The University of New Hampshire Law Review

Volume 19 | Number 2 Article 7

5-1-2021

Israel's SIGINT Oversight Ecosystem: COVID-19 Secret Location Tracking as a Test Case

Amir Cahane

Amir Cahane

Israel's SIGINT Oversight Ecosystem: COVID-19 Secret Location Tracking as a Test Case

19 U.N.H. L. Rev. 451 (2021)

ABSTRACT. By mid-March 2020, Israel had experienced the first wave of the COVID-19 pandemic. Within a fortnight, confirmed coronavirus cases surged from half a dozen to 178 cases. In response to the challenge of identifying potential carriers, the government tasked the Israeli Security Agency (the ISA, or Shin Bet) with tracing the routes of confirmed coronavirus patients via cellphone location tracking and identifying individuals with whom the patients had been in close contact.

Israel's ISA communications metadata collection measures have been shrouded in veil of secrecy. The debate – in parliament and in court – regarding the use of the country's secret service counterterrorism mass surveillance measures to contain the spread of the pandemic is a rare opportunity to assess whether the institutional oversight mechanisms on SIGINT collection activities are sufficient and effective.

The paper will (1) describe the existing SIGINT oversight regime in Israel; (2) describe the SIGINT oversight ecosystem's response to COVID-19 location tracking in Israel; and, (3) in light of existing literature, provide an analysis of that response.

AUTHOR. Research Fellow, Federmann Cyber Security Center – Cyber Law Program, Hebrew University of Jerusalem; Researcher, Israel Democracy Institute. The Author wishes to thank the Symposium Editor, Derek Kaufman, and the University of New Hampshire Law Review editorial board for their efforts in bringing this article to publication

I. INTRODUCTION

> "The [Internal Affairs] committee states that there were some past incidents that could have been viewed as deviating from a direct security interest; The committee expresses its will that principle under which these services operate only in matters directly pertaining to the security of Israel shall be strictly followed."[1]

These two laconic lines by the Israeli's Knesset ad hoc parliamentary subcommittee for the matter of secret wiretapping devices and secret party services concluded the parliamentary response to the two Shin Bet operatives discovered in January 1953 while installing listening devices in the headquarters of the United Workers Party (Mapam). In the early years of the Israeli state, the mere existence of the Shin Bet, the domestic security service later to be known as the Shabak, the General Security Service (GSS) or the Israel Security Agency (ISA), was kept secret and was employed by the dominant ruling party, the Workers of Eretz-Israel Party (Mapai) against political opponents.[2]

In the following decades, public, parliamentary, and judicial attention to intelligence oversight in Israel tended to focus on HUMINT (Human Intelligence) investigatory powers.[3] More than half a century later, the COVID-19 pandemic reawakened the public discourse regarding the regulation and oversight of government surveillance practices.[4] The policy undertaken by the Israeli government in the wake of the first wave of the coronavirus – employing

---

1 DK (1956) 357, 370 (Isr.).

2 Ian Black & Benny Morris, Israel's Secret Wars 149–153 (1991). However, it should be noted that some of the Shin Bet counterespionage activities targeting Mapam were justified. According to the KGB archive, some Mapam MKs did in fact share classified information with the Soviet Union. *See* Christopher Andrew & Vasili Mitrokhin, The World Was Going Our Way: The KGB and the Battle for the Third World, (2005).

3 *See* for example the overview by Bitton, which highlights HUMINT cases such as the torture ruling by the high court of justice. Raphael Bitton, In Law We Trust: The Israeli Case of Overseeing Intelligence, in Global Intelligence Oversight: Governing Security in the 21st Century 141 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016) [hereinafter Global Intelligence Oversight].

4 It should be noted, however, that there was privacy-centered public discourse in Israel during the first two decades of the 21st century. The still ongoing campaign against the government biometric database and the campaign against the "Big Brother Law" (the Communications Data Law, *see infra* note 20), the latter culminating in HCJ 3809/08 Association for Civil Rights in Israel v. Israeli Police (2012) (Isr.) (unpublished), non-official English translation available at https://versa.cardozo.yu.edu/opinions/association-civil-rights-israel-v-israel-police [https://perma.cc/PX9X-F85N][hereinafter ACRI]. For the campaign against the biometric database, *see* Michelle Spektor, *Imagining the Biometric Future: Debates Over National Biometric Identification in Israel*, 29 Science as Culture 100–126 (2020).

surveillance measures which were reserved for counterterrorism purposes to contain the spread of the virus[5] – was not adopted by any other western democracy.[6] Whereas routine ISA practices are shrouded in secrecy for operational reasons, the unique biopolitical nature of Covid-19 surveillance, coupled with the political stalemate within which Israel met the first wave of the pandemic, fostered a publicly open response by oversight actors and an open debate of the ISA's online surveillance measures.

This paper will first briefly introduce the SIGINT oversight ecosystem in Israel during routine, non-COVID-related times and its applicable legal framework. Then it shall provide an outline of the response of the various actors of the Israeli SIGINT oversight ecosystem to the ISA's coronavirus surveillance, and will evaluate its main product, the Authorization Law.[7] Then it shall proceed to analyze the performance of the SIGINT oversight ecosystem in the COVID-19 epidemic, and assess what lessons can be learned regarding its performance in routine, COVID-free times.

II. SIGINT AND METADATA ACQUISITION IN ISREAL

The use of Signals Intelligence measures by Israeli intelligence services can be traced back to the era predating the formation of the country, as Jewish resistance movements operated comprehensive wiretapping operations, listening in on British officials and Arab leaders.[8] However, Signals Intelligence, or SIGINT, is not just wiretapping: it is, rather, a plethora of intelligence disciplines deriving information from electronic devices. This paper shall use the terms "SIGINT" and "online surveillance" interchangeably, to refer to intelligence measures involving the interception, collection, and analysis of data originating from electronic

---

[5] Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), *Report*, 78, U.N. Doc. A/75/147 (July 27, 2020).

[6] For a comparative review of contact tracing measures, *see* Tehila Shwartz Altshuler & Rachel Aridor Hershkowitz, Digital Contact Tracing and the Coronavirus: Israeli and Comparative Perspectives (Foreign Policy at Brookings, 2020).

[7] 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) 5780-2020, SH 2816, 166 (Isr.), https://www.nevo.co.il/law_html/law01/502_316.htm [https://perma.cc/6RJJ-DU46] [hereinafter Authorization Law].

[8] Stacy Perman, Spies, Inc.: Business innovation from Israel's masters of espionage 33 (2005).

communications.[9]

This paper focuses on SIGINT practices by two internal government agencies: the ISA, Israel's domestic security service, whose missions are primarily counterterrorism and counterintelligence,[10] and the police – Israel's leading law enforcement agency. There are other intelligence agencies in Israel's intelligence community that are tasked with the collection of international SIGINT, such as the Mossad and Israel Defense Force's SIGINT Unit 8200. However, the SIGINT practices of both agencies are not directly regulated under any specific law.[11]

Government-sanctioned online surveillance laws tend to differentiate between the rules pertaining to the interception, collection, processing and retention of content data and those applicable to metadata (data about the communications). The rules applying to the interception, collection, processing and retention of metadata traditionally tend to be more lax than those applying to content data and allow government agencies much more leeway, based on a tacit assumption that metadata is less revealing than content data. The same applies to Israeli online surveillance laws.

However, as technology progresses, traditional legal categories may no longer apply. The Dutch online surveillance law, prior to its recent reform, differentiated between cable-bound communications and non-cable-bound communications (i.e., electromagnetic transmissions via antennae).12 It may be the case that in an era predating cellular phones, where most non-cable-bound communications were for military purposes, this distinction merited different rules. Nowadays, it is obsolete. Similarly, technological developments gradually erode the underlying assumptions supporting the different rules for content data and metadata, which are becoming as obsolete as the distinction between the contents of a letter and the address details of its recipient.

---

[9] Jeffrey T. Richelson, *The Technical Collection of Intelligence, in* Handbook of Intelligence Studies 105, 108–111 (Loch K. Johnson ed., 2006); Julian Richards, Signals Intelligence, in Routledge Companion to Intelligence Studies 84, 85–93 (Robert Dover, Michael S. Goodman And Claudia Hillebrand eds., 2014).

[10] § 7, General Security Service Law, 5972-2002, SH 1832, 172 (Isr.). [hereinafter ISA Law], non-official English translation available at https://knesset.gov.il/review/data/eng/law/kns15_GSS_eng.pdf.

[11] Omer Tene, *Systematic Government Access to Private-Sector Data in Israel: Balancing Security Needs with Democratic Accountability in* Bulk Collection: Systematic Government Access to Private-Sector Data 91, 106 (Fred H. Cate and James Dempsey eds., 2017).

[12] Quirine Eijkman, Nico Van Eijk & Robert Van Schaik, Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017 21–22 (2018).

Indeed, "metadata," which no longer signifies the few data points on the back of an envelope,[13] but rather a voluminous amount of information, has become more valuable to intelligence services than ever. [14] This can be attributed to the convenience of its analysis (content data requires either human analyst or sophisticated AI techniques to process in mass volumes, where automated processing of metadata is much easier) as well as to the prevalence of connected mobile devices, either cellular phones, smartphones or other Internet of Things (IoT) devices, which produce a constant electronic trail of their users' activities that may be less 'escapable' than contents data.[15]

Another distinction found in SIGINT law worldwide is one of purpose. The rules applying to online surveillance for national security purposes tend to be more lax than those applying to law enforcement purposes.[16] An underlying reason is that the different balance of interests involved in national security justifies looser rules for governments engaged in SIGINT practices that infringe upon individuals' privacy rights. Israel is no different.

The interception of the contents of electronic communications for law enforcement purposes (by Israeli police and other law enforcement agencies) and

---

[13] *See ex parte* Jackson, 96 U.S. 727 (1877).

[14] *See for example* Intelligence and Security Committee of Parliament, Privacy and Security: A Modern and Transparent Legal Framework (2015); European Commission for Democracy Through Law, Report on The Democratic Oversight Of Signals Intelligence Agencies, ¶48 (2015) [hereinafter Signals Intelligence Report]; Parliamentary Joint Committee on Intelligence and Security, Review of the Mandatory Data Retention Regime, ¶ 71 (2019). On privacy threats posed by location data and contact data in the context of COVID19 contact tracing, *see* Privacy Protection Authority, 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) 8 (2020) [hereinafter PPA Opinion No. 1], available in Hebrew only at https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus/he/privacy-shabak-coronavirus.pdf

[15] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

[16] *See* Asaf Lubin, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 Chi. J. Int'l 502 (2018). For U.S. cases, *see for example* United States v. Butenko, 494 F.2d 593 (3d Cir. 1974); United States v. Hung, 629 F.2d 908 (4th Cir. 1980). Recently, the German Constitutional Court ruled that the BND must still respect the fundamental right to privacy of individuals when engaging in mass surveillance of foreign intelligence. *See* Russell A. Miller, *The German Constitutional Court Nixes Foreign Surveillance*, Lawfare, May 27, 2020, https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance [https://perma.cc/AF7Z-JKQR].

for national security purposes (by the ISA) is governed by the Wiretap Law,[17] which contains different provisions for each purpose. While police wiretapping is subject to a judicial warrant by a senior district judge and is limited to felony offences,[18] ISA wiretapping is not reviewed ex ante by the court, but by the Prime Minister.[19]

Acquisition of communications metadata by law enforcement agencies is regulated under the Communications Data Law,[20] and by the ISA under the ISA Law.[21] Pursuant to the Communications Data Law, law enforcement agencies may apply for a judicial warrant ordering licensed telecommunications providers[22] to provide communications metadata (defined as "Location Data, Subscriber Data and Traffic Data, precluding the contents of electronic communications"),[23] for purposes of protection of human life, investigation, detection or prevention of offences or offenders (of misdemeanors or felonies),[24] or lawful forfeiture. The police can request a warrant for acquisition of future metadata, limited to no more than 30

---

17 Wiretap Law, 5739-1979, SH 938 p.188 (Isr.) [hereinafter Wiretap Law]. *See also* Omer Tene, *supra* note 11.

18 § 6, Wiretap Law, *supra* note 17. Israeli Law distinguishes between three types of offenses: Felonies (offenses which bear a penalty more severe than three years of imprisonment), Misdemeanors (offenses which bear a penalty more severe than three months and less than three years of imprisonment) and Transgressions (offenses which bear a penalty of no more than three months of imprisonment). *See* § 24, Penal Law, 5737–1977, LSI (Special Volume) (Isr.).

19 § 4, Wiretap Law, *supra* note 17.

20 Criminal Procedure Law (Enforcement powers – Communications Data), 5768-2007, SH 2122 72 (Isr.), https://www.nevo.co.il/law_html/law01/999_876.htm [https://perma.cc/2CXJ-XMY8] [hereinafter Communications Data Law].

21 § 11, ISA Law, *supra* note 10.

22 Section 1 of the Telecommunications Law 5742-1982, SH 1060 218 (Isr.) [hereinafter Telecommunications Law], defines Telecommunication as the "transmission, transmission or reception of signs, signals, writing, images, sounds or information using wire, radio, optic systems or any other electromagnetic system." Accordingly, Internet Service Providers (ISPs), Cellular services providers and providers of landline communication services all require a license under the Telecommunications Law.

23 § 1, Communication Data Law, *supra* note 20, further defines Location Data (location data of a device held by a subscriber), Subscriber Data (type of telecommunication service provided to the subscriber; the subscriber's name, address and identification number; the subscriber's payment method and details; the address at which the device used by the subscriber was installed; and data identifying the subscriber's device) and Traffic Data (communication's type, time, volume and length, as data identifying the source, target and any other intermediating devices used and data identifying the other party thereto).

24 *See* §6, Wiretap Law, *supra* note 17.

days following the date of issue of the warrant.[25] The constitutionality of the Communication Data Law, and in particular its infringement upon the right to privacy,[26] was challenged in *ACRI v. Police*,[27] where the High Court of Justice ruled that the provisions of the Communications Data law are to be construed narrowly, allowing for targeted collection of metadata only.

While metadata acquisition for law enforcement purposes is subject to ex ante judicial review, limited to particular types of metadata, and subject to temporal constraints, the rules governing the ISA's acquisition, processing and retention of metadata are different. Under Section 11 of the ISA Law, the Prime Minister is empowered to set rules that define certain categories of data as categories that the ISA requires to fulfill its statutory duties and that licensed telecommunication service providers are obliged to transfer to the ISA.[28] "Data" is broadly defined as "excluding the content of a conversation as defined in the Wiretap Law 1979-5739." Accordingly, all types of metadata (rather than the exhaustive list in the Communications Data Law) are capturable under the ISA Law. As with content data, the ISA Law does not require any ex ante judicial review of the service's metadata SIGINT practices. The use of data obtained under the ISA Law is subject only to the authorization of the ISA director. Such authorization may be given for periods not exceeding six months and renewed indefinitely.[29] The rules governing the use, retention, security and processing of such data are set by the Prime Minister,[30] and like all rules set under the provisions of the ISA Law, remain secret.[31] Certain provisions in the telecommunications law authorize the Prime Minister to order license holders to install or configure devices, or otherwise assist security authorities, including the ISA, to the extent it is required for the fulfilment of the authorities under the law.[32]

Section 11 of the ISA Law was enacted in 2002. It was added to the draft bill in between the first reading and the following readings of the law, and it didn't receive

---

[25] § 3(g) Communications Data Law, *supra* note 20. Compare with the Australian provisions of *Telecommunications (Interception and Access) Act 1979* (Cth) ss 175–176, 178–180B (Austl.).

[26] *See* § 7, Basic Law: Human Dignity and Liberty, 5752, SH 1391, 150 (Isr.). English translation available at https://www.knesset.gov.il/laws/special/eng/basic3_eng.htm [https://perma.cc/C7E5-BFHK].

[27] *ACRI*, *supra* note 4. *See* also Tene, *supra* note 11 at 102–103.

[28] § 11(b), ISA Law, *supra* note 10.

[29] § 11(d), ISA Law, *supra* note 10.

[30] § 11(e), ISA Law, *supra* note 10.

[31] § 19(a), ISA Law, *supra* note 10.

[32] § 13(b), Telecommunications Law.

much attention. The ISA director at the time, Avi Dicther, later said that "we tried to pass it under the radar screen, because it was potentially a very problematic section, even though that in 2002 not everybody fully understood the implications of metadata."[33] Indeed, it was not until the early days of the first wave of COVID-19 outbreak that the Israeli public became aware of "the Tool."

Within two weeks of Prime Minister Netanyahu's televised statement regarding the intended use of digital monitoring tools to track coronavirus carriers,[34] an exposé by Ronen Bergman and Ido Shvartztuch revealed the existence of "the Tool."[35] According to Bergman and Shvartztuch, during the nearly two decades since authorized to do so in the ISA Law, the service has been building up a voluminous database containing all the metadata transferred through Israeli telecommunication services.

Unlike the contested American metadata bulk collection under the Section 215 program,[36] the Tool collects more than mere call detail records (CDRs).[37] Rather, the Tool collects the widest possible definition of "Data" in the ISA Law, including CDRs, location data, [38] web browsing history, [39] technical router data (where available) [40] and possibly other categories of metadata from which valuable information could be extracted. This richness of the data types it collects renders

---

[33] Avi Dichter, speaking in College of Management, *A Decade to the ISA Law*, YouTube (Mar. 20, 2012), https://www.youtube.com/watch?v=BZ1sZqa0BR0 [https://perma.cc/D28Q-QZQR] (at minute 19, in Hebrew, translated by author).

[34] Judah Ari Gross, *Netanyahu sparks privacy scare with move to track corona patients' phones*, The Times of Israel (15.3.2020), available at https://www.timesofisrael.com/netanyahu-sparks-privacy-concerns-with-move-to-track-corona-patients-phones/ [https://perma.cc/W38U-SFZP].

[35] Ronen Bergman and Ido Shvartztuch, *The 'Tool', the ISA secret database has been collecting data on all Israeli citizens and knows: where were you, whom you have spoken to, and when* Yediot Aharonot (25.3.2020) [Hebrew] available at https://www.yediot.co.il/articles/0,7340,L-5701611,00.html [https://perma.cc/64JS-QQTK].

[36] *See* Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT ACT and on the Operations of the Foreign Intelligence Surveillance Court (2014).

[37] *See* 50 U.S.C. § 1861(k)(3) (2018).

[38] As can be inferred from its use for contact tracing.

[39] Bergman & Shvartztuch, *supra* note 35.

[40] *See for example* Ran Bar Zick, *Here's How to Protect Yourself Against Israel's Cyber Snooping* Haaretz (Nov. 12, 2020) (Isr.), https://www.haaretz.com/israel-news/tech-news/.premium-here-s-how-to-protect-yourself-against-israel-s-cyber-snooping-1.9303295 [https://perma.cc/6DBZ-L4VD].

the Tool much more effective than its American parallel, whose utility is doubted.[41] According to Bergman and Shvartztuch's account, the Tool has been successful in countless counterterrorism operations. Naturally, other agencies have sought access to the Tool over the years, which has rarely been granted.[42]

The ISA's immense database is allegedly safeguarded from misuse – however, there is very scarce evidence to support that assertion other than the assurances made by former ISA employees interviewed by Bergman and Shvartztuch. Despite the astounding public revelation by Bergman and Shvartztuch, a thorough Israeli public discussion of the Tool, echoing the ones held worldwide in the aftermath of the Snowden revelations, did not follow.[43]

III. THE ISRAELI SIGINT OVERSIGHT ECOSYSTEM

Oversight of intelligence and law enforcement agencies is an essential feature of democratic regimes.[44] Activities that infringe upon human rights are inherent to

---

[41] *See* discussion at Susan Landau & Asaf Lubin, *Examining the Anomalies, Explaining the Value: Should the* USA FREEDOM *Act's Metadata Program be Extended?*, 11 HAR. NAT'L SEC. J. 308 (2020).

[42] Before Bergman and Shvartztuch's revelation, the only public evidence of such an attempted access to the Tool's database was when the state comptroller requested the ISA to provide location tracking and cellular traffic data of certain senior security officials involved in a scandal investigated by the Comptroller's office. The state comptroller report bitterly complains the ISA's refusal to comply. *See* STATE COMPTROLLER OFFICE, REPORT ON THE "HARPAZ" AFFAIR 24–25 (2012) [Hebrew]. Bergman and Shvartztuch mention additional attempts to use the Tool for purposes other than those authorized by law, *see* § 6, ISA Law, *supra* note 10, including propositions to use the Tool to track illegal immigrants, or to monitor the communications of high-ranking officials (including the director of the Mossad and the head of the Military Intelligence) to monitor for potential leaks of plans to strike Iran), which were denied. Bergman & Shvartztuch, *supra* note 35.

[43] *See* Amir Cahane, *The (Missed) Israeli Snowden Moment* INT'L J. INTELLIGENCE & COUNTERINTELLIGENCE (forthcoming, 2021).

[44] On Intelligence oversight, *see* Hans Born, *Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices*, 3(4) CONNECTIONS: THE Q. J. 1 (2004); HANS BORN & IAN LEIGH, MAKING INTELLIGENCE ACCOUNTABLE: LEGAL STANDARDS AND BEST PRACTICE FOR OVERSIGHT OF INTELLIGENCE AGENCIES (2005) [hereinafter BORN & LEIGH]; WHO'S WATCHING THE SPIES?: ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY (Hans Born et al. eds., 2005); DEMOCRATIC CONTROL OF INTELLIGENCE SERVICES – CONTAINING ROGUE ELEMENTS (Hans Born & Marina Caparini eds., 2007); AIDAN WILLS, GUIDEBOOK: UNDERSTANDING INTELLIGENCE OVERSIGHT (2010); AMY ZEGART, EYE ON SPIES: CONGRESS AND THE UNITED STATES INTELLIGENCE COMMUNITY (2011); INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY (Hans Born et al. eds., 2011); OVERSEEING INTELLIGENCE SERVICES: A TOOLKIT (Hans Born & Aidan Wills eds., 2012) [hereinafter TOOLKIT]; Claudia Hillebrand, *Intelligence Oversight and Accountability*, *in* ROUTLEDGE COMPANION TO INTELLIGENCE STUDIES 305 (Robert Dover, Michael S. Goodman & Claudia Hillebrand eds., 2014); GENEVIEVE LESTER, WHEN SHOULD

these agencies,[45] and therefore mechanisms should be in place that ensure such infringements are limited by standards of proportionality and necessity. Proper oversight and control over intelligence and law enforcement services contribute to their accountability and to public trust,[46] whereas ineffective oversight ecosystem can serve as a veneer of legitimacy enabling unhindered misuse of power.[47] Regardless of the legality of mass surveillance practices,[48] the potential reach of modern SIGINT activities requires the special attention of policymakers to design proper oversight mechanisms, ensuring minimal invasion of privacy and adherence to standards of necessity and proportionality, as well as safeguards against potential mission creep or private misuse of surveillance powers. As the ISA has been siphoning bulk metadata into the Tool for nearly two decades, the importance of its oversight mechanisms cannot be overstated.

The Israeli SIGINT oversight ecosystem is basically its intelligence oversight array. At times it may focus on specific SIGINT matters. On the internal level, which some view as a primary guarantee against abuses of power,[49] we can only assume that members of the Israeli IC deploy basic automated measures and documentation to log and control internal access to restricted information. Former senior ISA employees claim that such measures and internal procedures are in place, and that the few occurrences of misuse of the Tool int its early days resulted in severe sanctions, so the contemporary organizational culture treats the Tool with

---

State Secrets Stay Secret?: Accountability, Democratic Governance, and Intelligence (2015); Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 Stan. J. Int'l. L. 69 (2015); Sarah Eskens, Ot van Daalen & Nico van Eijk, Ten Standards for Oversight and Transparency of National Intelligence Services (2015); Loch K. Johnson, Spy Watching: Intelligence Accountability in the United States (2018); Hugh Bochel, Andrew Defty &d Jane Kirkpatrick, Watching the Watchers: Parliament and the Intelligence Services (2014).

45 *See* Aidan Wills, Understanding Intelligence Oversight 31 (2007); European Parliament's Committee on Civil Liberties, Parliamentary Oversight of Security and Intelligence Agencies in the European Union 85 (2011); European Commission for Democracy Through Law, Report on The Democratic Oversight of the Security Services 4 (2015)[hereinafter Security Services Report]; Council of Europe Commissioner for Human Rights, Democratic and Effective Oversight of National Security Services 23–27 (2015) [hereinafter COEHR].

46 Monica den Boer, *Conducting Oversight, in* Toolkit, *supra* note 44, at 69, 83.

47 Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branches from Within*, 115 Yale L. J. 2314, 2321 (2006).

48 The ECtHR grand chamber ruling in the *Big Brother Watch* case is still pending (for the ruling of the first instance, *see infra* at 96).

49 Security Services Report, *supra* note 45, at 29.

"the fear of God."[50]

In addition to internal control mechanisms, Israeli law enforcement and security agencies have their own gatekeepers.[51] In the ISA, these are the legal advisor and the internal comptroller. The internal comptroller enjoys a special status, under a set of specific provisions in the ISA Law that strengthen the ISA comptroller's independence and jurisdiction further than comptrollers of other public authorities.[52] Unlike the comptroller, the legal advisor is not defined by statute; Pursuant to the aftermath of the 300 affair in the 1980s, the legal department of the service has been reorganized and its legal advisor became a part of the service's higher management.[53]

Executive oversight of SIGINT activities is performed on several levels. Wiretaps for national security purposes are subject to a ministerial ex ante authorization.[54] Although properly deliberated ex ante authorizations may be time-consuming,[55] the larger share of oversight activity is ex post and is mainly handled by the Attorney General's office.

The Attorney General (AG) in Israel is the "authorized interpreter of the law vis a vis the Executive."[56] This approach, different from the one prevailing in the U.S.,

---

[50] Bergman & Shvartztuch, *supra* note 35.

[51] Amir Cahane & Yuval Shany, Oversight of Online Surveillance in Israel 190–194 (2020) [Hebrew].

[52] § 13, ISA Law, *supra* note 10.

[53] Eli Bachar, The Role of the Legal Counsel in Security Agencies 66 (2013) [Hebrew].

[54] § 4, Wiretap Law, *supra* note 17. It should be noted that any wiretapping or other SIGINT practices of content acquisition whose targets are foreign are not subject to the provisions of the Wiretap Law. *See* CivA 4211/91 State of Israel v. Al Masri et al., 47(5) PD 636; Amir Cahane & Yuval Shany, Regulation of Online Surveillance in Israeli Law and Comparative Law 233–238 (2019) [Hebrew].

[55] *See for example*, the comment of UK's Independent Reviewer of Terrorism Legislation, David Anderson Q.C., that "my starting point was . . . the remarkable fact (at least to an outsider) that the Home Secretary routinely signs thousands of warrants per year, most of them concerned with serious and organized crime and the remainder with national security (principally terrorism)." David Anderson, A Question of Trust: Report of the Investigatory Powers Review 270 (2015). Note that pursuant to AdminA 4349/14 Association for Civil Rights in Israel v. Prime Minister, (2015) (Isr.) [Hebrew], the annual number of ministerial wiretap warrants in Israel remains secret, and therefore the actual ministerial load is also unknown.

[56] HCJ 4267/93 Amitai-Citizens for Proper Administration and Integrity v. The Government of Israel, 47(5) PD 441, 475 (Isr.) [Hebrew].

where the AG is a "hired gun,"[57] coupled with the Israeli AG's statutory oversight functions, allows the office of the AG to significantly influence the interpretation of Israeli online surveillance law and practices. The Prime Minister provides a quarterly report to the AG about wiretap authorizations.[58] Heads of security services must promptly report to the AG any emergency authorization to wiretap privileged communications which was given in lieu of judicial authorization, and the AG may revoke them.[59] Pursuant to the provisions of the ISA Law, the Director of the ISA reports quarterly to the AG of authorizations to use the Tool.[60] According to former senior ISA employees, "the quarterly meetings with the AG are thorough, we argue . . . it is a very excruciating experience for the ISA Director."[61] AG oversight of police SIGINT activities is more detailed. The police commissioner reports monthly to the AG regarding wiretap warrants.[62] The police commissioner must also promptly report to the AG any emergency authorization to wiretap in lieu of a judicial warrant, and the AG may revoke it.[63] Any application for a judicial warrant for wiretapping privileged communications is subject to the authorization of the AG.[64]

Parliamentary oversight of SIGINT in Israel is conducted through the Knesset's committees. General oversight of intelligence matters is under the purview of the Knesset's Foreign Affairs and Security Committee and is handled through its Intelligence and Secret Services Subcommittee (hereinafter: the Intelligence Subcommittee). The Intelligence Subcommittee is the statutory parliamentary oversight body of the ISA.[65] Pursuant to the ISA Law, the ISA director reports to the Intelligence Subcommittee on matters pertaining to the service's activities.[66] Regulations and rules the prime minister is authorized to set under the ISA Law are subject to the approval of the Intelligence Subcommittee.[67] Also, any executive

---

57 *See* Yoav Dotan & Michael R. Asimow, *Hired Guns and Ministers of Justice: The Role of Government Attorneys in the United States and Israel*, 19 ISRAEL L. REV. 1 (2016).

58 § 4(d), Wiretap Law, *supra* note 17.

59 *Id.* at § 5(b).

60 § 11(d), ISA Law, *supra* note 10.

61 Bergman & Shvartztuch, *supra* note 35.

62 § 6(f), Wiretap Law, *supra* note 17.

63 *Id.* at § 7(b).

64 *Id.* at § 9.

65 § 6, ISA Law, *supra* note 10.

66 *Id.* at § 12(b).

67 *Id.* at §§ 11(a), 21(b).

resolution authorizing the ISA to perform activities in an area that is not among its statutory core areas requires the Subcommittee's approval.[68]

The meetings of the Intelligence Subcommittee are confidential, unless it has decided otherwise.[69] Accordingly, little is known of the Subcommittee's activities; however it appears that its main concentration is on the operational efficacy of the Israeli IC, as well as budget review, rather than on matters of legal compliance and respect to human rights.[70] Many of the former members of the subcommittee interviewed by Bergman and Shvartztuch exhibited "a puzzling lack of knowledge and understanding" of the Tool.[71]

The parliamentary oversight of police activities is under the Internal Security Subcommittee, established in 2015. However, annual police wiretap reports and annual police metadata acquisition reports (when applicable) [72] are made to the Constitution, Law and Justice Committee.

The Knesset may also elect ad hoc inquest committees in matters pertaining to SIGINT. In 1950, following the Mapam wiretap scandal, such an ad hoc committee was established.[73] A parliamentary investigatory committee was established also in 2006, to "examine the legal framework and balances between the right to privacy and other public interests" and to "investigate the matter of wiretapping for crime prevention and detections (and not for national security) purposes."[74]

Ex ante judicial oversight of SIGINT is limited. While wiretaps and metadata acquisition for law enforcement purposes are subject to a judicial warrant, ISA wiretaps and metadata acquisition are not.[75] The inadmissibility of unlawful

---

[68] *Id.* at § 7(b)(6). *See also* HCJ 2109/20 HCJ 2019/20 Ben Meir v. Prime Minister (unpublished) ¶¶ 15–20 (2020) (Isr.), English translation available at https://versa.cardozo.yu.edu/opinions/ben-meir-v-prime-minister-0 [https://perma.cc/QL4M-RZZH] [hereinafter Ben Meir Ruling].

[69] § 6(b), ISA Law, *supra* note 10.

[70] *See* CAHANE & SHANY (2020), *supra* note 51, at 194–95.

[71] Bergman & Shvartztuch, *supra* note 35.

[72] § 6(f) Wiretap Law, *supra* note 17. Under §14, Communications Data Law, *supra* note 20, the minister responsible for the police shall annually provide statistics of metadata acquisitions under the law to the Knesset's Constitution, Law and Justice committee. Pursuant to its sunset provision, the section expired in 2012.

[73] *See supra* note 1.

[74] *Summary of Hearings on Wiretap Inquiry Before the Knesset Investigatory Comm.* (Jan. 26, 2009) [Hebrew].

[75] § 9, Wiretap Law, *supra* note 17, is a singular exception, under which ISA wiretaps of privileged communications are also subject to a judicial warrant.

wiretaps incentivizes its ex post judicial review.[76] However SIGINT acquired for national security purposes is rarely used in court, and if so it is presented ex parte. Accordingly, the Israeli court cannot apply random oversight of ISA wiretaps nor of ISA metadata collection through litigation.[77] Nevertheless through constitutional or administrative challenges, Israeli court can potentially have an important role as an oversight body – at a policy level – of all governmental online surveillance practices, as it did the in *ACRI v. Police* or the *Ben Meir* case.[78]

Another oversight actor is the State Comptroller. In the past, the State Comptroller's office has examined the use of police wiretapping.[79] The Israeli IC is also within its purview, [80] yet prior to the State Comptroller's 2020 interim special report on Israel's response to the COVID-19 crisis,[81] which examined the use of the ISA for contact tracing, no other review by the Comptroller of Israel's IC's SIGINT practices has been made public to date. Under Israeli law, the State Comptroller is highly independent and is free to select matter to review.[82] The law allows for parts of the State Comptroller's reports to remain secret for reasons of national security, or in order to avoid an impairment of Israel's foreign relations or its international trade. [83] The recommendations made by the State Comptroller are not legally binding.[84]

Although the Privacy Protection Authority (hereinafter: PPA and formerly known as ILITA (Israel Law and Information Technology Authority)), serves as Israel's independent data protection authority, the extent of its oversight over national security is undefined and limited. Prior to the coronavirus epidemic, no

---

[76] § 13 Wiretap Law, *supra* note 17.

[77] *Cf.* Mark Rumold, *Regulating Surveillance Through Litigation: Some Thoughts from the Trenches*, *in* The Cambridge Handbook of Surveillance Law 579, 580 (David Gray and Stephen E. Henderson eds., 2017).

[78] *ACRI*, *supra* note 4; *Ben Meir* Ruling, *supra* note 68.

[79] *See* Cahane & Shany (2020), *supra* note 51, at 204–06.

[80] *Id.* at n.894.

[81] State Comptroller's Office, The State of Israel Response to the Covid-19 Crisis - Special Interim Report (Oct. 2020) [Hebrew]. English version of the forward to the report is available at https://www.mevaker.gov.il/sites/DigitalLibrary/Documents/2020/COVID-19/2020-COVID-19-003-preface-EN.pdf [https://perma.cc/B66U-JEHU].

[82] §2 (b), Basic Law: The State Comptroller, 5748, SH No. 1237 p.30 (Isr.).

[83] § 17 (a), State Comptroller Law, 5718-1958 [Consolidated Version], SH 248 p. 92, (Isr.). English translation available at https://www.mevaker.gov.il/En/Laws/Documents/Laws-Compotroller-law.pdf, [perma.cc/TWK9-LJWU] [hereinafter State Comptroller Law].

[84] HCJ 9223/10 Movement for Quality Government in Israel v. Prime Minister ¶ 21 (2012) (Isr.) (unpublished).

statutory provision has given the PPA explicit oversight authority over security services, and the exceptions granted thereto in the provisions of Israel's privacy protection law[85] renders the PPA's theoretical SIGINT oversight mandate virtually moot.

Although not officially part of the SIGINT oversight ecosystem, civil society bodies and academia play a role, in Israel and everywhere else,[86] in keeping SIGINT practices in check. NGOs and academics alike provide the public with information regarding state SIGINT practices, and through litigation aim to shape its policies and legal framework. Civil society bodies were significant actors in the oversight ecosystem during the coronavirus outbreak.

Eskens et al.[87] offered a set of standards that will be used here to assess the Israeli SIGINT oversight ecosystem. First, before outlining them, another standard should be mentioned: a detailed legislative framework for SIGINT is a condition for effective oversight.[88] Basic democratic precepts mandate such a framework.[89] In addition to the precondition of a legal framework regulating state practices of online surveillance, there are other standards according to which an oversight ecosystem could be assessed:

---

[85] §§ 12(c), 13, 19, 23(B) Privacy Protection Law, 1981-5741, SH No. 1011 p. 128 (Isr.). Unofficial English translation available at https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf.

[86] *See* COEHR, *supra* note 45, at 59-60; EU Agency for Fundamental Rights, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, vol. I, at 12 (2015) [hereinafter FRA2015]; EU Agency for Fundamental Rights, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, vol. II, at 15 (2017) [hereinafter: FRA2017].

[87] Sarah Eskens, Ot van Daalen & Nico van Eijk, Ten Standards for Oversight and Transparency of National Intelligence Services (2015).

[88] *See* Lauren Hutton, *Overseeing Intelligence Collection*, *in* Toolkit, *supra* note 44, at 89, 100; Born & Leigh, *supra* note 44, at 19; FRA2017, *supra* note 86, at 11; Martin Scheinin (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism), *Rep. Pt. II: Compilation of Good Practices on Legal and Institutional Frameworks for Intelligence Services and Their Oversight*, ¶ 11, U.N. Doc. A/HRC/14/46 (May 17, 2010); Ian Leigh, *Overseeing the Use of Personal Data*, *in* Overseeing Intelligence Services, *supra* note 44, at 105, 122; Thorsten Wetzling, *Intelligence Governance in Post Cold-War Germany: A Steady Beat of Constant Trouble? in* Intelligence Oversight in the Twenty-First Century (Ian Leigh and Njord Wegge eds., 2019).

[89] *See* Scheinin, supra note 88, at ¶ 34; Born & Leigh, supra note 44, at 17, 41; Signals Intelligence Report, supra note 14 ; Electronic Frontier Foundation, Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance 27 (May 2014).

- ***Complete oversight*** – an effective oversight ecosystem must be institutionally, temporally, procedurally and substantively complete. Institutionally, the oversight ecosystem should be composed of internal and external actors, of which one should be a designated independent oversight body.[90] Internal and executive controls are insufficient.[91] Temporally, an oversight ecosystem should encompass ex ante, ex post and ongoing review.[92] Procedurally, oversight should attend to all aspects of the intelligence cycle: collection, retention, selection and examination and analysis. The substantive completeness of an oversight ecosystem requires attention to matters of legal compliance and operational efficacy, as well as human rights adherence and budgetary controls. The literature does not always mention all these as oversight purposes, and indeed oversight bodies tend to focus on two purposes or even a single one.[93]
- ***Independence*** – at least one oversight actor should be independent.[94] Independence – both institutional and political – influences the efficacy of many oversight bodies.[95] EU jurisprudence tends to rely on the judicial branch as an ex ante independent SIGINT oversight body.[96] In lieu of judicial oversight, the jurisprudence of the European Court Of Human Rights requires an independent oversight actor.[97]

---

[90] Eskens et al., *supra* note 44, at 35–36; Hans Born & Gabriel Geisler Mesevage, *Introducing Intelligence Oversight*, *in* TOOLKIT, *supra* note 44, at 3, 20; Scheinin, *supra* note 88, at ¶¶ 13, 32, 35.

[91] SIGNALS INTELLIGENCE REPORT, *supra* note 14, ¶ 186; *Id.* at ¶ 269. *See also* RICHARD A. CLARKE, ET AL., THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD, ch. 3 (2014).

[92] Eskens et al., *supra* note 44, at 35–36; Hans Born & Gabriel Geisler Mesevage, *Introducing Intelligence Oversight*, *in* TOOLKIT, *supra* note 90, at 20; Den Boer, *supra* note 45, at 84; PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE ¶ 20 (May 2014).

[93] Michelle Cayford et al., *Plots, Murders, and Money: Oversight Bodies Evaluating the Effectiveness of Surveillance Technology*, 33 INTELLIGENCE NAT'L SECURITY 999, 1011–1012 (2018).

[94] *See, e.g.*, Stuart Farson, *Establishing Effective Intelligence Oversight Systems*, *in* TOOLKIT, *supra* note 44, at 23, 43; Den Boer, *supra* note 44, at 79.

[95] FRA2017, *supra* note 86, at 11; European Commission For Democracy Through Law, *supra* note 89, ¶ 20; COEHR, *supra* note 45, at 11.

[96] Eskens et al., *supra* note 44, at 16, 19–20; Klass v. Ger., No. 5029/71, Eur. Ct. H.R., ¶ 56 (1978 Big Brother Watch v. U.K., Nos. 58170/13, 62322/14, & 24960/15, Eur. Ct. H.R., ¶¶ 16–26 (2018) (Koskelo, J., dissenting).

[97] Big Brother Watch, *supra* note 96, at 51; Iordachi v. Mold., No. 25198/02, Eur. Ct. H.R., ¶ 40 (2009); Dumitru Popescu v. Rom., No. 71525/01, Eur. Ct. H.R. (2007); Weber v. Ger., No. 54934/00,

- ***Ex ante oversight –*** Eskens et al. recommend that the SIGINT oversight ecosystem should be temporally complete, and they stress the importance of ex ante oversight.[98]
- ***Power to declare a measure unlawful and to provide for redress*** – effective SIGINT oversight requires that some of the oversight actors have the power to declare surveillance measures unlawful, or to refrain from authorizing the security and intelligence services to use it ex ante,[99] as well as providing individual redress. [100]
- ***Adversarial principle*** – as ex ante proceedings are often ex parte, any judicial or quasi-judicial oversight body authorizing ex ante online surveillance measures should incorporate adversarial positions. [101] Special advocates or amicus curiae may serve as such adversarial function.[102]
- ***Expertise*** – SIGINT oversight is a complex task that requires interdisciplinary knowledge and skills in national security, intelligence, legal and technological matters. Accordingly, the efficacy of an oversight ecosystem depends on the expertise of its personnel.[103] Without proper expertise, oversight actors that may even enjoy unrestricted access to data cannot critically examine it. Furthermore, expertise allows for stronger independence, as it reduces capture and deference.

Eur. Ct. H.R., ¶ 55 (2006); Rotaru v. Rom., No. 28341/95, Eur. Ct. H.R., ¶ 59 (2000); ANDERSON, *supra* note 55, at 271.

98 Eskens et al., *supra* note 44, at 37–38; *See also* BORN & LEIGH, *supra* note 44, at 37–42; Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), *Working Draft Legal Instrument on Government-led Surveillance and Privacy*, Art. 3(7)(b), U.N. Doc. version 0.7 (Feb. 28, 2018)

99 COEHR, *supra* note 45, at 11–13; Eskens et al., *supra* note 44, at 38; FRA2017, *supra* note 86, at 14.

100 *See* BORN & LEIGH, *supra* note 44 at 109; Craig Forcese, *Handling Complaints about Intelligence Services*, *in* TOOLKIT, *supra* note 44, at 181, 195; FRA2017, *supra* note 86, at 14; European Commission For Democracy Through Law, *supra* note 89, ¶ 26.

101 On the problematic position of national security courts, *see, e.g.*, Sudha N. Setty, *The United States*, *in* COMPARATIVE COUNTER-TERRORISM LAW 49, 59 (Kent Roach ed., 2015).

102 *See, e.g.*, European Commission For Democracy Through Law, supra note 89, ¶ 17. *See also* Foreign Intelligence Surveillance Act (FISA Act), 50 U.S.C. § 1803(i) (2018); Chad Squitieri, *The Limits of the FREEDOM Act's Amicus Curiae*, 11 WASH. J. L. TECH. & ARTS 197, 209–10 (2015); Ben Cook, *The New FISA Court Amicus Should Be Able to Ignore its Congressionally Imposed Duty*, 66 AM. U. L. REV. 539 (2017).

103 Den Boer, *supra* note 46, at 79.

- ***Sufficient Resources*** – budgets of intelligence services, and in particular those who develop and operate online surveillance measures, tend to be exorbitant, [104] while their oversight bodies are usually under-budgeted.[105] Proper allocation of funds, which reflects the extent of their mandate,[106] allows for effective oversight and fortifies both the expertise and the independence of oversight bodies.[107]
- ***Transparency*** – establishing public trust in the oversight ecosystem (and subject to its findings, in the IC) requires a degree of transparency. [108] Due to national security considerations, full disclosure of a finding is rarely possible, especially in operational matters,[109] but layered transparency could be introduced to SIGINT oversight ecosystems.[110]
- ***Access to information*** – effective oversight of intelligence and law enforcement agencies requires maximal access to information.[111] Full access to information should be the default rather than the exception,[112] but the breadth of information access should match the needs of the oversight mandate.[113]

---

[104] *See, e.g.*, Haim Levinson, *Israel Doubled the Budgets of Shin Bet and Mossad in 12 Years to $2.4 Billion*, HA'ARETZ (May 5,.2017), https://www.haaretz.com/israel-news/.premium-funding-for-shin-bet-and-mossad-doubled-in-12-years-1.5468640 [perma.cc/FFS9-CRQK]. During 2016, the UK defense minister announced that the secret services shall receive an overall increase of £2.5 billion GBP for the fiscal years 2016-2021. 618 Parl Deb HC (6th ser.) (2016) col. 17 (UK). The aggregate estimated budget of UK's SIGINT agency, GCHQ, was in the 1960s similar to that of the entire foreign affairs office. *See* Richard J. Aldrich, *Counting the Cost of Intelligence: The Treasury, National Service and GCHQ*, 128 ENG. HIST. REV. 596, 613 (2013). *See also* MARK M. LOWENTHAL, THE FUTURE OF INTELLIGENCE, ch. 4 (2017).

[105] Russell A. Miller, *Intelligence Oversight – Made in Germany*, *in* GLOBAL INTELLIGENCE, *supra* note 4, at 270; Kent Roach, *Review and Oversight of Intelligence in Canada*, *in* GLOBAL INTELLIGENCE OVERSIGHT, *supra* note 4, at 183.

[106] BORN & LEIGH, *supra* note 44, at 84.

[107] Eskens et al., *supra* note 44, at 39; FRA2017, *supra* note 86, at 11.

[108] Laurie Nathan, *Intelligence Transparency, Secrecy, and Oversight in a Democracy*, *in* TOOLKIT, *supra* note 44, 54.

[109] ANDERSON, *supra* note 57, at 306.

[110] Eskens et al., *supra* note 44, at 40. *See also* CAHANE & SHANY (2020), *supra* note 51, at 224–226.

[111] Eskens et al., *supra* note 44, at 40-41; FRA2017, *supra* note 86, at 12; COEHR, *supra* note 45, at 13.

[112] Nathan, supra note 108, at 64; Cannataci, supra note 98, at Art. 14.

[113] Den Boer, *supra* note 46, at 83.

The prerequisite of a proper oversight ecosystem – a detailed legislative framework of government online surveillance activities – is not fully met in Israel. Israeli online surveillance law is dated, thin, and shrouded in secrecy. [114] Furthermore, applying these standards to the Israeli SIGINT oversight ecosystem[115] shows that it is incomplete. The lack of a dedicated and independent expert oversight body is noticeable – judicial ex ante oversight of SIGINT activities in Israel is limited, and lack adversity, and there is no external continuous oversight of the routine operations of SIGINT measures. The State Comptroller – one of the only oversight actors that can lead thorough, in depth inquiries in matters pertaining to SIGINT –rarely uses its authority. Also noticeable is the lack of transparency, as the rules governing the Tool are confidential, and any parliamentary oversight activities thereof are secret by default. In the following we shall see how the Israeli SIGINT oversight ecosystem reacted to the government's resolution to authorize the ISA to use the Tool for contact tracing purposes during the coronavirus outbreak.

IV. COVID-19 IN ISREAL: COUNTERTERRORISM MEASURES TO WARD OFF A PLAGUE

A few weeks following the report of the first confirmed coronavirus carrier, who had come aboard a Diamond Princess cruise ship to Israel, [116] the number of coronavirus carriers increased exponentially.[117] Israel responded in mid-March by introducing a series of restrictive measures, including a general lockdown[118] and the use of location metadata for both epidemiological investigations and for

---

[114] *See also* CAHANE & SHANY (2019), *supra* note 54, at 274–79.

[115] For a full account, *see* CAHANE & SHANY (2020), *supra* note 51, at 228–47.

[116] *Israel confirms first Coronavirus case as cruise ship returnee diagnosed,* TIMES OF ISR. (Feb. 2, 2020), https://www.timesofisrael.com/israel-confirms-first-coronavirus-case-as-cruise-ship-returnee-diagnosed/ [perma.cc/77RW-U79B].

[117] *See Coronavirus disease 2019 (COVID-19) Situation Report – 55.* (Mar. 3, 2020). WHO, https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200315-sitrep-55-covid-19.pdf [perma.cc/NN2T-FNN2].

[118] Ayeal Gross, *Rights Restrictions and Securitization of Health in Israel During COVID-19,* BILL OF HEALTH (May 29, 2020), https://blog.petrieflom.law.harvard.edu/2020/05/29/israel-global-responses-covid19/ [perma.cc/D9VW-WMJZ]; Jeremie Bracka, *A Human Rights and Rule of Law Assessment pf Legislative and Regulatory Response to the COVID-10 Pandemic across 27 Jurisdictions,* BONAVERO INST. OF HUMAN RIGHTS (Oxford), Oct. 30, 2020, at 233–48 ("Israel"), https://www.law.ox.ac.uk/sites/files/oxlaw/bonavero_report_7_2020.pdf [perma.cc/2FYM-QMTA].

monitoring compliance of self-quarantined individuals.[119] The lockdown managed to contain the spread of the virus by May.[120] However, with no exit strategy, a second wave of the pandemic was soon to follow. In early July, Health Minister Edelstein stated that Israel was entering a second wave of COVID-19,[121] and in mid-September, a second general lockdown was in place.[122]

Israel entered the first wave of the pandemic with a caretaker government at a political stalemate, and three consecutive parliamentary elections held within a year did not resolve with the forming of a coalition.[123] However, the coronavirus crisis may have served as a catalyst – or an excuse – for an opposition party, Kahol Lavan, to form a coalition with reigning Likud party.[124] Negotiations between the parties took place during April, and by May 2020, the new government was sworn in.[125]

As early as March 9th, the Ministry of Health (MOH) requested that the ISA complement a singular epidemiological investigation with its technological

---

[119] Emergency Regulations (Location Data), 5780-2020 KT 8390 p. 772 (Isr.) [Hereinafter Police Coronavirus Regulations]; Emergency Regulations (Authorizing the General Security Agency to assist in the national efforts to reduce the spread of the Novel Coronavirus), 5780-2020 KT 8393 p. 782 (Isr.) [Hereinafter ISA Coronavirus Regulations, and together with the Police Coronavirus Location Data Regulations, Hereinafter Emergency Coronavirus Regulations]. *See also* Amir Cahane, *The Israeli Emergency Regulation for Location Tracking of Coronavirus Carriers*, LAWFARE (Mar. 21, 2020) https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-corona virus -carriers [perma.cc/3K57-PWKK].

[120] David Horovitz, *Netanyahu celebrates a victory over COVID-19; it marks his political triumph too*, TIMES OF ISR. (May 5, 2020) https://www.timesofisrael.com/netanyahu-celebrates-a-victory-over-covid-19-it-marks-his-political-triumph-too [perma.cc/WTD9-L6MX].

[121] Gali Weinreb, *"Edelstein: Comply with guidelines or face lockdown"* GLOBES (June 29, 2020), https://en.globes.co.il/en/article-edelstein-comply-with-guidelines-or-face-lockdown-1001333961 [perma.cc/3GEQ-P5CT].

[122] Amos Harel, *Israel Welcomes the New Year With a Heavy Heart and a Patchwork Lockdown*, HA'ARETZ (Sept. 18, 2020), https://www.haaretz.com/israel-news/.premium-israel-welcomes-the-new-year-with-a-heavy-heart-and-a-patchwork-lockdown-1.9165820 [perma.cc/Q5VR-AJKV].

[123] On the political crisis in Israel, *see* Itai Bar-Siman-Tov, *Covid-19 meets politics: the novel coronavirus as a novel challenge for legislatures*, 8 THEORY PRAC. LEGIS. 11, 30–31 (2020).

[124] Raoul Wootliff, *Netanyahu and Gantz said forming unity government; Blue and White collapses*, TIMES OF ISR. (Mar. 26, 2020), https://www.timesofisrael.com/gantz-and-netanyahu-said-forming-unity-government-blue-and-white-collapses [https://perma.cc/DHH3-R2FH].

[125] *Knesset approves establishment of Israel's 35th government; Prime Minister Netanyahu: "Unity government costs much less than fourth election,"* KNESSET NEWS (May 17, 2020), https://main.knesset.gov.il/EN/News/PressReleases/Pages/press1752020r.aspx [https://perma.cc/4J75-ETNH].

measures – the Tool.[126] The ISA, pursuant to an internal approval by its legal advisor, provided the MOH with a list of places where the patient stayed, as well as the details of individuals who had come into close contact with the patient. On March 11th, the ISA's legal advisor, in consultation with senior AG employees, agreed that for future requests, a "new procedure [would] be established, subject to the approval of the AG."[127] However, the next day the MOH requested the ISA's assistance regarding a second Coronavirus patient. The Director of the ISA approved the request. The following day, the ISA Director approved expanding the scope of the service's assistance to the MOH, subject to the approval of the AG. The position of the AG's office at the time was that the proper legal path to regulate the ISA's coronavirus surveillance was through a government resolution authorizing it.[128]

At these early stages, the core tenets of the ISA's coronavirus surveillance operation had already been established: the ISA would not provide MOH with direct access to the Tool, and would provide MOH only with designated information (the route of a coronavirus carrier and the persons with whom she has been in close contact rather than raw metadata); the ISA would refrain from any corona-related enforcement activities; and the ISA would not directly contact Israeli citizens.[129]

The government initially attempted to pass Resolution 4897, authorizing the ISA to assist in the national effort to reduce the spread of the novel coronavirus[130] pursuant to provisions of the ISA Law, which permits the ISA to undertake activities beyond its statutory defined remit, subject to a government resolution approved by the Intelligence Subcommittee.[131] The resolution authorized the ISA to "obtain, collect and process Technological Data in order to assist the Ministry of Health in an epidemiological investigation whose purpose is examining locations and routes of a confirmed coronavirus carrier or of individuals who may have contracted coronavirus as well as individuals with whom they have been in contact."[132]

---

[126] STATE COMPTROLLER'S OFFICE, *supra* note 81, at 97.

[127] *Id.*

[128] *Id.* at 99.

[129] *Id.* at 98–99.

[130] Government Res. No. 4897, Authorizing ISA to assist in the national effort to reduce the spread of the Novel Coronavirus, (Mar. 15, 2020). [Hebrew] https://www.law.co.il/media/computer-law/gov-corona-shbak.pdf [perma.cc/K3B8-2B78] [hereinafter Resolution 4897].

[131] *See supra* note 68.

[132] Resolution 4897, *supra* note 130, at § 1. Under a purpose limitation clause, the resolution authorized the ISA to use the undefined "Technological Data" only for the aforementioned purpose. Pursuant to the resolution, ISA's assistance to the MOH is subject to a request by either

However, Resolution 4897 did not pass. The Intelligence Subcommittee meeting to approve the Resolution was scheduled a few hours before the 22nd Knesset and its parliamentary committees were dissolved and the new Knesset was sworn in. The Intelligence Subcommittee refused to merely rubber-stamp Resolution 4897. While deliberating on Resolution 4897, however, the subcommittee was dissolved without reaching a conclusion or an approval of the Resolution. In lieu of parliamentary authorization, the government resolved to enact the Emergency Coronavirus Regulations, which authorized ISA to conduct Coronavirus surveillance for epidemiological investigations, and authorized the police to obtain communications metadata of quarantined individuals (specifically, their last cellular location) for monitoring purposes.[133] Within days, the High Court of Justice issued an interim order in the matter of *Ben Meir*, following an appeal by several NGOs and activists, under which the powers of the ISA under the Emergency Coronavirus Regulations was to be suspended within a few days unless a proper parliamentary oversight committee was established. The court also suspended the police's power to obtain communication data for quarantine enforcement under the Emergency Coronavirus Regulations until further notice.[134]

Following the reestablishment of some of the Knesset committees, including the Foreign Affairs and Security Committee and its Intelligence Subcommittee, the latter began a series of meetings to discuss the proper legal framework to authorize ISA Coronavirus surveillance as well as to draft a temporary amendment to the Communication Data Law that would authorize the police to obtain cellular location to monitor individual compliance with quarantine orders. Upon the expiration of the Emergency Coronavirus Regulations the Intelligence Subcommittee approved

---

the chief executive officer of the ministry, or the head of the public health services. ISA's response shall be made directly thereto and shall include only data directly required for the aforementioned purpose. The resolution explicitly stated that the authorization thereunder shall not authorize ISA to enforce quarantine order or monitor individuals who are under quarantine. The resolution was meant to stay in force for 30 days.

133 *See supra* note 119.

134 HCJ 2109/20 Ben Meir v. Prime Minister (Mar. 19, 2020) (Isr.) (unpublished, interim order). English translation available at https://versa.cardozo.yu.edu/sites/default/files/upload/opinions/Ben%20Meir%20v.%20Prime%20Minister.pdf [perma.cc/3LWZ-YF2W]. The police emergency powers were later to be reinstated by the high court of justice in an updated interim order. *See* HCJ 2109/20 Ben Meir v. Prime Minister (Mar. 24, 2020) (Isr.) (unpublished, interim order). English translation available at https://versa.cardozo.yu.edu/viewpoints/coronavirus-interim-order-update [perma.cc/3AYK-T9QV].

the amended Resolution 4950, effective for a 30-day period.[135] The draft amendment to the Communications Data Law was eventually shelved by the Minister for Internal Security.

The *Ben Meir* case was decided towards the end of effective period of Resolution 4950, and the High Court of Justice ordered that if the government sought to authorize ISA to engage in coronavirus surveillance, such authorization should be made through legislation. However, the court also allowed for further extensions of Resolution 4950 by "a few weeks," should the government pursue such a legislative process. Indeed, the Subcommittee allowed for several more extensions of Resolution 4950, while deliberating on further drafts of the authorization bill, the last two of which narrowed 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."[136] At the request of the ISA director, the government refrained from approving further extensions of Resolution 4950, which expired the second week of June.

Within a fortnight after the expiration of the Resolution 4950, the second wave of the pandemic ushered in a renewed sense of urgency. By June 25, the bill was approved by the cabinet and subsequently passed in a preliminary reading in the Knesset plenum. The bill was split in two: the main bill and temporary provisions. The latter were effective for 21 days to allow for immediate reauthorization of ISA coronavirus surveillance activities, while allowing for more thorough parliamentary deliberations on the main bill, which was eventually enacted on July 20 as 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 (hereinafter: the Authorization Law).

The Authorization Law authorizes the ISA to process Technological Data[137]

---

[135] Government Res. No. 4950, Authorizing ISA to assist in the national effort to reduce the spread of the Novel Coronavirus, (Mar. 31, 2020) https://www.gov.il/he/departments/policies/dec4950_2020 [hereinafter: Resolution 4950]. On Resolution 4950, *see* Amir Cahane, *Counterterrorism measures to counter epidemics: Covid-19 contact tracing in Israel*, BLOGDROITEUROPÉEN (Jul. 18, 2020), https://blogdroiteuropeen.com/2020/07/18/counterterrorism-measures-to-counter-epidemics-covid-19-contact-tracing-in-israel-by-amir-cahane/ [perma.cc/9RN3-ALQX].

[136] Omer Kabir, *Lawmakers Extend Spy Agency's Covid-19 Patient Tracking Program by Three Weeks*, CTECH (May 26, 2020), https://www.calcalistech.com/ctech/articles/0,7340,L-3827350,00.html [perma.cc/JM54-A6FV].

[137] Defined in Section 2 of the Authorization Law, *supra* note 7, as "Identification Data, Location Data and Call Record Data, excluding the contents of a call as defined in the Wiretap Law [*supra* note 17]." Identification Data are defined therein as "Name, ID number, telephone number and date of birth"; Location Data are defined as "The location data of a cellular phone device"; and "Call

regarding a patients[138] and individuals with whom they had been in close contact for the 14-day period preceding his diagnosis, and to provide MOH with the Patient's Location Data during said period and with the Identification Data, the time of contact with the Patient and the location of that contact, of individuals who have been in close contact with the Patient.[139] These powers are effective only pursuant to a government declaration of ISA authorization, which is subject to the approval of the Foreign Affairs and Security Committee.[140] Such declaration will be in effect not longer than 21 days.[141] Under the Authorization Law, the Health Minister must provide the public with civilian contact tracing technology, and promote its use.[142]

The Authorization Law includes several oversight mechanisms. The first one, mentioned above, is the government declaration of authorization. The legal instruments preceding the Authorization Law were set to expire within weeks of their promulgation and automatically authorized the ISA to partake in coronavirus surveillance. The Authorization Law, however, assumed that during its effective period of six months, continuous ISA surveillance would not necessarily be required. The declaration is a trigger mechanism which requires the approval of the Foreign Affairs and Security Committee.[143]

The provisions of the Authorization Law require both the ISA Director and MOH representative to provide the Foreign Affairs and Security Committee and the Attorney General's office with detailed weekly reports.[144] Unlike the reports made to the Subcommittee pursuant to the ISA Law,[145] these reports are not deemed

---

Record Data" are defined as "Incoming call phone number, Outgoing call phone number and the time of the call." Compare the definition of Technological Data to the inclusive definition of both Technological Data and of 'Data' in Section 11 of the ISA Law, *supra* note 10, as well as to the narrower language defining Metadata in the Communications Data Law, *supra* note 20.

138 Defined in Section 2 of the Authorization Law, *supra* note 7, as "a patient with a positive laboratory result to the novel coronavirus." Compare with the ISA Law, *supra* note 10, and *see Ben Meir* interim order, *supra* note 134, at ¶ 4(a).

139 § 5(a), Authorization Law, *supra* note 7.

140 § 3-3a, Authorization Law, *supra* note 7.

141 § 3(d), Authorization Law, *supra* note 7.

142 § 12a, Authorization Law, *supra* note 7. Under section 12a(b), such civilian contact tracing technologies are to be installed only voluntarily, subject to the user's consent.

143 Under section 3a of the Authorization Law, the Foreign Affairs and Security Committee may approve, shorten, or not approve the declaration's effective period. When the Committee decides not to approve a declaration, it expires within 24 hours.

144 § 19, Authorization Law, *supra* note 7.

145 § 19, ISA Law, *supra* note 10.

classified by default. MOH procedures under the Authorization Law are to be made public,[146] while ISA procedures thereunder are classified.[147]

A redress mechanism is also placed in the Authorization Law, which allows individuals who were identified by the ISA as persons who have been in close contact with a patient to appeal to the MOH. The MOH may request in such cases that the ISA reexamine the data which indicated that the appellant was in close contact with a coronavirus carrier, and must inform the appellant within 24 hours of its decision.[148] More than 63% of the appeals submitted under this procedure were granted, indicating the Tool's low efficacy in identifying coronavirus carriers.[149]

The Authorization Law also establishes a ministerial committee to reexamine the necessity of further use of ISA measures pursuant to its provisions. The ministerial committee, which includes the Prime Minister, the alternate Prime Minister,[150] and the Justice, Health, and Intelligence Ministers, as well as other ministers as the government may decide, considers the contribution of ISA activities to containing the spread of the pandemic and the existence of alternatives thereto, in light of the right to privacy. The ministerial committee is to be provided with the opinion of the PPA.[151]

---

146 § 10(c), Authorization Law, *supra* note 7.

147 § 9(b), Authorization Law, *supra* note 7.

148 § 8, Authorization Law, *supra* note 7.

149 Privacy Protection Authority, 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) 8 (2020) [hereinafter PPA Opinion No. 5], available in Hebrew only at https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus_5/he/5OPINION.pdf; The State Comptroller Interim reports states that the number of individuals who were notified that they were in close contact with patients is lower than the number of contacts provided by the ISA to the MOH, and therefore the error rate of the ISA is even higher. See STATE COMPTROLLER'S OFFICE, supra note 81, at p. 110. One of the possible reasons for the ISA's inaccuracy is its use of Call Record Data (as defined in the ISA under the Authorization Law), as there were complaints of individuals who were identified as having contacts with coronavirus carriers with whom they merely talked on the phone. Dikla Ahron Shafran, *Did you talk on the phone or SMSed with a confirmed patient? you might be sent to quarantine* KAN (November 2020) available at https://perma.cc/6F8B-CN4E.

150 See § 13a, Basic Law: Human Dignity and Liberty, 5761-1992, SH 1780 158 (Isr.). English translation available at https://www.knesset.gov.il/laws/special/eng/basic3_eng.htm [https://perma.cc/C7E5-BFHK].

151 § 12, Authorization Law, *supra* note 7. So far, the PPA produced seven such opinions: PPA Opinion No. 1, supra note 14; PPA Opinion No. 5, *supra* note 149; PRIVACY PROTECTION AUTHORITY, PPA OPINION IN ACCORDANCE WITH THE LAW TO AUTHORIZE THE ISA TO ASSIST IN THE NATIONAL

However, the ministerial committee inherently cannot be independent. It is part of the executive and as such perhaps plays the part of an internal oversight mechanism, but it may lack sufficient independence from changing political pressures to be an effective oversight measure. Furthermore, although the statutory reports allow the PPA to voice its opposing opinion against ISA coronavirus surveillance, their reports did not seem to have any influence on the recommendations of the ministerial committee or the continuous approvals by the Knesset's Foreign Affairs and Security Committee of government declarations under the Authorization Law.

V. THE OVERSIGHT ECOSYSTEM RESPONSE TO COVID-19

A. Internal and Executive Oversight

During the first wave of the pandemic, internal and AG oversight of ISA activities remained confidential. The AG office was central in the process of drafting the various legal instruments authorizing ISA activities – appearing before the Intelligence Subcommittee and during the first days of the pandemic – involved in authorizing the first two contact tracing operations. It appears that while the AG office opted for government authorization under section 7(b)(6) of the ISA Law, which entails partial parliamentary oversight by way of the Intelligence Subcommittee's approval, it did allow the exceptional authorizations by the ISA

Effort to Contain the Spread of the Novel Coronavirus (Temporary Provisions) 8 (2020) [hereinafter PPA Opinion No. 2], available in Hebrew only at https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus_2/he/privacy-shabak-coronavirus-2.pdf; Privacy Protection Authority, 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) 8 (2020) [hereinafter PPA Opinion No. 3], available in Hebrew only at https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus_3/he/privacy-shabak-coronavirus-3.pdf; Privacy Protection Authority, 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) 8 (2020) [hereinafter PPA Opinion No. 4], available in Hebrew only at https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus_4/he/privacy-shabak-coronavirus_4.pdf; Privacy Protection Authority, 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) 8 (2020) [hereinafter PPA Opinion No. 6], available in Hebrew only at https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus-6/he/opinion6.pdf; Privacy Protection Authority, 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) 8 (2020) [hereinafter PPA Opinion No. 7], available in Hebrew only at https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus-7/he/777777777777777.pdf

Director for contact tracing analysis of the first two COVID-19 patients without any such scrutiny. It is unknown whether internal AG discussion raised concerns of the potential mission of the ISA's Tool. Prima facie, however, the AG office allowed it to occur, perhaps mitigating it by preferring parliamentary involvement in the rulemaking process.

B. Judicial Oversight

As mentioned above, there is no ex ante judicial oversight of ISA SIGINT measures. Accordingly, ISA COVID-19 surveillance reached the High Court of Justice only through a petition from civil society bodies that at first challenged the constitutionality of the Coronavirus Emergency Regulations, and later challenged the legal framework set under the 4897 Resolution.

The interim order in *Ben Meir* reflected a position favoring parliamentary oversight: the court conditioned continued ISA authorization under the Coronavirus Emergency Regulations on relevant oversight parliamentary committees being formed.[152] Two months into the COVID-19 outbreak, the *Ben Meir* ruling continued emphasizing parliamentary supremacy. It focused on the Israeli non-delegation doctrine,[153] under which the ISA may be authorized to engage in coronavirus location tracking only through primary legislation, rather than by a government resolution (albeit subject to the approval of a parliamentary subcommittee) [154]or emergency regulations (that are not enacted by the Knesset).[155] The *Ben Meir* ruling did pay tribute to privacy considerations, albeit as dicta,[156] while its holding focused on the proper interpretation of the term "National Security" within the context of the "mission creep" clause of the ISA Law.

Subsequent to the enactment of the Authorization Law, it was challenged in the High Court of Justice. [157] Currently the case is pending, yet it seems that the court

---

[152] Ben Meir interim order, *supra* note 134, at ¶ 4(a).

[153] Elena Chachko, *"The Israeli Supreme Court Checks COVID-19 Electronic Surveillance"* LAWFARE. (5.5.2020). [https://perma.cc/E7N7-A5F3].

[154] § 7(b)(6), ISA Law, *supra* note 10.

[155] *See* § 38-39, Basic Law: Human Dignity and Liberty, 5761-1992, SH 1780 158 (Isr.). English translation available at https://www.knesset.gov.il/laws/special/eng/basic3_eng.htm [https://perma.cc/C7E5-BFHK].

[156] *See* Ben Meir ruling, *supra* at 68, at ¶¶ 35–42.

[157] HCJ 6732/20 Association for Civil Rights in Israel v. Knesset (2020) (Isr.). The preceding challenges to the Authorization Law were dismissed on procedural grounds. For the Israeli petitions, *see* HCJ 5746/20 Association for Civil Rights in Israel v. Knesset (2020) (Isr.). For an overview of the petition *see* Adalah, ACRI, ADALAH, PHRI & PRIVACY ISRAEL PETITION ISRAELI

is not comfortable with the ongoing use of the ISA measures for coronavirus, following an interim order demanding to know why should the ISA coronavirus surveillance is restricted to cases where patients refuse to cooperate with epidemiological investigations.[158] The court further demanded the respondent explain why the MOH is not upholding its statutory duties to promote alternative civilian technologies.[159]

C. Parliamentary Oversight

Two days following the Prime Minister's public statement regarding the intended use of digital counterterrorism measures to identify COVID-19 carriers,[160] the Intelligence Subcommittee adjourned to discuss the government request to approve Resolution 4950. However, that meeting was terminated before reaching a resolution, because the Knesset dissolved and a new parliament was sworn in.

The first round of hearings by the newly-formed Intelligence Subcommittee was devoted to drafting the amended Resolution 4987. At its early stages, the Subcommittee expressed a tepid position: they would approve the amended Resolution 4987 for a limited 30-day period, but further approval would be conditioned upon thorough and detailed evidence prepared by an expert government body explaining that no alternatives were available.[161] This stance gradually eroded as the outbreak progressed and the Knesset coalition was formed. By the end of the first effective period of Resolution 4987, the Subcommittee's chairperson, MK Ashkenazi, was to become the Foreign Minister in the forming coalition. MK Ashkenazi did not insist on any evidence regarding available

---

Supreme Court: Repeal law authorizing Shin Bet to track citizens with COVID-19, https://www.adalah.org/en/content/view/10085 [https://perma.cc/9HFS-JC2R]. For a critique of the procedural dismissal of these petitions and others See Adam Shinar, *Why decide if you can avoid?* Dyoma (Sept. 6, 2020) [Hebrew] [https://www.dyoma.co.il/%D7%97%D7%95%D7%A7-%D7%95%D7%9E%D7%A9%D7%A4%D7%98/463-%D7%9C%D7%9E%D7%94-%D7%9C%D7%94%D7%9B%D7%A8%D7%99%D7%A2-%D7%90%D7%9D-%D7%90%D7%A4%D7%A9%D7%A8-%D7%9C%D7%94%D7%AA%D7%97%D7%9E%D7%A7 [https://perma.cc/MV7J-BMH4].

158 HCJ 6732/20 Association for Civil Rights in Israel v. Knesset (November 11, 2020) (Isr.) (Unpublished, Interim Order). *See also* Yonah Jeremy Bob, *High Court puts the heat on Shin Bet coronavirus surveillance*, The Jerusalem Post (Nov. 11, 2020). English available at https://www.jpost.com/israel-news/high-court-puts-the-heat-on-shin-bet-coronavirus-surveillance-649389 [https://perma.cc/UME3-3EZF].

159 § 12, Authorization Law, *supra* note 7.

160 *Supra* note 34.

161 Intelligence and Secret Services Subcommittee Minutes, Knesset Security and Foreign Affairs Committee, protocol no. 3, March 30, 2020, at 40.

alternative measures to the ISA coronavirus surveillance[162] and approved the extension of the effective period for a week in order to allow the government to pursue a legislative path to ISA authorization, per *Ben Meir*.[163] As MK Ashkenazi left the Subcommittee for greener pastures, the incoming chairperson, MK Hauser, also from a coalition party, exhibited an approach more tolerant of the government's position, favoring ISA surveillance and less insistent on the development and promotion of civilian alternatives.

Thematically, the Subcommittee's discussions tended to focus on the necessity of the Tool for containing the spread of the pandemic, rather than assessing its proportionality. Even in the early stages of discussion, members of the committee had at times drifted into general questions of Israel's COVID-19 strategy. During April 2020, the Subcommittee also engaged in several discussions pertaining to the drafting of an amendment to the Communications Data Law, authorizing the police to obtain location data for quarantine monitoring purposes, even though oversight of the police forces is not within the Subcommittee's purview.[164] At some point during the second wave of the pandemic, the discussions were steered towards MK Hauser's initiative to reduce the length of the quarantine period from 14 to 10 days. Even if this step could have increased the Israeli public's overall compliance with quarantine orders, its relevance to the extension of the declaration period under the Authorization Law is indirect at best.

The initial expertise gap of the Intelligence Subcommittee members, as reported by Bergman and Shvartztuch,[165] was bridged in a series of confidential Subcommittee hearings with ISA members, at least one of which was attended by an academic expert.[166] Nevertheless, some statements made in the early meetings, and the change made in the Subcommittee's membership pursuant to the formation of the government, indicate that its members were not fully informed at

---

[162] Intelligence and Secret Services Subcommittee Minutes, Knesset Security and Foreign Affairs Committee, protocol no. 8, April 30, 2020, at 13–14.

[163] Ben Meir ruling at ¶ 34.

[164] Furthermore, under the proposed amendment, modeled after the Police Coronavirus Regulations, the police were empowered to obtain Location Data directly from licensed telecommunication providers, with no involvement of the ISA.

[165] *Supra* note 71.

[166] Intelligence and Secret Services Subcommittee Minutes, Knesset Security and Foreign Affairs Committee, protocol no. 1, March 26, 2020, at 36.

all times. [167] Changing statistical indices [168] could have also contributed to information gaps and confusion of policymakers.

The Subcommittee, however, did open to the public most hearings pertaining to ISA coronavirus surveillance from its first discussions on the matter, contrary to the default rule classifying the Intelligence Subcommittee's hearings. Furthermore, the Subcommittee invited civil society bodies and privacy experts to participate in its meetings (although during the October-November meetings on the extension of the declaration period they were hardly encouraged to voice their opinions.)[169] Nevertheless, despite its rare public openness, and even rarer moment of independence,[170] the Subcommittee appeared to be influenced by the political shifts in the background, as well as by its chairperson's agenda. The Subcommittee further lacked initiative. For example, the initiative to narrow the scope of ISA's surveillance to "particular and unique cases"[171] came from the ISA, rather from the parliamentary overseers.

D. The Privacy Protection Authority

Initially, the PPA was not involved in the authorization of the first two instances of ISA coronavirus surveillance. According to the schedule of the acting head of the PPA, only after Prime Minister Netanyahu's televised statement regarding the intention to employ digital counterterrorism means to contain the pandemic did the management of the PPA discuss the matter.[172] Although its schedule indicates that the PPA was preoccupied with ISA coronavirus surveillance matters as early as mid-March, the PPA did not make any public statement on the matter, nor did PPA

---

[167] Intelligence and Secret Services Subcommittee Minutes, Knesset Security and Foreign Affairs Committee, protocol no. 3, March 30, 2020, at 20.

[168] *See for example* the letter by Privacy Israel to the Foreign Affairs and Security committee, pointing out that the computation methodology of certain indicators in the MOH reports was changed, thereby presenting results favorable to the continued use of ISA surveillance. Privacy Israel, *Examining the ISA Tool's effectiveness: quantitative indicators* (Letter from Privacy Israel to the Foreign Affairs and Security committee, (Jan 1, 2020) [Hebrew] (on file with the UNH Law Review).

[169] Omer Kabir, *"Experts' boycott Knesset hearings on ISA surveillance: we are silenced"* CALCALIST (Nov. 11, 2020) [Hebrew] available at https://www.calcalist.co.il/internet/articles/0,7340,L-3875031,00.html [https://perma.cc/7CCV-JB3R].

[170] *Supra* at note 161.

[171] *Supra* at note 136.

[172] Schedule of the acting PPA Head, Dr.Shlomit Wagman, Jan.–June 2020. [Hebrew] available at https://www.odata.org.il/dataset/4bfcdd69-b76f-4bb8-9f45-afc6b9694565 [https://perma.cc/9CEN-BJBU].

representatives attend the early hearings of the Intelligence Subcommittee. Towards the end of April, the PPA was invited to join the Subcommittee only after the Justice Minister received a letter from a group of privacy experts protesting the PPA's absence from the hearings.[173]

Gradually, the PPA's voice was heard. Following the suggestion of the Defense Minister to source a private company to develop an Israeli "health scoring" system,[174] the PPA published a critical survey of credit scoring systems.[175] In late May, the PPA published a survey of COVID-19 digital monitoring systems, which concluded that the ISA measures were the most privacy-infringing measures available.[176]

As of mid-July, under the Authorization Law, the PPA provided the Ministerial Committee with its opinion regarding the ISA authorization. In its seven opinions (as of December 2020),[177] the PPA consistently raised an opposing voice to the continuing use of the ISA's measures for Coronavirus location tracking, doubting its efficacy,[178] calling for the promotion and development of alternative civilian measures. In its opinions under the Authorization Law, the PPA also expressed its opposition to any involuntary surveillance measure.[179] The PPA further noted no correlation had been found between the use of technological measures (voluntary or involuntary) in other jurisdictions and the spread of the pandemic.[180]

Nevertheless, although the PPA is granted a statutory role, it appears to be that of a mere privacy advocate. The PPA lacks any effective teeth – it cannot veto the

---

173 Omer Kabir, *"Privacy Experts to Government: there are those who want that the right to privacy will not interfere with the corona crisis"* CALCALIST (Apr. 22, 2020) [Hebrew] available at https://www.calcalist.co.il/internet/articles/0,7340,L-3809882,00.html [https://perma.cc/CA82-8FH8].

174 Yasmin Yablonko, *"Bennett plans using NSO to rate individual virus exposure"* GLOBES (March 30, 2020) [https://perma.cc/YKH3-KBBS].

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

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

177 *Supra* note 151.

178 *See* PPA Opinion No. 4 at 1; PPA Opinion No. 5 at 2; PPA Opinion No. 7 (referring to State Comptrollers Interim Report, *supra* note 81).

179 PPA Opinion No. 5 at 1, discussing § 12a(b), Authorization Law, *supra* note 7.

180 PPA Opinion No. 7 at 4.

authorization of ISA surveillance like the Foreign Affairs and Security Committees. Any research prepared for the PPA opinions appears to rely on publicly available sources, and accordingly it may be the case that the PPA lacks any actual oversight powers that provide it with better access to information than civil society bodies. However, the PPA opinions, like the State Comptroller's interim reports, may influence other oversight actors as they serve to reinforce legal or policy arguments in court or in parliamentary deliberations.

E. The State Controller

As the first wave of the pandemic ended, the State Comptroller Matanyahu Englman stated in parliament that his office would review ISA coronavirus location tracking as part of its annual review.[181] The report, published in late October, befitting the approach of Mr. Englman,[182] carefully avoided any direct accusations,[183] yet the information it provided was sufficient to suggest that ISA coronavirus surveillance was inefficient.[184]

During July and until mid-August 2020, the State Comptroller's Office investigated the ISA's coronavirus surveillance activities. In addition to performing an audit on the ISA, the Comptroller's Office also engaged with the ministry of Intelligence and the PPA.

The part of the report that was made public[185] analysed the effectiveness of the Tool by offering two different indices – SNR (signal to noise ratio) and BDA (battle damage assessment). According to the report, the overall BDA, which is the ratio between the number of confirmed patients examined by the ISA and the number of confirmed patients discovered by the ISA, was 28.5%–for nearly every three patients

---

[181] Intelligence and Secret Services Subcommittee Minutes, Knesset Security and Foreign Affairs Committee, protocol no. 3, March 30, 2020, at 40.

[182] Jacob Magid "*Officials in state comptroller's office accuse him of defanging their audits*" THE TIMES OF ISRAEL (Jan. 1, 2020) available at https://www.timesofisrael.com/officials-in-state-comptrollers-office-accuse-him-of-defanging-their-audits/ [https://perma.cc/WKZ4-ZP6S].

[183] *"Israel Needs a Different State Comptroller"* HA'ARETZ (Oct. 27, 2020) available at https://www.haaretz.com/opinion/editorial/israel-needs-a-different-state-comptroller-1.9267366 [https://perma.cc/B4ZV-FSAW].

[184] Yaniv Kubovich, *"Watchdog: Tracking by Israel's Security Service Is Invasive, Ineffective in COVID Fight"* HA'ARETZ (Oct. 26, 2020) available at https://www.haaretz.com/israel-news/.premium-watchdog-tracking-by-shin-bet-is-invasive-ineffective-in-covid-fight-1.9263930 [https://perma.cc/8GSQ-6VKP].

[185] *See* STATE COMPTROLLER'S OFFICE, *supra* note 81 at 91. Pursuant to Section 17 of the State Comptroller Law, the Knesset's control committee subcommittee decided not to make public of certain parts of the state comptroller's special interim report.

referred to the ISA, the Tool detected one other coronavirus carrier.[186] The report further stated that the SNR, which is the ratio between the number of patients detected by the ISA and the overall number of contacts detected as associated with them, was 3.5% – out of more than 25 individuals that the ISA identified to have been in close contact with a coronavirus carrier, only one was eventually found to be a confirmed carrier of the virus. The report compared the SNR of the ISA measures to the SNR of the still ongoing traditional epidemiological investigations, which was much higher (nearly 24%). Despite this data, the report did not draw any direct conclusion as to the efficacy of the Tool.

Another revelation made by the report is that ISA location tracking activity for the first two coronavirus patients referred to by the MOH was undertaken without any legal basis, based on the authorization of the ISA legal advisor and the ISA Director. [187] The report also made note of several incidents in which data was not properly handled.[188] The matter of alternative civilian measures was also discussed, and the the report called on the MOH and the Ministry of Intelligence to promote such measures.[189] The report recommended that the Ministerial Committee remap the process and form a recommendation if, under current circumstances, considering the efficacy of ISA activities and potential privacy harms, there was sufficient reason to continue relying on ISA coronavirus surveillance or if other alternatives based on thorough epidemiological investigations might be preferable.[190]

F. Civil Society

As an oversight actor, civil society was engaged in several fronts during the coronavirus epidemic. First, it researched and informed public debate on ISA coronavirus surveillance and its civilian alternatives;[191] second, civil society bodies and activists were the initiators of the *Ben Meir* case, and the subsequent proceedings against the Authorization Law; and, finally, civil society bodies, activists and privacy experts took an active role in the Intelligence Subcommittee's hearings (at first), providing parliamentarians with opinions and background information.

---

186 State Comptroller's Office, *supra* note 81, at 105.

187 State Comptroller's Office, *supra* note 81, at 97–99.

188 State Comptroller's Office, *supra* note 81, at 115–17.

189 State Comptroller's Office, *supra* note 81, at 118–22.

190 State Comptroller's Office, *supra* note 81, at 123.

191 *See* Altshuler & Hershkowitz, *supra* note 6.

The protest letter, as mentioned above, rendered the PPA more involved in the ISA coronavirus public discourse, and contributed to its inclusion in the parliamentary subcommittee's discussions.[192] A bill drafted by civil society bodies and privacy experts proposed a framework promoting alternative measures to ISA surveillance.[193] Albeit not fully acknowledged by the Intelligence Subcommittee, the bill appears to have influenced the drafting of the Authorization Law. Section 12a, added pursuant to the civil society suggested bill, provides that the Health Minister must provide the public with civilian contact tracing technology, and promote its use.

However, during late November, civil society bodies and experts regularly invited to the Intelligence Subcommittee committee hearings regarding ISA coronavirus surveillance notified the Chairperson that they would be boycotting the hearings. Their letter claimed that the Subcommittee had been avoiding a serious discussion about ISA coronavirus surveillance, and would rather drift into matters outside its purview, such as shortening the mandatory quarantine period, while also neglecting the discussion of the failure of Israel's contact tracing app, Hamagen 2.0.[194] The letter also claimed that during the previous two months, civil society experts had been no more than extras, hardly heard in the Subcommittee hearings held via Zoom.[195]

Overall, civil society organizations, activists and privacy experts were crucial to the oversight ecosystem during the coronavirus pandemic, as they were an independent voice promoting privacy considerations and offering policy alternatives. Their activities served as a catalyst and prompted other oversight bodies – such as the PPA and the courts - to act.

G. Revisiting Eskens et al.

The framework offered by Eskens et al. and expanded on in part 3 of this paper can be used to examine the performance of the Israeli SIGINT oversight ecosystem during the coronavirus crisis, as was described above.

---

192 *See supra* note 173.

193 Ronit Sella, *"Israel: a bill proposes alternatives to ISA tracing of Covid-19 patients"* LAW.CO.IL (July 13, 2020) available at https://www.law.co.il/en/news/2020/07/13/civilian-alternatives-to-isa-tracing-of-covid-19-patients/ [https://perma.cc/A7F7-FYJH].

194 On the failure of Hamagen 2.0, *see* Josh Mitnick, "How Israel's COVID contact tracing app rollout went wildly astray" CIO (July 11, 2020) available at https://www.cio.com/article/3591570/how-israels-hamagen-contact-tracing-app-rollout-went-wildly-astray.html [https://perma.cc/PJ5M-7FFE].

195 Kabir, *supra* note 169.

- ***Detailed Legislative Framework*** – the absence of a detailed legislative framework regulating Israel's SIGINT practices allowed for extended deliberations by the parliamentary oversight body – the Intelligence Subcommittee – which took an active part in designing the legal frameworks ruling the ISA coronavirus location tracking. Had there been a more detailed legislative framework, coronavirus surveillance would have been addressed as a routine (albeit under unique circumstances) oversight issue.[196]
- ***Complete oversight*** – while the SIGINT oversight ecosystem in Israel remained institutionally incomplete during the coronavirus pandemic, lacking a designated independent SIGINT, some improvements are noticeable in the narrow context of ISA coronavirus surveillance. An appeal mechanism was introduced, and the temporal completeness of the Israeli oversight ecosystem has improved as well – as the continuity of the parliamentary and executive oversight of ISA coronavirus surveillance was enhanced under the Authorization Law, which requires both MOH and ISA to provide them with weekly reports.
- ***Independence*** – as mentioned above, Israel's oversight ecosystem lacks an independent actor. The parliamentary Subcommittee did exhibit a modicum of independence at the early stages of its response to the government's intention to utilize the ISA for coronavirus surveillance, yet this independence fluctuated and eroded with the political backdrop. Additionally, as much as the High Court is indeed independent, it is neither a dedicated or continuous oversight body, and its tendency to delay the post *Ben Meir* appeals against the Authorization Law[197] may be attributed to external political pressures.
- ***Ex ante oversight.*** Although ex ante oversight is less relevant to location tracking,[198] the declaration mechanism in the Authorization law could be deemed as providing the Knesset's Foreign Affairs and Security Committee

---

[196] This hypothetical scenario depends on the nature of the theoretical legislative framework therein, and of any changes to the existing oversight ecosystem it might introduce. However, the downside of elaborate SIGINT legislation are the technical language often used inside which uses terms of art which serves to obscure the actual surveillance practices from lawyers and policymakers alike. *See* 231 Parl. Deb. HC (2014) col. 89 (UK); Maria Helen Murphy, Surveillance and the Law: Language, Power and Privacy (2018).

[197] *Supra* note 157.

[198] *See infra* at part 6.

with some measure of ex ante authorization powers.[199]

- ***Power to declare a measure unlawful and provide redress***. The High Court of Justice did use its powers to order the police and the ISA not to use their powers under the Emergency Coronavirus Regulations. The appeal mechanisms under the Authorization Law may not provide full redress to individuals quarantined based on the ISA's Tool, but it offers them a way to cancel the quarantine order.
- While the ***Adversarial principle*** is more relevant in the ex ante context, its instances in ex post oversight and policymaking regarding ISA COVID-19 surveillance were evident. However, the rare openness of the Intelligence Subcommittee and its initial inclusion of civil society bodies allowed the latter to express an adversarial position, thereby mitigating potential capture of the subcommittee members.[200] The *Ben Meir* case was handled with both parties present in the court room, rather than in ex parte proceeding (which are more common in ex ante cases).
- The increased ***Transparency*** was most discernible in the Israeli SIGINT oversight ecosystem during the coronavirus epidemic. The oral arguments in *Ben Meir* were streamed online in real time, as were most of the Intelligence Subcommittee's hearings. Unlike the 1950s two-line report by the Israeli's Knesset ad hoc Parliamentary Subcommittee for the Matter of Secret Wiretapping Devices and Secret Party Services,[201] the Intelligence Subcommittee hearings generated a plethora of reports and documents offering opinions and data to an extent previously unavailable. However, the quality of some of the data, as a measure of the ***Access to information*** standard set by Eskens et. al, was at times less than optimal. Reports made by various stakeholders included conflicting information, which at times caused policymakers to compare apples with oranges. Changes in data computations were introduced in a manner meant to present the utility

---

[199] Compare with the British 'double lock' system in the UK Investigatory Powers Act 2016. *See* MURPHY, *supra* note 196, at 64; Byron Karemba, *The Investigatory Powers Bill: Introducing Judicial Authorisation of Surveillance Warrants in the United Kingdom – Putting the 'Double-Lock' in Focus (Part I)*, UK CONSTITUTIONAL LAW BLOG (March 22, 2016) available at https://ukconstitutionallaw.org/2016/03/22/byron-karemba-the-investigatory-powers-bill-introducing-judicial-authorisation-of-surveillance-warrants-in-the-united-kingdom-putting-the-double-lock-in-focus-part-i/ [https://perma.cc/MFS2-9DPY].

[200] *See* MURPHY *supra* at 196, at 93–97; Hendrik Hegemann, *Toward 'Normal' Politics? Security, Parliaments and the Politicisation of Intelligence Oversight in the German Bundestag*, 20 THE BRITISH J. OF POL. & INT'L RELATIONS 175, 179 (2018).

[201] *Supra* note 1.

and efficacy of the ISA tool in a better light.[202]

An overall assessment of the Israeli SIGINT oversight ecosystem during the coronavirus epidemic shows increased levels of transparency and procedural adversity. However, the low level of independence exhibited by the main oversight actors may indicate that the increased levels of transparency and procedural adversity were supported by ephemeral conditions unique to the biological nature of the surveillance target, and, as the next part suggests, that these slight improvements in the oversight ecosystem might not apply to routine SIGINT practices. Furthermore, given that the Israeli IC kept on using SIGINT measures for national security purposes during the coronavirus outbreak, it would be safe to assume that these changes were compartmentalized to apply only to coronavirus surveillance matters.

VI. COVID-19 AS A TEST CASE?

A side effect of the coronavirus was piercing the veil of secrecy surrounding Israel's SIGINT oversight ecosystem. However, some of the circumstances that allowed this rare glimpse may not apply to the routine workings of the SIGINT oversight ecosystem.

First, the bio-political nature of the ISA's coronavirus location tracking differs greatly from the routine ISA surveillance for counterterrorism and counterintelligence purposes. As coronavirus location tracking is not terror-related, nor is it political, there is hardly any reason for secrecy. There is no adversary whose awareness of being under surveillance might bring about operational risks.

Second, since no one is immune to COVID-19, there is a certain likelihood that overseers and policymakers will also contract the virus and be subjected to surveillance. This possibility may contribute to enhanced sensitivity regarding privacy matters, whereas it is highly unlikely that overseers or policymakers shall become targets of counterterrorism surveillance. Accordingly, the willingness to sacrifice rights and liberty for national security purposes is greater when the "other" is expected to pay the toll.

Third, targeted coronavirus surveillance, or even untargeted coronavirus surveillance might not be significantly improved by judicial authorization. Whereas surveillance for law enforcement purposes – and, at times, for national security purposes – requires a certain estimate of human culpability, the standards applying to coronavirus are not legal but medical. It has become, therefore, the subject matter

202 *Supra* note 169.

of experts.[203] Therefore, the question of ex ante review of online surveillance is rendered moot within the context of coronavirus surveillance, while it is one of the most salient lacunae in the Israeli SIGINT oversight system.

Additionally, the SIGINT oversight ecosystem during the COVID-19 pandemic was mainly concerned with policy-level oversight. The focus of the Subcommittee and to some extent the High Court in *Ben Meir* were the necessity of , and the safeguards and controls required for, ISA coronavirus surveillance. Although some policy determinations, especially those attempting to assess the efficacy of ISA surveillance, attempted to be data driven, the day-to-day working of ISA surveillance was rarely reviewed.

Even before the coronavirus, Cohen claimed that in Israel the executive branch overtook the Knesset, and that parliamentary oversight in Israel was ineffective.[204] The COVID-19 outbreak significantly marginalized parliaments worldwide vis-a-vis the executive branch.[205] However, due to the political circumstances in Israel upon the outbreak, the Intelligence Subcommittee was in a position of independence before a coalition formed. Once the coalition formed, the dominance of the executive was reestablished and, accordingly, the Subcommittee repeatedly approved extending the ISA's authorizations. While the source of these circumstances is not COVID-19, it is highly unlikely to resurface in a future SIGINT-related crisis.

Although the coronavirus presented a set of unique circumstances for the Israeli SIGINT oversight ecosystem, some lessons can still be carried forward. The coronavirus affair demonstrated the importance of transparency. Transparency, which fosters democratic accountability of intelligence services in general, also allows oversight to flourish. Information is, after all, the life blood of oversight. Transparent information flow (subject, of course, to reasonable confidentiality) to the public is the precondition to the work of civil society bodies, whose contribution to the oversight ecosystem throughout the covid-19 epidemic was of immeasurable importance. However, transparency is not the statutory default but the exception, and during ordinary, COVID-free times the Intelligence Subcommittee, the ISA and the AG retain strict confidentiality as to SIGINT and its oversight.

---

[203] On the rule of technocrats during the pandemic (in a parliamentary context) *see* Eric L. Windholz, *Governing a pandemic: from Parliamentary Sovereignty to Autocratic Technocracy"* 8 The Theory and Practice of Legislation 93–113 (2020).

[204] *See* Amichai Cohen, the Constitutional Revolution and Counter-Revolution [Hebrew] (2020).

[205] Elena Griglio, *"Parliamentary Oversight Under the Covid-19 Emergency: Striving Against Executive Dominance"* 8 The Theory and Practice of Legislation 49–70 (2020).

Despite the important role played by civil society and academia in creating feedback loops inside the oversight ecosystem (through litigation or the call for strengthening the position of the PPA, which in their turn contributed to an independent discourse), a dedicated expert SIGINT oversight body cannot be replaced thereby. I have suggested elsewhere that an independent SIGINT oversight agency, modeled after the British Investigatory Powers Commissioner (IPCO), will be able to fill in the gaps in the Israeli oversight ecosystem.[206] The suggested independent Israeli SIGINT commission, which would (similar to IPCO) have quasi-judicial powers to authorize online surveillance warrants, could not be downplayed in the coronavirus scenario to the position of the PPA as a toothless privacy advocate, as it would have the authority to veto coronavirus surveillance.

While the Authorization Law did introduce some enhanced oversight mechanisms, their scope is limited to the contact tracing practices of the ISA. It is unlikely that the Authorization Law will transform into a wider legal reform of the Israeli SIGINT laws and oversight ecosystem, neither pursuant to the pending decision in *Association for Civil Rights in Israel v. Knesset*,[207] nor following a parliamentary initiative. However, the lessons derived from the COVID-19 epidemic illustrate the importance of transparency, expertise and independence for the SIGINT oversight ecosystem in ordinary times, as well as the significance of the inclusion of well-informed civil society organizations in the deliberative process.

206 Cahane & Shany (2020), *supra* note 51.

207 *Supra* note 157.