanimously authorized digital surveillance of the country's citizens who are suspected of being "coronavirusters" or helping them. Under cover of the panic, no serious public discussion has developed on this decision and its long-term implications and the danger it embodies that in a so-called democratic state, the head of state holds the digital means of controlling the country's citizens . . . The dramatic decision to use spy technology against Israeli citizens and its implementation, has no parliamentary supervision. (personal communication, March 20, 2020)

A.A.'s March 17 post raises similar concerns: "Let them [government members] persuade a judge, and if they received a court order, then they can track me until their last breath. Otherwise—no! It bothers me how such a dramatic decision passed 'unanimously' in the government" (personal communication, March 17, 2020).

The authors whose writings are quoted here come out against the "procedure," in the sense of the way the decisions about surveillance were made. However, they clarify that the problem they are warning about is the symbolic meaning of the decision-making process. They believe the hasty decision to use the GSS and the surveillance tool it had developed to track the population in general, without the support of the legislative authority, damages the state's liberal infrastructure—meaning, it is the turning point at which a liberal democratic state turns into a dictatorship. Even if not written explicitly, it emerges from the posts that, from the authors' viewpoints, if the surveillance decision had been made in accordance with the state's laws and regulations, then no decision would have been taken to use GSS tools for surveillance, and the population's privacy would not have been breached. Thus, although the post suggests distrust in the political system, it appears to place trust in the country's legal system.

Resistance to State Surveillance: The Social (Arendtian) Approach

A theme that clearly emerged from the analysis is that state surveillance, in the manner it was carried out, jeopardizes society as a whole. In line with the Arendtian approach to privacy, the authors of some of the posts saw forced surveillance by the security forces as a practice threatening privacy, and by implication, the very fabric of the democratic state. As many current privacy scholars note: Privacy allows citizens to develop their own political beliefs free from the skewing effects of being watched, monitored, and judged (e.g., Fuchs, 2021; Lyon, 2021). An example is this post that G.D. uploaded on the site on July 2: "Our human rights are slowly (and quickly) disappearing, and it will be very difficult to get them back . . . It's true we can still demonstrate, but with GSS location data, it's easy to 'incriminate' an entire demonstration" (personal communication, July 2, 2020).

The use of the first-person plural pronoun ("our") alludes to society as a whole, which the author believes to be at risk on account of forced surveillance. The infringement of human rights, the author proceeds to explain, is tantamount to the violation of basic democratic values—values that both enable and symbolize democracy, such as the right to express personal opinions in public. This conception corresponds with Arendt's (1998) idea that privacy safeguards freedom, which is a prerequisite to politics, an enterprise that she saw as the highest form of human activity. Such concerns also arise in M.M.'s post, published on June 25:

> The government! Which is responsible, among other things, to enforce and prevent impingement on privacy, is the very same which has authorized itself to harm you. It is taking what is private, what is personal, your life, and turning it into its own legacy for purposes that who even knows what they are. Today it's COVID-19, tomorrow it's preventing demonstrations, and next year police officers will knock on your door if you write something bad about the leader. (personal communication, June 25, 2020)

The author opposes the surveillance policy on the grounds that it damages democratic values by allowing the government to restrict public gatherings (such as demonstrations) and prevent one from expressing one's opinion in public. In line with the Arendtian tradition, the author suggests that constraints enabled by forced surveillance would destroy the democratic infrastructure of the country and promote dictatorship. This claim is also echoed in the post by R.L. published on June 20: "Every day the country sinks lower and lower into a murky pit of dictatorship in the name of medicine. . . . We are the enemy. . . . The immune system (the government, police, GSS) is set against us" (personal communication, June 20, 2020).

Here too, the author mentioned long-term dangers forced surveillance poses to the entire society—a phenomenon often referred in the literature on state surveillance during COVID-19 as "surveillance creep" (Leslie, 2020; Lyon, 2021).

The use of first-person pronouns "we" and "us" clearly implies that society at large, and not only individuals, would suffer from privacy violation enacted by the State. While expressing concerns about future risks, the author aptly couches the argument in a specific context of the corona pandemic, by way of health-related metaphors: "The State of Israel has developed a severe *autoimmune disease*—the *immune* system

(the government, police, GSS)" (personal communication, June 20, 2020; emphasis added). This rhetorical strategy accentuates another salient theme that emerged from the analysis of the posts, namely that the surveillance policy does not solve the health as argued (e.g., by Harari, 2020), but rather that the health crisis serves as an excuse for imposing autocracy. An example is the post uploaded by A.H. on July 3: "How long will you continue swallowing this bluff?! Coronavirus is a false excuse, under which every atrocity is permissible." Another post, published on the same day by M.H., endorses this position: "[The surveillance is] allowed by the world discovery of the century, the fake news of 'coronavirus': an attempt to change the rulership. Legislating antidemocratic laws which negate basic rights. Power and subjugation of the people with tracking citizens" (personal communication, July 3, 2020).

The argument that the surveillance policy is a cover story for turning Israel into a dictatorship recurred in several other posts. Their authors viewed surveillance as a tool that the Israeli prime minister used to protect his status and ensure the advancement of his personal interests. Thus, for example, in a post on April 15, A.R. wrote:

> The prime minister was to have appeared in court on Tuesday . . . It begins with closing the courthouses, and continues with them sending the GSS to track you . . . We will not allow cynical exploitation of the coronavirus to shatter democracy. (personal communication, April 15, 2020)

Another example of this position is the post by Y.G., published on September 21:

> A corrupt and destructive prime minister who makes his decisions not in line with what is good for the people, but based on personal-trial interests, while identifying his personal benefit with the good of the state, and in the spirit of the famous statement by Louis XIV, "I am the state." (personal communication, September 21, 2020)

Other posts, too, claimed that the surveillance policy is a governmental tool designed to protect the government and advance the personal interests of the people at its head. The authors warned that privacy had been crushed, with long-term (and not only local) implications for the future of the state institutions and authorities. One example is D.A.'s post, published on March 18:

> We are but a hairbreadth from a human calamity whose consequences and dimensions cannot be anticipated. Just a hairbreadth from the greatest tragedy of our lives. And I am not even speaking about coronavirus. I am talking about the governmental revolution [the strengthening of right-wing parties], which is currently taking place in Israel, in the most classic manner: under cover of an "emergency situation" and while methodically and gradually silencing all the institutions. (personal communication, March 18, 2020)

The analysis of the posts in the corpus examined shows that the authors view surveillance—particularly when forcibly implemented by the security forces, and without the authorization of the legislative authority—as an infringement of the public's privacy. Following the Arendtian tradition, they underscore the political implication of state surveillance, arguing that infringements of the right to privacy on the part of the state cause long term damage to the democratic infrastructure that serves as the foundation for the State of Israel. They believe that the tracking forcibly implemented by the state and its arms abrogates their right, as citizens, to act in public and openly present their opinions, and exposes them to social or even legal sanctions. Related to that is the fear of the panopticon effect, a situation in which one knows that one is liable to be tracked but is unaware when this happens, of the reason for this measure, or of the use made of the information thus gathered. They feel the fear of being tracked prevents them and others from participating in the public arena—an activity which, according to Arendt and her many followers, is essential to democracy. Thus, for example, G.H. wrote on March 14:

> Ask yourselves, what will happen on the day all the panic will end? Will all the means of monitoring and control vanish from your lives? It's a known rule with technology that it tends to remain even after it is no longer needed.

A similar sentiment is expressed by A.A. in a post published on March 17: "Yesterday, the foundations were laid for the Fascist regime in which the secret police track citizens and attack them if they don't act 'properly' . . . that's how things start. Where will they end? I don't know" (personal communication, March 14, 2020).

Conclusions

The Israeli government's declaration authorizing forced surveillance of all the country's residents by the security forces was a sharp blow to the right to privacy in Israel (Birnhack & Zar, 2020). This battle against privacy is being waged by the right-wing antidemocratic leadership that came to power in November 2022. Accordingly, this article sets out to examine the public discourse on Facebook about forced surveillance by networked technologies developed by the GSS. To this end, the article has focused on the transformative governmental policy in the shadow of COVID-19, demonstrating public resistance to these measures, and in particular to the marshalling of the security forces to implement them. More importantly, the study has also shown that the authors of the posts view the infringement of the right to privacy resulting from the surveillance policy as long-term damage to individuals as well as to the democratic values on which the state is purportedly built on. Some even regard the surveillance policy under the cover of coronavirus to be a tool through which the Israeli government sought to establish its power and to preserve the personal interests of the person at its head.

The study thus demonstrated that privacy is perceived as a basic individual right essential to subjectivity and self-determination (as per the liberal-individualist tradition). It has likewise revealed concerns over broader citizens' rights (as per the social approach to privacy) such as the right to participate in political activities (e.g., demonstrating), to be informed (in this case, to obtain reliable information about the disease and means to combat it), and to live in a democratic state with separated powers that safeguards its citizens' basic rights, like the right to be let alone and control access to their personal information. The analysis of the corpus of Facebook posts during the coronavirus crisis period has clearly disclosed their authors' conviction that, even during a pandemic, people's ability to control how information about them flows, is a basic condition not only for individual autonomy but also for democratic participation and the creation of a public sphere.

In a broader context, the analysis of organic discourse on surveillance that was formed by privacy activists has revealed how activists, who often articulate and advocate for normative values and principles surrounding privacy, understand privacy, and why surveillance rules matter to them. By examining these conversations through the analytical lenses of two key approaches to privacy—the liberal-individualist and the social (Arendtian) frameworks—researchers are able to move beyond the traditional focus on individual privacy. This allows for greater attention to normative values and principles surrounding privacy and also tracks the evolving social and political dimensions of privacy concerns. This is crucial in shaping public opinion and influencing policy debates about privacy rights after COVID.

References

Afroogh, S., Esmalian, A., Mostafavi, A., Akbari, A., Rasoulkhani, K., Esmaeili, S., & Hajiramezanali, E. (2022). Tracing app technology: An ethical review in the COVID-19 era and directions for post-COVID-19. *Ethics and Information Technology, 24*(3), 1–15. doi:10.1007/s10676-022-09659-6

Arendt, H. (1998). *The human condition*. Chicago, IL: Chicago University Press.

Austin, J. L. (1962). *How to do things with words*. Oxford, UK: Oxford University Press.

Bergman, R., & Shvartztuch, I. (2020, March 27). Ha'cli Nechshaf [The big tool is now exposed]. *Yedioth Ahronot*. Retrieved from https://www.ynet.co.il/articles/0,7340,L-5701412,00.html

Birnhack, M. (2020). Pratiyot Be'Mashber: Handasa Chkatit VeHandasat Pratiyot [Privacy in crisis: Constitutional engineering and privacy engineering]. *24 Law and Government in Israel, 149*, 1–19. Retrieved from https://ssrn.com/abstract=3650193

Birnhack, M., & Zar, M. (2020). *Privacy in crisis: Privacy guidelines for the design of contact tracing technologies* (Work paper). Tel Aviv, Israel: Faculty of Law Tel Aviv University. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3683166

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review, 126*(7), 1904–1933.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., . . . Fraser, C. (2020). Quantifying SARS-Cov-2 transmission suggests epidemic control with digital contact tracing. *Science, 368*(6491), eabb6936. doi:10.1126/science.abb6936

French, M., & Monahan, T. (2020). Dis-ease surveillance: How might surveillance studies address COVID-19? *Surveillance & Society, 18*(1), 1–11. doi:10.24908/ss.v18i1.13985

Fuchs, C. (2021). Everyday life and everyday communication in Coronavirus capitalism. In *Communicating COVID-19* (*Society now*) (pp. 17–61). Leeds, UK: Emerald Publishing. doi:10.1108/978-1-80117-720-720211003

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal, 89*(3), 421–471.

Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Anchor Books.

Gostin, L. O., Moon, S., & Meier, B. M. (2020). Reimagining global health governance in the age of COVID-19. *American Journal of Public Health, 110*(11), 1615–1619. doi:10.2105/AJPH.2020.305933

Handel, A., & Dayan, H. (2017). Multilayered surveillance in Israel/Palestine: Dialectics of inclusive exclusion. *Surveillance & Society, 15*(3/4), 471–476. doi:10.24908/ss.v15i3/4.6643

Harari, Y. N. (2020, March 26). Ha'Magefa Mechiven Nisoiim Chasri Takdim Ve'Hem Yeshano et Haolam [The pandemic demands unprecedented social experiments—And they will change the world]. *Ha'aretz*. Retrieved from https://www.haaretz.co.il/misc/article-print-page/.premium-MAGAZINE-1.8710074

Kan Hadashot. (2020, April 16). *History at the Supreme Court: A live broadcast on the issue of the State's surveillance of citizens* [Video file]. YouTube. Retrieved from https://www.youtube.com/watch?v=DQj3SNRYGxw

Kitchin, R. (2020). 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*(3), 362–381. doi:10.1080/13562576.2020.1770587

Leung, K., Wu, J. T., & Leung, G. M. (2021). Real-time tracking and prediction of COVID-19 infection using digital proxies of population mobility and mixing. *Nature Communications, 12*(1501), 1–8. doi:10.1038/s41467-021-21776-2

Leslie, D. (2020). Tackling COVID-19 through responsible AI innovation: Five steps in the right direction. *Harvard Data Science Review*, *10*, 1–78. http://dx.doi.org/10.2139/ssrn.3652970

Lucivero, F., Marelli, L., Hangel, N., Zimmermann, B. M., Prainsack, B., Galasso, I., . . . Van Hoyweghen, I. (2022). Normative positions towards COVID-19 contact-tracing apps: Findings from a large-scale qualitative study in nine European countries. *Critical Public Health, 32*(1), 5–18. doi:10.1080/09581596.2021.1925634

Lyon, D. (2021). *Pandemic surveillance*. London, UK: John Wiley & Sons.

Madianou, M. (2020). A second-order disaster? Digital technologies during the COVID-19 pandemic. *Social Media + Society, 6*(3), 1–5. doi:10.1177/2056305120948168

Marciano, A. (2021). Israel's mass surveillance during COVID-19: A missed opportunity. *Surveillance & Society, 19*(1), 85–88. doi:10.24908/ss.v19i1.14543

Marwick, A. E. (2023). *The privacy is political: Networked privacy and social media*. New Haven, CT: Yale University Press.

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the COVID-19 pandemic. *Big Data & Society, 7*(2), 1–14. doi:10.1177/2053951720976680

The Privacy Protection Authority. (2020). Emdat Harashot Leprtiot Legagei Haasitaiut Beshirot Habitachon leitor Magaim [The Privacy Protection Authority's position regarding the assistance of the General Security Service for contact tracing]. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.il/BlobFolder/dynamiccollectorresultitem/doc_53/he/shabak_omicron_opinion.pdf

Richards, N. (2022). *Why privacy matters*. Oxford, UK: Oxford University Press.

Rössler, B. (2005). *The value of privacy*. Cambridge, UK: Polity.

Solove, D. J. (2010). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Turow, J. (2021). *The voice catchers: How marketers listen in to exploit your feelings, your privacy, and your wallet*. New Haven, CT: Yale University Press.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220. doi:10.2307/1321160

Westin, A. (1984). The origins of modern claims to privacy. In F. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 56–74). Cambridge, UK: Cambridge University Press.

Zhou, Q., Su, Z., & Su, S. (2021). Government trust in a time of crisis. *China Review, 21*(2), 87–116. Retrieved from https://www.jstor.org/stable/27019011

Zureik, E., Lyon, D., & Abu-Laban, Y. (2010). *Surveillance and control in Israel/Palestine: Population territory and power*. London, UK: Routledge.