Israel Public Policy Institute

HEINRICH BÖLL STIFTUNG

HEINRICH BÖLL STIFTUNG TEL AVIV

German-Israeli Tech Policy Dialog Program

Who Will Watch the Watchmen?

Oversight of Online Surveillance in Israel

Amir Cahane

Rethinking Privacy and Mass Surveillance in the Information Age

Paper Series by the Israel Public Policy Institute and Heinrich Böll Foundation

Who Will Watch the Watchmen?

Oversight of Online Surveillance in Israel

Author

Amir Cahane

Project Lead

Heinrich Böll Foundation, Foreign and Security Policy Division, Berlin

Heinrich Böll Foundation Tel Aviv

Israel Public Policy Institute (IPPI)

Please cite as follows:

Cahane, A. (2020). *Who Will Watch the Watchmen? Oversight of Online Surveillance in Israel.* Paper Series "Rethinking Privacy and Mass Surveillance in the Information Age". Israel Public Policy Institute and Heinrich Böll Foundation

About the Project

The following paper has been commissioned by the Heinrich Böll Foundation and the Israel Public Policy Institute (IPPI) as part of the paper series *"Rethinking Privacy and Mass Surveillance in the Information Age."* Against the backdrop of the COVID-19 pandemic, this publication series has set out to examine the societal and political implications of the spillover of surveillance technologies from the security sphere into everyday life.

About the German-Israel Tech Policy Dialog Program

The paper series "Rethinking Privacy and Mass Surveillance in the Information Age" is part of the German-Israeli Tech Policy Dialog program of the Heinrich Böll Foundation and the Israel Public Policy Institute (IPPI). By facilitating a collaborative space for researchers and practitioners from politics, academia, tech and civil society, the program sets out to cultivate a community of committed professionals from both countries to deliberate the impact and governance of emerging technologies and to generate new actionable insights in support of democratic values.

Israel
Public Policy
Institute

Israel Public Policy Institute (IPPI)

The Israel Public Policy Institute (IPPI) is an independent policy think-and-do-tank and a multi-stakeholder dialog platform at the intersection of society, technology and the environment. Through its research activities, knowledge sharing, networking and public outreach, IPPI contributes to the innovation of public policy with the goal of understanding, guiding, and advancing the transformation process of our societies towards a sustainable and democratic future. IPPI works with a global network of actors from government, academia, civil society, and the private sector to foster international and interdisciplinary cross-pollination of ideas and experiences.

HEINRICH
BÖLL
STIFTUNG

Heinrich Böll Foundation

The Heinrich Böll Foundation is an independent global think-and-do-tank for green visions. With its international network of 33 international offices, the foundation works with well over 100 project partners in more than 60 countries. The foundation's work in Israel focuses on fostering democracy, promoting environmental sustainability, advancing gender equality, and promoting dialog and exchange of knowledge between public policy experts and institutions from Israel and Germany.

Contents

Executive Summary

Among the initial Israeli responses to the COVID-19 pandemic was the harnessing of counterterrorism surveillance measures used by the Israel Security Agency (also known as the ISA, GSS, "Shin Bet" or "Shabak") for coronavirus location tracking purposes. Israel was the only western country to publicly use its domestic security service to surveil its citizenry to ward off the crisis.

ISA coronavirus surveillance has brought into the limelight the "Tool," a database to which the service has been secretly siphoning communications metadata for nearly twenty years. The public parliamentary deliberative process and the juridical proceedings pertaining to the design of the legal framework authorizing the ISA to use the Tool for purposes beyond its statutory remit, provided us with a rare opportunity to examine the workings of the Israeli online surveillance oversight array.

Overall, it appears that since the spread of COVID-19, parliamentary oversight has managed to advance a more nuanced legal framework for ISA surveillance, adding controls and safeguards against human rights infringements. Judicial review of the framework at its early stages contributed to anchoring it in a statutory form, rather than in emergency regulations, thus ensuring enhanced parliamentary scrutiny. However, by focusing on the question of whether ISA coronavirus location tracking was necessary, the parliamentary oversight did not manage to promote alternative measures that would have entailed significantly fewer infringements.

Both the judicial review and parliamentary oversight have focused mainly on policymaking and designing the legal framework for ISA coronavirus surveillance. The attempt to introduce supervisory aspects of oversight – ensuring legal compliance and adherence to human rights standards on a routine basis – was less successful.

The lessons learned from Israeli SIGINT oversight during the COVID-19 crisis stress the importance of expertise and data-driven policymaking, as well as the significance of public participation by civil society actors and of transparency – both of which contribute to the enhancement of public trust in the ISA and, by extension, in other intelligence agencies. Finally, the shifting positions reviewed in this paper of the parliamentary oversight subcommittee regarding the necessity of alternative measures to ISA coronavirus location tracking can serve to indicate that proper SIGINT oversight should be independent of external political influences, stressing the need for a dedicated independent expert body tasked with the daily overseeing of SIGINT activities.

1. Introduction: Government Online Surveillance and its Oversight

Online Surveillance is a measure of SIGINT,[1] or Signals Intelligence. SIGINT is intelligence derived from the interception of signals, traditionally electromagnetic, used for communication or for other purposes.[2] In this paper, SIGINT will be used interchangeably with the term Online Surveillance, the latter applying to surveillance measures that intercept or otherwise collect data from communications networks (cellular, landlines the internet, etc.).

Rapid technological developments in recent decades have contributed to the accelerated proliferation of telecommunication technologies, and have enhanced the ability to process voluminous quantities of data. User data, when intercepted, collected, stored and analyzed provide business insights for commercial actors,[3] as well as invaluable intelligence to national security, counterterrorism, counterintelligence and law enforcement agencies.

> **The chilling effects of online surveillance are not limited to interference with one's online freedom of expression.[5]**

Notwithstanding that SIGINT may have legitimate purposes, the use of massive scale online surveillance measures by government authorities is also harmful. First and foremost, government-sanctioned online surveillance interferes with privacy rights (including privacy-related rights such as data protection rights or the right, originally established in the context of a German constitutional ruling, to informational self-determination).[4] Government surveillance also has potentially chilling effects, inhibiting or stifling individuals who are aware that they are being watched, followed or listened to, from freely expressing themselves. The chilling effects of online surveillance are not limited to interference with one's online freedom of expression.[5]

Online surveillance may also affect online search patterns[6] and, given the increasing prevalence of IoT devices – it may also interfere with offline activities.[7]

It is commonly accepted that proper legal safeguards, controls and oversight mechanisms over SIGINT activities can mitigate its harmful effects and reduce abuses of state surveillance powers for the furthering of illegitimate interests (be they political or individual).[8] However, despite their potential harmful effects, no SIGINT measures, including mass surveillance – i.e. the indiscriminate collection of bulk communications by intelligence agencies for national security purposes – are under any form of absolute prohibition by international legal standards (although a relevant case is pending before the Grand Chamber of the European Court of Human Rights).[9]

Despite the absence of international legal standards for SIGINT oversight, oversight infrastructure exists in some legal systems. Oversight mechanisms ensure that no individual abuses of power take place, monitor compliance to the legal framework pertaining to online surveillance and ideally promote adherence to human rights standards. Additionally, SIGINT oversight can reduce or even prevent individual and political abuse of surveillance powers. It also serves to prevent "purpose creep" – the use of data acquired for a specific purpose for a different purpose altogether. The mere existence of SIGINT oversight bodies may encourage compliance by intelligence agencies and law enforcement authorities.[10] Effective oversight mechanisms can strengthen public trust in national intelligence and law enforcement agencies[11] – a trust that since the Snowden revelations of 2013 has been eroded significantly.[12]

> **The use of counterterrorism surveillance measures to monitor the spread of the pandemic has also severely infringed upon the right to privacy.[17]**

Like any intelligence matters, SIGINT activities are usually kept secret. The ongoing COVID-19 crisis, where the Israeli government sought to use the online mass surveillance measures of its domestic security service – the Israel Security Agency, the ISA, also known as "Shabak" or "Shin Bet" – to track coronavirus carriers, provides us with a rare glimpse into the workings of the ISA oversight mechanisms. Several lessons can be drawn from this affair.

2. COVID-19 Location Tracking in Israel

2.1. Background

The first confirmed carrier of the novel coronavirus reached the shores of Israel in late February 2020.[13] Within a fortnight,[14] the exponential surge in the number of coronavirus carriers prompted a government response of implementing various restrictive measures,[15] such as a general lockdown limiting the freedom of movement to a 100-meter radius and the closing of certain commercial sectors, mainly in the service industry, impinging on the freedom of employment.[16] The use of counterterrorism surveillance measures to monitor the spread of the pandemic has also severely infringed upon the right to privacy.[17]

In early May 2020, following several weeks of lockdown, during which additional restrictive measures were applied, Prime Minister Benjamin Netanyahu celebrated his victory over the pandemic.[18] Restrictions were gradually removed, and as will be described below, coronavirus surveillance was phased out.

However, the second wave of the pandemic followed close on the heels of the first.[19] The ISA surveillance measures were promptly reinstated[20] and "red" cities were placed under nightly curfew. [21] The public's general perception appeared to be that due to government mismanagement, Israel is entering the second wave underprepared.[22] As these lines are being written, the government has ordered a second general lockdown.[23]

2.2. ISA Location Tracking of Coronavirus Carriers in Israel

2.2.1. ISA Location Tracking

When the vector of an airborne pandemic is human, such as in the case of COVID-19, contact tracing is a central tool in the process of identifying potential carriers of the disease and containing its spread.[24] During the first wave of the outbreak in Israel, contact tracing was initially handled by means of epidemiological investigations that relied mainly on oral questioning of confirmed coronavirus carriers, coupled with a manual review of their recent credit card history and public transportation digital logs for corroboration.[25] However, following PM Netanyahu's mid-March statement that the Israeli government intended to employ advanced digital monitoring tools to track coronavirus carriers,[26] the ISA was eventually authorized to use its surveillance measures to assist the Ministry of Health (MOH) in contact tracing.

> **Alongside ISA coronavirus surveillance operations, the government sought to authorize the police to acquire cellular location data from telecommunications providers in order to enforce quarantine orders.**

The ISA provided the MOH with cellular location data of the whereabouts of every identified coronavirus carrier as well as the identity of any other persons with whom they had been in close contact. To this end, the ISA utilized the "Tool," a secret database that was later exposed in the media. The Tool is a metadata communications database that has been accumulated by the ISA for nearly two decades[27] and contains metadata from all telecommunications licensees.[28]

At first, alongside ISA coronavirus surveillance operations, the government sought to authorize the police to acquire cellular location data from telecommunications providers in order to enforce quarantine orders.[29] Pursuant to a court order, these authorities were revoked,[30] restored,[31] but soon after shelved by the Minister of Justice.[32] Another COVID-19 surveillance technique employed in Israel was through the voluntary contact tracing app "Hamagen" ("the Shield," in Hebrew),[33] based on standard location APIs (not based on Bluetooth technology).[34] The second version of "Hamagen," launched during the second wave of the pandemic, failed to reach significant market penetration,[35] as 40% of its users eventually deleted it,[36] despite endorsement by the Privacy Protection Authority (PPA)[37] and leading privacy experts.

Among other surveillance measures that were suggested during the first wave of the pandemic but not adopted, were a health scoring monitoring system,[38] akin to the Chinese social scoring system, as well as mandatory installation of COVID-19 monitoring apps as an entry requirement for malls and commercial spaces.[39]

2.2.2. Development of a COVID-19 Legal Regime

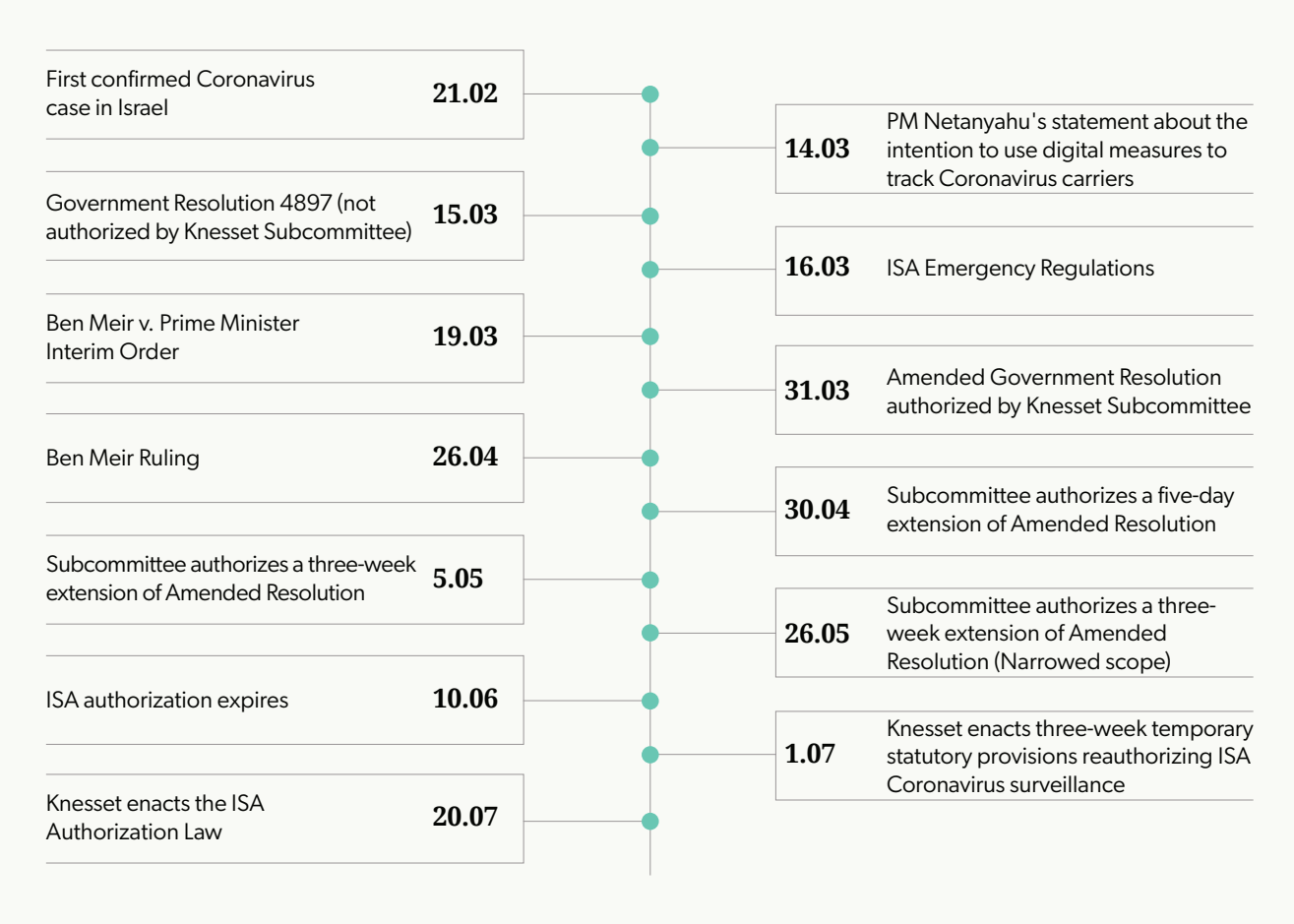
Israeli law limits the ISA's use of the Tool to a closed list of the organization's statutory purposes.[40] Unlike other jurisdictions, the list does not include public health.[41] However, the 2002 ISA Law authorizes the ISA to undertake activities designed to safeguard and promote vital state security interests other than those on the statutory list, pursuant to a government resolution authorized by the Knesset Service Affairs Committee (the Intelligence Subcommittee).

On March 15, the government attempted to pass a resolution to authorize the ISA to assist in the national effort to reduce the spread of the novel coronavirus.[42] However, given the timing of the recent elections, the day the Intelligence Subcommittee was due to convene to discuss the matter coincided with the day the new Knesset was to be sworn in, dissolving all acting parliamentary committees of the former, including the Intelligence Subcommittee. The Subcommittee refused to approve the resolution without a thorough discussion.[43]

The government responded by enacting emergency regulations overnight, authorizing the ISA to use metadata, as well as allowing the police to use cellular location data to address the coronavirus outbreak, effective for 30 days.[44] Several NGOs and activists challenged the constitutionality of the emergency regulations in what is known as the Ben Meir petition, and the High Court of Justice issued an interim order suspending the police from using its powers to enforce the regulations, thereby limiting the ISA's powers.[45] The court further ordered that unless the relevant parliamentary committees are established within five days, no use of the ISA's powers under the emergency regulations shall be made.

Figure 1.

Milestones in ISA Tracking and Parliamentary Oversight



Pursuant to the swearing in of the new Knesset, the Intelligence Subcommittee was reestablished, and began – while the emergency regulations were still in force – to discuss the authorization of the ISA and the police to engage in location tracking of coronavirus carriers. On the date the emergency regulations were scheduled to expire, following several meetings in which the Subcommittee was deliberating the necessity of these measures and the question of what legal framework could authorize them, the Subcommittee eventually approved an amended government resolution authorizing the ISA to engage in location tracking, effective for 30 days.[46]

While the amended government resolution was in effect, the High Court of Justice held a public hearing on the Ben Meir case, and issued its ruling several days before the amended resolution was set to expire.[47] The court ordered that upon expiration, any further authorization of ISA COVID-19 related surveillance could be delegated to a parliamentary subcommittee, but must be enacted in statutory law. However, the ruling also authorized extension of the effective period of the amended government resolution by "a few weeks", were such a legislative process to be sought by the government.

Subsequently, the Subcommittee authorized further extensions of the amended resolution,

to allow for an expedited drafting process. Within two weeks, a memorandum of law was published for public consultation. A week later, the Subcommittee authorized an additional three-week extension of ISA powers, narrowing the scope of ISA coronavirus location tracking to "particular and unique cases wherein identification of the persons who came into close contact with the [COVID-19] patient cannot be achieved by regular epidemiological investigative methods."[48] The final extension of the resolution was for two additional days, until the law could be brought to parliament by the government. Since the government chose not to approve further extensions, reportedly at the request of the ISA director, it expired on June 11, 2020.

Towards the end of June, as the second wave of the pandemic was looming, the bill was approved by the cabinet and subsequently passed in a preliminary reading in the Knesset plenum.[49] Following the suggestion of Intelligence Subcommittee chairperson MK Zvi Hauser, the bill was split in two: the main bill and temporary provisions. The latter were effective for 21 days and provided the Ministry of Health with immediate ISA assistance, while allowing for more thorough parliamentary deliberations on the main bill.

2.2.3. The Authorization Law

On July 20, the Knesset enacted the Law to Authorize the ISA to Assist in the National Effort to Contain the Spread of the Novel Coronavirus and to Promote Use of Civilian Technology to Locate Individuals who were in Close Contact with Patients (Temporary Provisions) 2020-5780 (hereinafter: The Authorization Law);[50] the law will remain in effect until January 20, 2021.

Under the Authorization Law, the government may declare that the ISA is authorized to process the "Technological Data" – certain categories of metadata defined in the Authorization Law – pertaining to a coronavirus carrier and to individuals with whom the carrier had been in close contact, and to transfer to the MOH the Required Information – defined as location data and movement routes in the 14 days preceding the diagnosis of the coronavirus carrier, as well as identification data of individuals who were in close contact with the carrier and their exposure time and location.

Such a declaration will be valid for a period not exceeding three weeks, and is permissible if the government is convinced that use of the ISA is necessary due to the likelihood of the spread of the disease, and provided that there is no suitable alternative measure available and pursuant to the recommendation of a ministerial team. The ministerial team will evaluate whether the stated need to use the ISA is in accordance with the law, taking into account the level of the spread of the pandemic, the contribution of ISA activities to its containment and the existence of alternative measures to the ISA. The ministerial team will be provided with the opinion of the Privacy Protection Authority (PPA). During the effective period, the MOH may request the assistance of ISA if the daily number of newly confirmed cases exceeds 200 patients. The declarations are subject to the approval of the Security and Foreign Affairs Committee of the Knesset.

The Authorization Law further determines the interface between the ISA and the MOH. It contains a notification and appeals procedures for individuals identified by the ISA as having been in close contact with coronavirus carriers. ISA

internal procedures under the Authorization Law are subject to Attorney General's approval and are classified. The MOH is instructed to determine particular procedures and to make them public. The law contains security and data protection provisions relating to purpose limitation, retention period and restricted access. The law further stipulates that the MOH shall provide the public with and promote the use of civilian location tracking technology to identify individuals who were in close contact with coronavirus carriers.

The process described above, of a constantly evolving legislative framework regulating the use of ISA for coronavirus location tracking, extends beyond the chosen regulatory legislative measure. Throughout this process, changes were introduced by various oversight actors. For example, the original government resolution (which failed to win the Intelligence Subcommittee's approval and did not come into force) was lacking a definition of the "Technological Data" the ISA was authorized to receive, process and collect. The definition offered by the subsequent emergency regulations reiterated the inclusive definition of the "Data" the service is authorized to collect under the ISA Law – "excluding the content of a conversation as defined in the Wiretap Law 1979-5739," namely all types of metadata. The amended government resolution narrowed the definition to include only location data, subscriber data and call history. The amended Authorization Law further elaborates by defining all three.

Analogous developments can be traced in other parameters such as the design of privacy safeguards and controls, and the reporting procedures. The detail and scope of privacy safeguards and controls were eventually expanded and refined. Similarly, whereas the original government resolution lacked any reporting procedures, under the provisions in the amended Authorization Law, both the ISA and MOH are required to provide a detailed weekly report to the Intelligence Subcommittee.

2.3. Oversight Bodies' Responses to the COVID-19 Crisis

2.3.1. Parliamentary Oversight – the Knesset Intelligence Subcommittee

The Israeli parliamentary committee generally responsible for oversight of the intelligence services is the Knesset Security and Foreign Affairs Committee, through its Intelligence Subcommittee. The ISA Law therefore designates the Intelligence Subcommittee as the Knesset committee for ISA affairs. The law requires the ISA director to report to the Subcommittee on the service's activities, and regulations and rules made under the ISA law are subject to the Subcommittee's approval. By default, its meetings are secret. During the COVID-19 pandemic, the Intelligence Subcommittee was the body responsible for overseeing all SIGINT activities – both due to its statutory role and unique circumstances brought about by the political instability in Israel at the time, which also enabled the Subcommittee to publicly express an independent position.

The Subcommittee's initial insistence on conducting a proper deliberative process rather than rubber-stamping the original government resolution that authorized the ISA to engage in coronavirus carriers' location tracking, was followed – after the Intelligence Subcommittee was dissolved, then re-established with the newly elected Knesset – by a series of thorough discussions in the Subcommittee. Most of these hearings were uniquely open to the public,

and civil society organizations as well as academic experts were welcome to contribute their viewpoint.

> **Most of the hearings – regardless of the legislative instrument discussed therein – focused on assessing the threat level and the necessity of utilizing the ISA to ward it off.**

It appears that most of the hearings – regardless of the legislative instrument discussed therein – focused on assessing the threat level and the necessity of utilizing the ISA to ward it off. Senior MOH representatives in the hearings repeatedly stressed the need to rely on ISA measures in lieu of alternatives. This was particularly evident in the earlier hearings, when the legal framework governing ISA activities was the amended government resolution and its subsequent extensions.

During these stages, the discussions at times appeared to lose focus as they drifted into a general debate on the national strategy to counter the pandemic. Members referred to the number of nurses qualified to conduct epidemiological investigations and to the number of daily coronavirus tests performed by the MOH. This diffuse focus appears to echo the "purpose creep" of the ISA in the COVID-19 affair from national security matters to the realm of public health. Despite the lack of focus on the dangers of surveillance, the Subcommittee did, however, address proportionality considerations, albeit implicitly. The various legal frameworks of ISA authorization contained evolving privacy and data protection safeguards.

The Intelligence Subcommittee stressed at an early stage that further extensions of the amended resolution would be conditioned upon thorough interdepartmental efforts to locate less intrusive measures. However, with a changing political landscape as a backdrop, the discussion of alternatives to ISA surveillance was deferred to early June, when the first wave of the pandemic was nearly over.

A recent exposé, referring to the era before COVID-19, criticized Subcommittee members for lacking familiarity with the Tool.[51] However, during the first meetings of the Subcommittee on ISA location tracking authorization, Subcommittee members received classified briefs by the ISA as to the scope and nature of the Tool, hence filling the expertise gap alleged by the exposé. Nevertheless, it appears that some confusion remained at the early stages of the meetings, when Subcommittee members were not aware that the proposed ISA authorization merely allows for a data-transfer scheme to the MOH, and assumed that a second metadata database would be created.[52] Also, new members of the Subcommittee that joined following the forming of the coalition between the Likud and the Blue and White parties, were not as well-informed as the carryover members from the Subcommittee disbanded prior to the change of government.

The Intelligence Subcommittee is a parliamentary oversight body. As such, it is susceptible to external political influences, albeit subtle. The advancing coalitional negotiations might have softened the insistence of Subcommittee chairperson MK Gabi Ashkenazi (later to become the Foreign Minister) on alternative measures. MK Hauser, Ashkenazi's successor as chairperson, being a member of a coalition party, expressed a position favoring ISA surveillance in lieu of civilian alternatives, with less insistence on developing alternative measures.

Overall, it appears that during the COVID-19 pandemic, parliamentary oversight has managed to further a more nuanced legal framework for ISA

surveillance, introducing controls and safeguards that the original government resolution was lacking. It was also unprecedentedly transparent, conducting publicly televised hearings.

> **By focusing on the necessity of isa coronavirus location tracking, the subcommittee did not manage to promote its replacement with alternative measures whose infringement of civil and human rights adhered to the standard of proportionality.**

However, By focusing on the necessity of isa coronavirus location tracking, the subcommittee did not manage to promote its replacement with alternative measures whose infringement of civil and human rights adhered to the standard of proportionality.

The public promotion of the government-developed app, Hamagen, which was approved by leading privacy experts, should have been more adamantly demanded by the Subcommittee, as the voluntarily downloaded app is far less intrusive than the non-voluntary measure employed by the ISA.

Bureaucrats are experts in their policy areas and have substantial informational advantages over their political overseers,[53] which are amplified within the national security context. The secretive technical nature of SIGINT activities often fosters organizational cultures within the intelligence agencies which elude the normal democratic oversight mechanisms.[54] However, it appears that the expertise gap of Subcommittee members has been bridged by thorough hearings, coupled with the assistance of civil society organizations. The active role played by the latter and by privacy experts contributed to richer, more informed deliberations.

The Subcommittee mainly concerned itself with policymaking, by designing the legal framework pertaining to ISA coronavirus surveillance. Its supervisory role, through repeated extensions of ISA powers under the amended government resolution, was lacking. In fact, the suggestion to narrow the scope of ISA coronavirus location tracking to "particular and unique cases" in the penultimate extension of the amended government resolution was reportedly initiated by the ISA itself, rather than by the Subcommittee.

2.3.2. Judicial Oversight

Unlike both police wiretapping and acquisition of metadata in Israel, which is subject to a court order, ISA surveillance is free from ex ante judicial review (see below). Accordingly, the High Court of Justice rarely hears cases pertaining to ISA SIGINT activities. The COVID-19 pandemic provided a rare instance where such matters were brought before the court. Upon the enactment of the emergency regulations authorizing the ISA to use its surveillance measures to track coronavirus carriers and authorizing the police to obtain location data of quarantined individuals to monitor their compliance with quarantine orders, several NGOs challenged the legality of the regulations by appealing to the Israeli High Court of Justice.

The interim decision in the Ben Meir case was rendered promptly, freezing the emergency regulations authorizing police cellphone location acquisition (only to unfreeze it within a week). The decision further limited the scope of ISA surveillance to confirmed coronavirus carriers, prohibiting surveillance of suspected cases pending laboratory confirmation. Notwithstanding, the court further ordered that ISA refrain from using its powers under the

emergency regulations unless it was apparent that the relevant parliamentary commission would be formed within several days.

> **Chief Justice Hayut stressed that authorizing the ISA to engage in location tracking severely infringes the right to privacy, given that the ISA is a domestic counterterrorism agency and that it collects communications metadata without the consent of the data subjects.**

The majority opinion in the Ben Meir ruling determined that the amended government resolution was initially valid, in light of the unknown threat posed by the pandemic at its early stages. However, since the government initially managed to contain the outbreak, the court – citing considerations of the separation of powers (the nondelegation doctrine in Israeli law)[55] – took care to stipulate that the proper legal instrument for authorizing ISA coronavirus surveillance is statutory law rather than a government resolution approved by a parliamentary subcommittee.[56] Furthermore, Chief Justice Esther Hayut's majority opinion, while not including a full proportionality review, did pay tribute to privacy rights considerations in an obiter dictum.

Chief Justice Hayut stressed that authorizing the ISA to engage in location tracking severely infringes the right to privacy, given that the ISA is a domestic counterterrorism agency and that it collects communications metadata without the consent of the data subjects.[57]

Following its enactment, the constitutionality of the Authorization Law was challenged in the High Court of Justice by some of the petitioners in Ben Meir. However, the court dismissed the petitions on procedural grounds.[58]

It appears that in the Ben Meir interim order, the court tried to stabilize the political situation by offering incentives to form the parliamentary committees. The application of the nondelegation doctrine in the Ben Meir opinion also reflects a view supporting parliamentary supremacy. However, despite strengthening the Knesset, the court did intervene regarding the proportionality of the ISA measures – first, in the interim order, by narrowing the scope of the emergency regulation to confirmed coronavirus carriers only; and second, in the Ben Meir opinion, albeit in an obiter dictum, by stressing the severe privacy violations caused by ISA authorization and by further emphasizing the importance of finding an effective alternative thereto.[59]

2.3.3. Other SIGINT Oversight Actors

The Privacy Protection Authority

Israel's data protection authority is the Privacy Protection Authority (PPA, formerly known as Israel Law and Information Technology Authority, ILITA). Although the PPA may have been internally consulted by the legal teams in the Ministry of Justice that drafted the legislative framework authorizing ISA coronavirus surveillance activities, it was not present in the early hearings of the Intelligence Subcommittee.

Only following a letter addressed to the Justice Minister by a group of privacy experts protesting the PPA's absence from the Subcommittee's hearing,[60] was the PPA invited to join them.

The PPA, however, did publish several opinions during the COVID-19 crisis. Following the Defense Minister's initiative of harnessing controversial private cyber actor NSO to develop a "health scoring" system akin to the notorious Chinese credit scoring systems,[61] the PPA published a

critical survey of credit scoring systems.[62] During early May 2020, in a letter to the Public Privacy Protection Committee, the PPA expressed its support for developing alternative measures to ISA surveillance.[63] Later that month, the PPA released a review of coronavirus digital monitoring measures, stating that acquisition of communication data (the measure employed by the ISA) is the most privacy-infringing measure among the alternatives.[64]

The Authorization Law requires the PPA to submit a periodic evaluation to the ministerial team reviewing the continuing need to engage the ISA under the law.[65] As of early September 2020, the PPA had submitted three such opinions,[66] calling for further implementation and promotion of the government-developed contact tracing app Hamagen 2.0 and expansion of the epidemiological investigative teams.

Despite its statutory role, the Authorization Law grants no additional legal powers to the PPA. Unlike the Subcommittee, an authorization deceleration under the Authorization Law is not subject to the PPA's approval. The circumstances under which the PPA received its advisory role to the ministerial team further suggest that its customary supervisory role over SIGINT activities is at best limited, if existent at all.

State Comptroller (Inspector General)

On several past occasions, the State Comptroller's Office has examined the use of police wiretapping.[67] While no state comptroller review of Israel's intelligence community's SIGINT practices has been made public to date, the ISA, Mossad and the military intelligence are within its purview.[68] Three months after the first outbreak of COVID-19, the State Comptroller's Office stated that it would include ISA coronavirus location tracking in its annual review.

NGOs, academics and privacy experts participated in the parliamentary hearings of the Intelligence Subcommittee on ISA coronavirus location tracking and voiced their concerns.

Civil Society Actors

Civil society organizations, while lacking any formal oversight role, played an important part in the COVID-19 crisis. The Ben Meir Case was brought before the High Court of Justice by two NGOs.

NGOs, academics and privacy experts participated in the parliamentary hearings of the Intelligence Subcommittee on ISA coronavirus location tracking and voiced their concerns. Many position papers and comparative legal and technical studies pertaining to location tracking technologies were published and submitted to the Subcommittee, fully informing its members regarding alternative measures to ISA surveillance. Also, as described above, were it not for the involvement of civil society, the PPA would not have been invited to join the Subcommittee's discussion and the general public debate on the matter.

3. Israeli SIGINT Oversight Framework

3.1. Legal Framework Pertaining to Government SIGINT Practices

The constitutional right to privacy in Israel is enshrined in Basic Law: Human Dignity and

Liberty, whose provisions state that "All persons have the right to privacy and to intimacy" and that "There shall be no violation of the confidentiality of conversation, or of the writings or records of a person."[69] However, the constitutional right to privacy in Israel is subject to a proportionality test, under which violations of the right to privacy may occur "by a law befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required."[70]

The Privacy Protection Law (PPL)[71] further provides for the protection of privacy in Israel, defining certain privacy infringements as civil tortious or criminal acts. The PPL also contains provisions pertaining to data protection and registration duties of database owners. However, the PPL also provides an exemption for privacy infringements perpetrated by security authorities and their employees, if committed reasonably and within the scope of their functions.

The SIGINT practices of law enforcement agencies are regulated through the Wiretap Law,[72] pertaining to the acquisition of content data (traditionally through wiretapping), and the Communications Data Law,[73] which sets the rules for law enforcement agencies' acquisition of communication metadata from licensed telecom service providers. There is also some crossover: Wiretapping for national security purposes is also covered by the Wiretap Law, while a provision in the ISA law regulates the ISA collection of communications metadata (reportedly using the Tool).

Similar to SIGINT legal regimes worldwide, the provisions governing online surveillance for national security purposes are laxer than those pertaining to law enforcement purposes, and the provisions applying to metadata are even laxer than those applying to content data.[74]

Israel's online surveillance law is dated, thin and mostly secret. It does not, for example, properly regulate automated processing, nor does it tackle issues of data retention or open-source intelligence collection (OSINT).[75] Furthermore, it should be noted that the SIGINT practices of the Mossad and of the military (through its SIGINT division, unit 8200) are not explicitly regulated under any specific law.[76]

3.2. The ISA's Tool

Not long after the government promulgated the emergency regulations authorizing the ISA to engage in coronavirus location tracking, an exposé provided a preliminary account of the Tool, the ISA's secret metadata database. Pursuant to certain provisions in the Communications Law (Telecommunications and Broadcasting)[77] – which is distinct from the privacy-focused Communications Data Law mentioned above – licensed telecom providers must cooperate with security forces, including the ISA. The ISA law further provides that the Prime Minister may create rules specifying data categories that it needs for its operations, and licensed telecom providers are required to comply with all such requests for data transfer. Combined, these provisions set the legal basis for the Tool that reportedly siphons all non-content data that streams through the channels of licensed telecommunications providers in Israel – internet service providers, cell phone carriers and land telephony providers.

According to the exposé, the ISA has been accumulating this database for two decades, and its treasure trove of metadata is coveted by many other government authorities.

3.3. Oversight Bodies in Israel: Main Actors

3.3.1. Parliamentary Oversight

The parliamentary committee overseeing the Israeli intelligence community is the Knesset Foreign Affairs and Defense Committee, to which the Prime Minister's Office – as well as the Defense, Foreign Affairs and Intelligence and Strategic Affairs Offices – reports on matters of security and foreign affair. It appears from the founding memorandum of the committee, drafted in 2005, that the committee focuses on overseeing efficacy aspects of intelligence collection,[78] rather than on questions of legal compliance and adherence to human rights standards.[79]

> **According to the exposé, the ISA has been accumulating this database for two decades, and its treasure trove of metadata is coveted by many other government authorities.**

Under the ISA Law, the Intelligence Subcommittee of the Foreign Affairs and Defense Committee, to which the ISA Director reports, has a statutory oversight role over the ISA. The Subcommittee is required to authorize rules and regulations dictated by the Prime Minister, as per the mandate given to him by the ISA law, as well as resolutions tasking the ISA with duties beyond its statutory remit, such as the government resolution to use the ISA for coronavirus location tracking. Unless decided otherwise, the Subcommittee's meetings are secret.

> **The lack of transparency, with no statutory duty to publicly publish annual reports, is concerning.**

The secrecy shrouding the Subcommittee's activities poses difficulties in assessing the quality of its oversight. Regardless of the general critique of parliamentary intelligence oversight,[80] expertise of its members in SIGINT matters, and especially the existence and capabilities of the Tool, was reportedly lacking also prior to the COVID-19 outbreak.[81] The lack of transparency, with no statutory duty to publicly publish annual reports, is concerning.

3.3.2. Judicial Oversight

Israel's judicial oversight of online surveillance in only partial.[82] Ex ante judicial review of SIGINT activities is purpose-limited. Wiretapping and communication data acquisition for law enforcement purposes are subject to an ex ante court order,[83] whereas SIGINT activities for national security purposes by the ISA require only internal ex ante executive approval.[84] It should be noted that the annual reports of the Internal Security Ministry show that courts' rejection rate of wiretap and data acquisition requests is extremely low, averaging less than 0.5%.[85]

All online surveillance activities may be subject to ex post facto judicial review; however, unlike targets of police wiretapping, which are incentivized to challenge the electronic evidence collected against them, there is small likelihood that unaware targets of secretive ISA measures will manage to do the same.[86]

The rules pertaining to government SIGINT activities may also be constitutionally challenged in court. Indeed, pursuant to such a challenge,

for example, the High Court of Justice narrowed the scope of the Communications Data Law[87] and recently, as described above, it invalidated the emergency regulations authorizing ISA coronavirus surveillance.

> **In light of the partial ex ante judicial oversight of online surveillance, coupled with its secretive nature and the general lack of court expertise in matters of national security and intelligence, it is doubtful that the Israeli court is an effective oversight body.**

While claims that judicial oversight of intelligence services in Israel is significant and effective[88] might be supported in light of the High Court of Justice's seminal ruling in the ISA torture case,[89] these arguments cannot be applied to SIGINT.

In light of the partial ex ante judicial oversight of online surveillance, coupled with its secretive nature and the general lack of court expertise in matters of national security and intelligence, it is doubtful that the Israeli court is an effective oversight body.[90]

3.3.3. Executive and Internal Oversight

Reportedly, the ISA has internal controls – some automated – overseeing its employees' compliance with internal rules and guidelines.[91] However, these rules and guidelines, as well as the internal controls, are all classified.[92]

Alongside these managerial controls, the ISA has two internal gatekeepers: the ISA comptroller and the service's legal advisor. The ISA comptroller has statutory standing, with special provisions in the ISA law that strengthen its position and independence.[93] The ISA legal advisor has no statutory grounding, and before 1973, there was no internal legal team in the service. Pursuant to the Bus 300 Affair in the 1980s, the service legal team was reorganized, and the service's legal advisor became a member of its directorate.[94]

A central role in the Israeli SIGINT oversight system is reserved for the Attorney General's Office. Both the Wiretap Law and the Communications Data Law, as well as the ISA Law, provide for the police and the ISA to report to the Attorney General on their online surveillance activity. The Attorney General may cancel wiretap authorizations granted by the ISA director or by the Police Commissioner in urgent circumstances (where a judicial or ministerial authorization could not have been timely secured).

Reportedly, the Attorney General's Office's monthly and quarterly reviews of police and ISA reports are thorough.[95] Nevertheless, in a 2009 parliamentary inquiry of police wiretaps, there were voices calling for even closer examination of every separate wiretap and permit[96] – a standard that seems impossible to apply to the massive data collection by the Tool.

The oversight functions of the Attorney General's Office, similar to the parliamentary oversight by the Intelligence Subcommittee, are shrouded in secrecy. There are no legal provisions providing for public reports of the routine review sessions held by the Attorney General, and none have been made public on a voluntary basis.

4. Conclusions: Lessons From the COVID-19 Pandemic

Before addressing the lessons derived from COVID-19 relating to Israel's SIGINT oversight array, we should take note of a more general insight. First and foremost, the pandemic has made the Israeli public more aware of the ISA's surveillance measures, and of the existence of the Tool.

> **The legislator should reexamine the provisions in the ISA law that authorized the service to acquire and retain any communications metadata transferred through the services of telecom providers, and provide a public accounting of the rules governing the Tool, which are currently classified.**

Now that Israel's domestic mass surveillance practices are no longer a secret, the Tool must be more carefully regulated.

The legislator should reexamine the provisions in the ISA law that authorized the service to acquire and retain any communications metadata transferred through the services of telecom providers, and provide a public accounting of the rules governing the Tool, which are currently classified.

The COVID-19 crisis also allowed for the first publicized deviation from the statutory purpose limitation of the Tool. This raises concerns of future "purpose creep" – now that the floodgates are open – where the Tool, a highly intrusive counterintelligence measure, will be further used for purposes that cannot justify its already questionable level of intrusive surveillance.

A set of unique circumstances during the COVID-19 pandemic provided a rare glance into the usually secretive working of SIGINT oversight in Israel. However, the critical lessons derived from the workings of the Israel's SIGINT oversight during the pandemic may be only partial, as routine SIGINT oversight in Israel has a geo-political aspect that is absent in the context of the coronavirus. The differences between countering a pandemic and countering terrorism relate to the type of oversight applied (policy-level rather than routine review and controls; lower relevance of ex ante judicial review) as well as to the manner in which the oversight is applied (increased public participation in the debate; more concern regarding human rights violations on the part of monitoring entities).

However, the Israeli SIGINT oversight array's handling of granting authorizations to the ISA for purposes of coronavirus surveillance did emphasize some important points that are to this day relevant to oversight functions.

The COVID-19 crisis stressed the importance of expertise and data driven policymaking. The Subcommittee's new members and arguably, also its existing members, had to be promptly briefed on the Tool. It may be the case that the lack of a coherent benchmark for ISA surveillance effectiveness vis-à-vis civilian alternatives contributed to the weakening of the Subcommittee's insistence on the latter.

SIGINT oversight during the pandemic was unprecedentedly transparent. Publicly televised court hearings and parliamentary subcommittee hearings pertaining to matters that are usually kept in the dark, facilitated public participation of civil society experts and had the potential of enhancing

public trust. Civil society actors also played an important role in filling the expertise gaps of the parliamentary Subcommittee, as well as initiating the legal proceedings that eventually invalidated the emergency regulations – if only temporarily.

> **The lack of a dedicated, independent, expert body tasked with the daily overseeing of SIGINT activities, is evident from the handling of the COVID-19 pandemic.**

However, the government seems to have squandered the public's trust, as is evident from the failure of the government-developed contact tracing app, Hamagen 2.0, to reach critical exposure.[97] The erosion of public trust could have been mitigated through reliable oversight mechanisms ensuring that government-sanctioned surveillance was kept in check and that the government-developed app was not a "spy tool."

In addition to an urgent need for a legal reform of Israeli surveillance law,[98] which stands to gain from a thorough deliberative process such as in the legislation of the Authorization Law (even if that too was not free of difficulties), the SIGINT oversight system should be revamped.

The changing attitudes of the Subcommittee towards authorization of ISA surveillance can be attributed to political shifts in the background. An external independent agency, free from political pressures, might have been more insistent regarding the need to find alternative measures to ISA mass coronavirus surveillance.

The lack of a dedicated, independent, expert body tasked with the daily overseeing of SIGINT activities,[99] is evident from the handling of the COVID-19 pandemic to date. This agency, the likes of which can be found in the UK,[100] the Netherlands[101] and in other European jurisdictions, should also be transparent, making its findings public on an annual basis, thus cultivating the eroded public trust in the national intelligence and law enforcement agencies.

Endnotes

[1] Cahane, A. and Shany, Y. (2019). Regulation of Online Surviellance in Israeli Law and Comparative Law. Israel Democracy Institute [Hebrew].

[2] Richards, J. (2014). Signals Intelligence. In Dover, R., Goodman, M.S. and Hillebrand, C. Routledge Companion to Intelligence Studies. Routledge.

[3] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs.

[4] 65 BVerfGE 1 (1983).

[5] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, pars. 2-16 (A/HRC/29/32, 2015).

[6] Marthews, A. and Tucker, C. (2017). The Impact of Online Surveillance on Behavior. In Gray, D. and Henderson, S.E., The Cambridge Handbook of Surveillance Law. Cambridge: Cambridge University Press. pp. 437-454.

[7] Tyagi, A.K. and Shamila, M. (2019), Spy in the Crowd: How User's Privacy Is Getting Affected with the Integration of Internet of Thing's Devices. https://www.ssrn.com/abstract=3356268.

[8] See for example Rättvisa v. Sweden, No. 35252.08, EUR. CT. H.R. (2018); Big Brother Watch and others v. The United Kingdom Nos. 58170/13, 62322/14 and 24960/15 EUR. CT. H.R. (2018).

[9] Applicants' Request for a Reference to The Grand Chamber, App. No. 58170/13 Big Brother Watch & ors v UK (12.12.2018).

[10] Deeks, A. (2013). The Observer Effect: National Security Litigation, Executive Policy Changes, and Judicial Deference. Fordham Law Review 82(2). pp. 827-898.

[11] Anderson, D. (2015). A Question of Trust (Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation).

[12] Greenwald, G. and MacAskill, E. (2013, June 11). Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data. The Guardian. https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

[13] Israel confirms first Coronavirus case as cruise ship returnee diagnosed. (2020, February 21). The Times of Israel. https://www.timesofisrael.com/israel-confirms-first-coronavirus-case-as-cruise-ship-returnee-diagnosed/.

[14] Coronavirus disease 2019 (COVID-19) Situation Report – 41. (2020, March 1). World Health Organization. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200301-sitrep-41-covid-19.pdf; Coronavirus disease 2019 (COVID-19) Situation Report – 55. (2020, March 15). World Health Organization. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200315-sitrep-55-covid-19.pdf.

[15] Gross, A. (2020, May 29). Rights Restrictions and Securitization of Health in Israel During COVID-19. Bill of Health. https://blog.petrieflom.law.harvard.edu/2020/05/29/israel-global-responses-covid19/.

[16] Albin, E., and Mundlak, G. (2020). COVID-19 and Labour Law: Israel. Italian Labour Law e-Journal 13(1S). DOI: https://doi.org/10.6092/issn.1561-8048/10794.

[17] Cahane, A. (2020, March 16). Chilling Effect: Online Surveillance in days of Corona. CSRCL blog. https://csrcl.huji.ac.il/blog/chilling-effect-online-monitoring-days-corona.

[18] Horovitz, D. (2020, May 5). Netanyahu celebrates a victory over COVID-19; it marks his political triumph too. The Times of Israel. https://www.timesofisrael.com/netanyahu-celebrates-a-victory-over-covid-19-it-marks-his-political-triumph-too.

[19] Ng, A. and Graham, E. (2020, July 15). Israel's leader is starting to pay a 'political price' as virus cases surge, protests erupt. CNBC. https://www.cnbc.com/2020/07/15/coronavirus-israels-cases-rise-leader-is-paying-a-political-price.html.

[20] Bob, Y.J. (2020, June 30). Knesset c'tee approves reinstating Shin Bet coronavirus surveillance. The Jerusalem Post. https://www.jpost.com/israel-news/politics-and-diplomacy/knesset-ctee-approves-reinstating-shin-bet-coronavirus-surveillance-633327.

[21] Bachner, M. (2020, September 9). A charade: Nightly curfew in 'red' cities mocked as measures go unenforced. The Times of Israel. https://www.timesofisrael.com/a-charade-nightly-curfew-in-red-cities-mocked-as-measures-go-unenforced/.

[22] Kaplan Sommer, A. (2020, September 17). 'Stupid, Scandalous, All Because of Bibi': In Quiet Tel Aviv Suburb, Rage Over Israel's Second Lockdown .Haaretz. https://www.haaretz.com/israel-news/.premium-it-s-all-because-of-bibi-in-quiet-tel-aviv-suburb-rage-over-second-lockdown-1.9160968.

[23] Coronavirus: Israel to impose three-week national lockdown (2020, September 14). BBC. https://www.bbc.com/news/world-middle-east-54134869.

[24] Kahn, J. and Technologies, J.H.P.E.G.D.C.T. (2020). Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance. Baltimore: Johns Hopkins University Press., DOI:10.1353/book.75831.

[25] Linder, R. (2020, March 8). "People are shocked when they learn they have corona. There are incidents of hiding it". TheMarker [HEBREW]. https://www.themarker.com/allnews/.premium-1.8637388?lts=1584220242283.

[26] Gross, A.J. (2020, March 15). Netanyahu sparks privacy scare with move to track corona patients' phones. The Times of Israel. https://www.timesofisrael.com/netanyahu-sparks-privacy-concerns-with-move-to-track-corona-patients-phones/.

[27] Bergman, R. and Shvartztuch, I. (2020, March 25) The 'Tool', the GSA secret database has been collecting data on all Israeli citizens and knows: where were you, whom you have spoken to, and when. Yediot Aharonot [Hebrew]. https://www.yediot.co.il/articles/0,7340,L-5701611,00.html.

[28] Tene, O. (2017). Systematic Government Access to Private-Sector Data in Israel: Balancing Security Needs with Democratic Accountability. In Cate, F.H. and Dempsey, J. Bulk Collection: Systematic Government Access to Private-Sector Data. pp. 91-110.

[29] Cahane, A. (2020, March 21). The Israeli Emergency Regulation for Location Tracking of Coronavirus Carriers. Lawfare. https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers.

[30] HCJ 2109/20 Ben Meir v. Prime Minister (unpublished, 19 March 2020). English translation available at https://versa.cardozo.yu.edu/sites/default/files/upload/opinions/Ben%20Meir%20v.%20Prime%20Minister.pdf.

[31] HCJ 2109/20 Ben Meir v. Prime Minister (unpublished, 24 March 2020) English translation available at https://versa.cardozo.yu.edu/viewpoints/coronavirus-interim-order-update.

[32] Coronavirus: Israel halts police phone tracking over privacy concerns. (2020, April 23). BBC. https://www.bbc.com/news/technology-52395886.

[33] Hamagen, Privacy Policy and Information Security, https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/ (Released 21 March 2020, updated 27 July 2020).

[34] Shwartz Altshuler, T. and Aridor Hershkowitz, R. (2020). Digital contact tracing and the coronavirus: Israeli and comparative perspectives. Brookings. https://www.brookings.edu/research/digital-contact-tracing-and-the-coronavirus-israeli-and-comparative-perspectives/.

[35] Sokol, S. (2020, July 27). Health Ministry launches revamped COVID-19 tracking app. Times of Israel. https://www.timesofisrael.com/health-ministry-launches-revamped-covid-19-tracking-app.

[36] Bender, A. (2020, August 8). Almost 40% of the Isrealies who downloaded 'Hamagen 2.0' - choose to remove it. Maariv [Hebrew]. https://www.maariv.co.il/business/tech/Article-781399.

[37] Hamagen 2.0 App – how does it protect both health and privacy?. (2020, September 15). Privacy Protection Authority [Hebrew]. https://www.gov.il/he/departments/general/app-ministry-of-health-privacy.

[38] Kabir, O. (2020, April 1). New Israeli Covid-19 Infection Ranking App Reminiscent of China's Citizen Ranking System, Experts Say. Calcalist. https://www.calcalistech.com/ctech/articles/0,7340,L-3805426,00.html.

[39] Israelis required to install coronavirus tracking app to gain entry to malls and markets. (2020, April 29). i24NEWS. https://www.i24news.tv/en/news/israel/society/1588191836-israelis-required-to-install-coronavirus-tracking-app-to-gain-entry-to-malls-and-markets.

[40] General Security Service Law, 5972-2002, SH No. 1832 p. 172, Sec. 11. (Hereinafter: ISA Law) English translation available at https://knesset.gov.il/review/data/eng/law/kns15_GSS_eng.pdf.

[41] See Investigatory Powers Act, 2016, c. 25 (Eng.), Section 61(7)(e). Note, however, that this section applies to targeted acquisition of communications metadata, whereas the ISA's 'Tool' is an instrument of mass, untargeted surveillance.

[42] Government Res. No. 4897, Authorizing ISA to assist in the national effort to reduce the spread of the Novel Coronavirus, 15 March 2020. [Hebrew] https://www.law.co.il/media/computer-law/gov-corona-shbak.pdf.

[43] Subcommittee on Secret Services refrains from voting on government's request to allow Shin Bet to take part in efforts to stop spread of coronavirus. (2020, March 15). Knesset News. https://main.knesset.gov.il/en/News/PressReleases/Pages/press17320b.aspx.

[44] Cahane (2020, March 21).

[45] Ben Meir (19 March 2020).

[46] Cahane, A. (2020, July 18). Counterterrorism measures to counter epidemics: Covid-19 contact tracing in Israel. Blogdroiteuropéen. https://blogdroiteuropeen.com/2020/07/18/counterterrorism-measures-to-counter-epidemics-covid-19-contact-tracing-in-israel-by-amir-cahane/.

[47] See HCJ 2109/20 Ben Meir v. Prime Minister (Unpublished, 26 April 2020) https://versa.cardozo.yu.edu/opinions/ben-meir-v-prime-minister-0.

[48] Kabir, O. (2020, May 26). Lawmakers Extend Spy Agency's Covid-19 Patient Tracking Program by Three Weeks. CTech. https://www.calcalistech.com/ctech/articles/0,7340,L-3827350,00.html.

[49] Ministers unanimously back phone-tracking bill opposed by Shin Bet. (2020, June 24). Times of Israel. https://www.timesofisrael.com/ministers-unanimously-back-phone-tracking-bill-opposed-by-shin-bet; Jaffe-Hoffman, M. (2020, June 24). Knesset advances bill to enable Shin Bet surveillance in coronavirus fight. The Jeruslaem Post. https://www.jpost.com/breaking-news/154-new-coronavirus-patients-in-israel-632601.

[50] The Law to Authorize the ISA to Assist in the National Effort to Contain the Spread of the Novel Coronavirus and to Promote Use of Civilian Technology to Locate Individuals who were in Close Contact with Patients (Temporary Provisions) 2020-5780, SH No. 2816, p. 166.

[51] Bergman and Shvartztuch (2020).

[52] Minutes of the Intelligence and Secret Services Subcommittee of the Knesset's Security and Foreign Affairs Committee, protocol no. 3 (30 March, 2020). See MK Ashkenazi's referral to "[Data] pool 2", p. 20.

[53] Banks, J.S. and Weingast, B.R. (1992). The Political Control of Bureaucracies under Asymmetric Information. American Journal of Political Science 36(2), pp. 509-524.

[54] Lester, G. (2015). When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence. Cambridge: Cambridge University Press.

[55] Ben Meir (26 April 2020).

[56] Chachko, E. (2020, May 5). The Israeli Supreme Court Checks COVID-19 Electronic Surveillance. Lawfare. https://www.lawfareblog.com/israeli-supreme-court-checks-covid-19-electronic-surveillance.

[57] Ben Meir (26 April 2020), para 38.

[58] Shinar, A. (2020, September 6). Why decide if you can avoid?. Deyioma [Hebrew]. https://bit.ly/32EM71N.

[59] Ben Meir (26 April 2020), para 40-42.

[60] Kabir, O. (2020, April 22). Privacy Experts to Government: there are those who want that the right to privacy will not interfere with the corona crisis. Calcalist [Hebrew]. https://www.calcalist.co.il/internet/articles/0,7340,L-3809882,00.html.

[61] Yablonko, Y. (2020, March 30). Bennett plans using NSO to rate individual virus exposure. Globes. https://en.globes.co.il/en/article-bennett-plans-using-nso-to-rate-individual-virus-exposure-1001323878.

[62] Social scoring in light of the right to privacy: a review regarding social scoring systems. (2020, April 23). Privacy Protection Authority [Hebrew]. https://www.gov.il/he/departments/publications/reports/social_ranking.

[63] Letter from Adv. Garson (Privacy Protection Authority) to Ms. Podemski (Public Privacy Protection Committee). (2020, May 3) [Hebrew]. https://www.law.co.il/media/computer-law/ppa-shabak.pdf.

[64] Digital monitoring in the Corona age in light of the right to privacy: technologies' review, a global comparative look and ranking of possible models. (2020, May 26). Privacy Protection Authority [Hebrew]. https://www.gov.il/he/departments/publications/reports/digital_tracking_riview.

[65] The Authorization Law, Section 12(a).

[66] PPA Opinion in accordance with The Law to Authorize the ISA to Assist in the National Effort to Contain the Spread of the Novel Coronavirus (temporary provisions). (2020, July 14). Privacy Protection Authority [Hebrew]. https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus/he/privacy-shabak-coronavirus.pdf; Opinion No. 2 in accordance with The Law to Authorize the ISA to Assist in the National Effort to Contain the Spread of the Novel Coronavirus (temporary provisions). (2020, August 6). Privacy Protection Authority [Hebrew]. https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus_2/he/privacy-shabak-coronavirus-2.pdf; Opinion No. 3 in accordance with The Law to Authorize the ISA to Assist in the National Effort to Contain the Spread of the Novel Coronavirus (temporary provisions). (2020, August 30). Privacy Protection Authority [Hebrew]. https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus_3/he/privacy-shabak-3.pdf.

[67] Cahane, A. and Shany, Y. (2020). Oversight of Online Surveillance in Israel. Israel Democracy Institute [Hebrew]. pp. 204-206.

[68] Cahane and Shany (2020), p. 204.

[69] Basic Law: Human Dignity and Liberty, 5752-1992, SH No. 1391 p.60 (Isr.), Art. 7.

[70] Barak, A. (2012). Proportionality: Constitutional Rights and their Limitations. Cambridge: Cambridge

University Press.

71 Privacy Protection Law, 1981-5741, SH No. 1011 p. 128 English translation available at https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf.

72 Wiretap Law, 5739-1979, SH No. 938 p. 188 (Isr.) [hereinafter: Wiretap Law].

73 Criminal Procedure Law (Enforcement powers – Communications Data), 5768-2007, Sec. 1, SH No. 2122 p.72 (Isr.) [hereinafter: Communications Data Law].

74 Murray, D. and Fussey, P. (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. Israel Law Review 52(1), pp. 31-60.

75 Cahane and Shany (2019).

76 Tene (2017).

77 Telecommunications Law 1982-5742, SH No. 1060 p. 218.

78 Cahane and Shany (2020), p. 217.

79 Cayford, M., Pieters, W. and Hijzen, C. (2018). Plots, Murders, and Money: Oversight Bodies Evaluating the Effectiveness of Surveillance Technology. Intelligence and National Security 33(7), pp. 999-1021.

80 Cahane and Shany (2020), pp. 74-83.

81 Bergman and Shvartztuch (2020).

82 Cahane, A. and Shany, Y. (2019, February 6). Partly undercover: Judicial Review of Online Surveillance in Israel. Parliament [Hebrew]. https://www.idi.org.il/parliaments/25693/25702.

83 Communications Data Law; Wiretap Law.

84 ISA law; Wiretap Law.

85 Cahane and Shany (2020), pp. 199.

86 Rumold, M. (2017). Regulating Surveillance Through Litigation: Some Thoughts from the Trenches. In Gray, D. and Henderson, S.E., The Cambridge Handbook of Surveillance Law 579. Cambridge: Cambridge University Press.

87 HCJ 3809/08 Association for Civil Rights in Israel v. Israeli Police (unpublished,28.5.2012) [hereinafter: ACRI]. unofficial English translation of the ruling available at https://versa.cardozo.yu.edu/opinions/association-civil-rights-israel-v-israel-police.

88 Bitton, R. (2016). In Law We Trust: The Israeli Case of Overseeing Intelligence. In Goldman, Z.K. and Rasscoff, S.J. Global Intelligence Oversight – Governing Security in the 21th Century.

89 HCJ 5100/94 Public Committee Against Torture v. Israel (6.9.1999). Unofficial English transltaion available at https://versa.cardozo.yu.edu/opinions/public-committee-against-torture-v-israel.

90 See, for example, State Comptroller's Opinion, Wiretapping in criminal investigations, (2010, June 28).

91 Bergman and Shvartztuch (2020).

92 ISA Law.

93 HCJ 5682/02 Doe v. Prime Minister (2003). Para 17 (Barak J.).

94 Bachar, E. (2013). The Role of the Legal Counsel in Security Agencies. Israel Democracy Institute [Hebrew]. pp. 66.

95 Bergman and Shvartztuch (2020).

96 Parliamentary inquiry committee regarding wiretapping. (2009). Summary of hearings. pp. 29-30.

97 See experts' comments in Kabir, O. (2020, September 21). Why Israelis delete the Hamagen 2.0 App?.

Calcalist [Hebrew]. https://www.calcalist.co.il/internet/articles/0,7340,L-3850763,00.html; see also Shwartz Altshuler, T., Aridor. R. and Toch, E. (2020, May 21). The Need for Voluntary Tracking. Israel Democracy Institute [Hebrew]. https://www.idi.org.il/articles/31389.

98 Cahane and Shany (2019).

99 See Cahane and Shany (2020) for a detailed policy outline of such an agency.

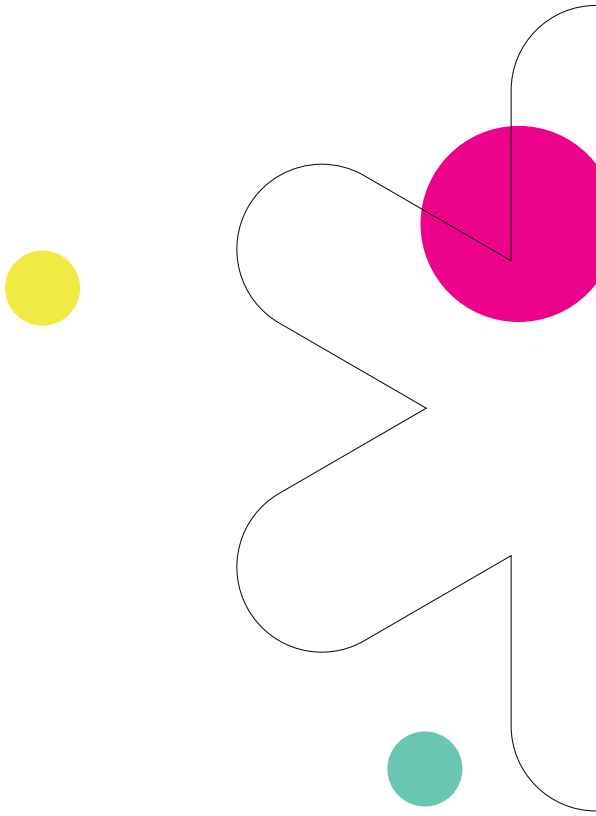
100 See Cahane and Shany (2020), pp. 125-132.

101 See Cahane and Shany (2020), pp. 170-171.

About the Author

Amir Cahane is a visiting scholar at the Federmann Cyber Security Center – Cyber Law Program at the Hebrew University, Jerusalem, since January 2018. His research interests are online surveillance law, encryption rights and AI. His book (with Prof. Yuval Shany), Oversight of Online Surveillance in Israel, was recently published in Hebrew by the Israel Democracy Institute, where he worked for three years as a researcher.

Amir holds a LL.B from the Interdisciplinary Center Herzliya (Israel) and a B.Sc in statistics and business management from Tel Aviv University (Israel). He earned his LL.M at Cambridge University (UK). Previously, Amir worked as an associate lawyer in the high-tech department of a major Israeli law firm.



Israel Public Policy Institute

Hapelech St. 7, Tel Aviv, Israel
→ office.israel@ippi.org.il
→ www.ippi.org.il

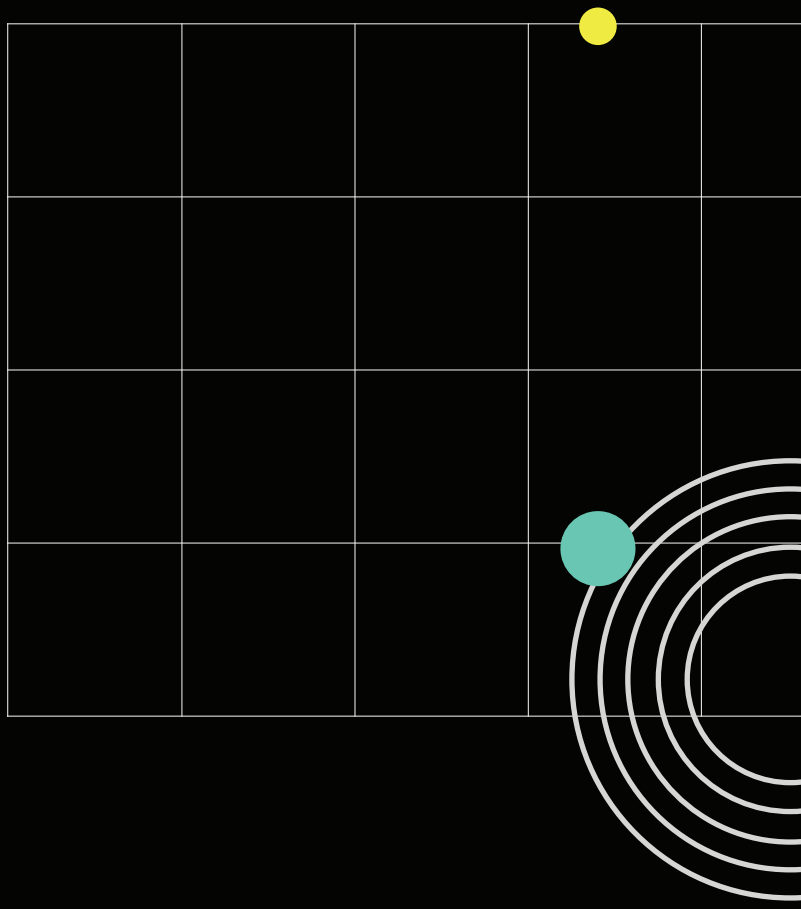
Heinrich Böll Foundation

Schumannstraße 8, Berlin, Germany
→ info@boell.de
→ www.boell.de

Heinrich Böll Foundation Tel-Aviv

Har Sinai St. 1, Tel Aviv, Israel
→ info@il.boell.org
→ www.il.boell.org

Release date: November 2020



HEINRICH
BÖLL
STIFTUNG

Israel
Public Policy
Institute

HEINRICH BÖLL STIFTUNG
TEL AVIV