Contact Tracing Technologies in Israel: How to Erode Trust and Alienate People

Eran Toch

Policy Paper | November 2020

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

*German-Israeli Tech Policy Dialog Program*

*Rethinking Privacy and Mass Surveillance in the Information Age*

# Imprint

**Contact Tracing Technologies in Israel:**

*How to Erode Trust and Alienate People*

**Author**

**Dr. Eran Toch**

**Project Lead**

**Giorgio Franceschini | Milena Grünewald**

Heinrich Böll Foundation, Foreign and Security Policy Division, Berlin

Email: [giorgio.franceschini@boell.de](mailto:giorgio.franceschini@boell.de); [milena.gruenewald@boell.de](mailto:milena.gruenewald@boell.de)

**Oz Aruch**

Heinrich Böll Foundation Tel Aviv

Email:oz.aruch@il.boell.org

**Polina Garaev**

Israel Public Policy Institute (IPPI)

Email: polina@ippi.org.il

**About the Project**

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

**About the German-Israel Tech Policy Dialog Program**

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

**Please cite as follows:**

Toch, E. (2020). *Contact Tracing Technologies in Israel: How to Erode Trust and Alienate People*. Policy Paper Series “Rethinking Privacy and Mass Surveillance in the Information Age”. Israel Public Policy Institute and Heinrich Böll Foundation

Release date: November 2020

License: Creative Commons (CC BY-NC-ND 4.0), https://creativecommons.org/licenses/by-nc-nd/4.0

The views expressed in this paper are those of the authors and do not necessarily reflect the views of the Heinrich Böll Foundation and/or the Israel Public Policy Institute.

**Contents**

Executive Summary…………………………………………………………………………………………

1. Introduction ……………………………………………………………………………………….
2. Contact Tracing Technologies ……………………………………………………………………
3. Typologies of Applications and History ………………………………………………………….
   1. HaMagen Contact Tracing App ………………………………………………………………..
   2. GSS Cellular Tracking ……………………………………………………………………….
4. Privacy Analysis of the Technologies ………………………………………………………………
5. Human Behavior and Deployment …………………………………………………………………..
   1. Installations of Contact Tracing Apps ……………………………………………………….
   2. Privacy and Deployment …………………………………………………………………..
   3. Mitigating Errors …………………………………………………………………………..
6. Conclusions ………………………………………………………………………………………..

Endnotes …………………………………………………………………………………………………

# Executive Summary

Contact tracing technologies can potentially help health organizations and governments stop the spread of COVID-19 by finding and isolating people who have been in contact with coronavirus carriers. However, they also pose serious threats to privacy, as they are based on identifying and analyzing contacts between individuals. Also, their effectiveness depends heavily on people's behavior, particularly on the proportion of people who install and use the technology. This behavior may be influenced by people's perceptions of the technologies' utility or by their perceptions of the potential privacy threats that may originate from personal information collection. The fast pace of the deployment of these technologies puts citizens into “privacy shock”: the need to form an attitude immediately regarding a new privacy threat and to determine the utility/privacy tradeoff.

This report analyzes two contact tracing technologies that were introduced by the Israeli government during the early days of the coronavirus crisis: a privacy-preserving mobile application (“HaMagen”) and a technology based on Israel’s General Secret Service (“The Tool”). The two technologies provide a natural experiment that can test how the characteristics of surveillance technologies shape user’s “privacy shock”. We examine how these characteristics affect the way people interact with these technologies, as well as their overall success. In this case study, we first analyze the technologies’ architectures and the privacy threats they pose. We then point to the possible effects that privacy concerns have on the success of contact tracing technologies.

# Introduction

The novel coronavirus has led to a global pandemic that seriously threatens the health and well-being of billions of people. Given the absence of a vaccine or a cure, health authorities turn to non-medical interventions, such as case isolation and quarantine, social distancing, and hygiene measures to reduce virus transmission. The pandemic puts pressure on governments to develop new policies, mechanisms, and technologies, in ways that would have been deemed quite inconceivable before the pandemic. In this report, we are focusing on a central technology: Contact Tracing Technologies (CTTs), which identify people who might have been exposed to COVID-19 positive people and aims to isolate them before they spread the virus further.

The coronavirus crisis has highlighted how different countries and democratic regimes are responding. Countries differ in terms of the type of technologies they develop, the way they frame and regulate the technologies, the way citizens react and behave with the given technology, and the overall success of the technology. This case study of contact tracing in Israel is fascinating for several reasons. First, Israeli citizens interacted with two types of contact tracing technology: voluntary and involuntary. This allows us to analyze a “natural experiment” in which we can assess how people respond and form their points of view regarding a new tracking technology. We can also take advantage of this natural experiment to help us understand a phenomenon we will call “**privacy shock**”: a situation in which citizens have to respond immediately to a new privacy challenge. This point of view can be helpful in designing and evaluating large scale technological public health interventions during this global pandemic. More generally, the case study can help policymakers recognize important aspects of surveillance technologies that are sometimes overlooked: specifically, the negative externalities of surveillance, which are not always apparent, leaving the discourse murky and unfocused. The concept of a “privacy shock” can help us focus our attention and isolate various effects that are mostly hidden.

# Contact Tracing Technologies

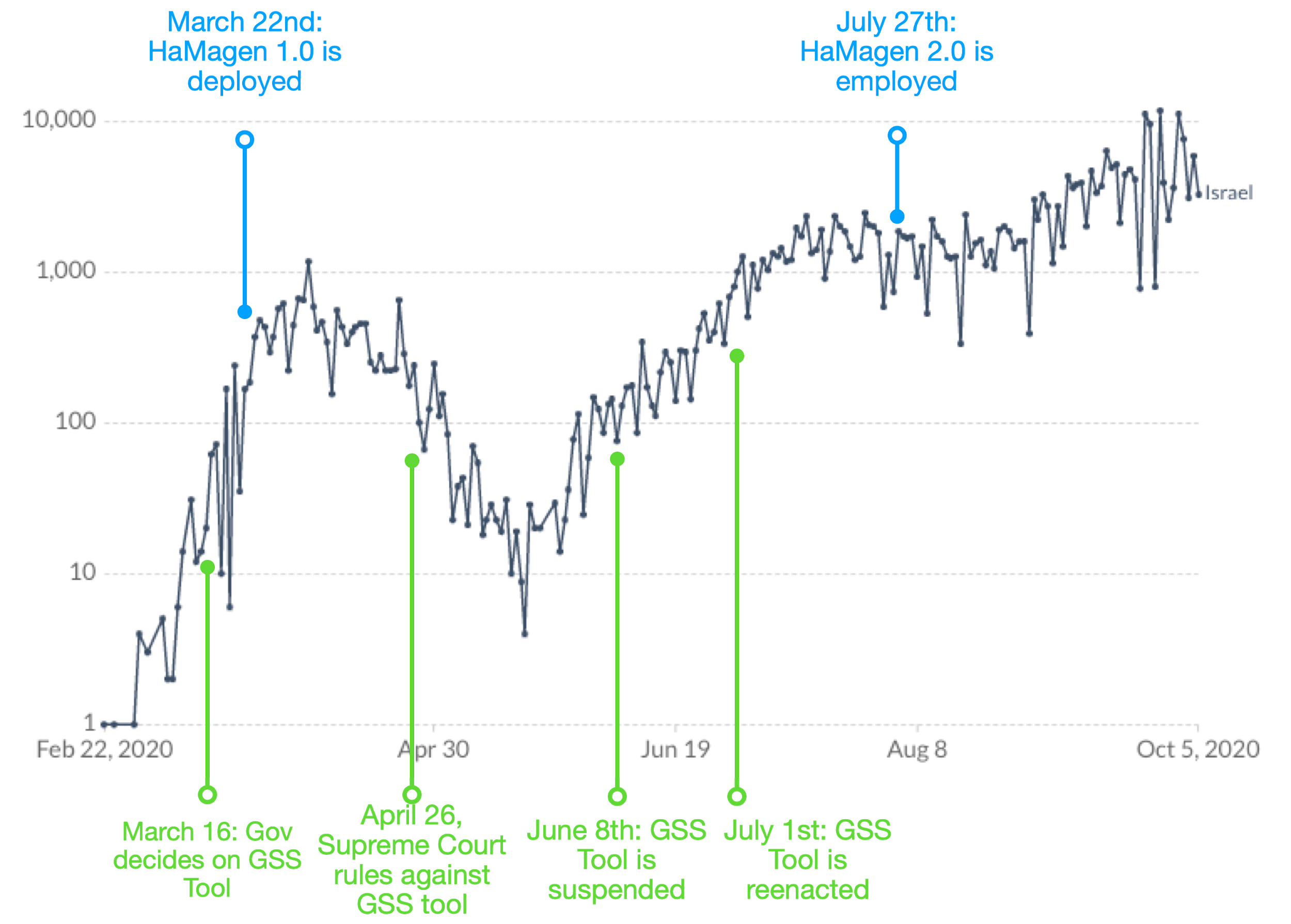
A key non-medical intervention in stopping the spread of the novel coronavirus is the use of Contact Tracing Technologies (CTTs), which can quickly identify infected people (usually those who have symptoms), leverage tracking technology to gather information about recent contacts, and follow up with and quarantine those contacts to interrupt further transmission of the epidemic.[[1]](#endnote-1) Contact tracing is not new. It has been used to prevent the spread of epidemical diseases such as HIV, Ebola, and tuberculosis. The widespread nature of the COVID-19 crisis and the explosion of mobile smartphone adoption have led to intense efforts to design and deploy CTTs that are unprecedented in scale and sophistication.

The effectiveness of CTTs is under serious debate. Simulation-based studies have shown that CTTs can be effective in epidemiological models, with the potential of bringing epidemics under control if contacts of positive cases are isolated quickly enough.[[2]](#endnote-2) If the adoption rates are high enough, the combination of isolation and contact tracing/quarantining can bring R, the effective reproduction number, below 1 and, therefore, effectively control the epidemic.[[3]](#endnote-3) However, other analyses have shown that CTT interventions can reduce the number of transmissions with any uptake in the adoption rates while minimizing the impact on the rest of the population.[[4]](#endnote-4)

# Typologies of Applications and History

Many countries have developed and deployed various types of CTT.[[5]](#endnote-5) CTTs can be distinguished by how centralized they are, how much control they provide to the user, how they infer contacts between people, and how they handle personal information privacy. The most crucial distinction can be made between voluntary and non-voluntary designs. Most CTTs rely on voluntary participation, in which individuals need to download and install an app on their phones. Singapore's TraceTogether App relies on Bluetooth Low Energy (BLE)[[6]](#endnote-6) and local matching with official data about the locations of infected people. Some countries employ involuntary CTT designs. For example, South Korea[[7]](#endnote-7) and Israel[[8]](#endnote-8) use cellular traces from mobile carriers for tracking contacts. Apple and Google announced a Bluetooth-based CTT platform to be embedded in both iOS and Android operating systems, based on proposals for privacy-preserving CTTs.[[9]](#endnote-9) CTTs also differ in how they utilize the results. Some CTTs provide personal notice to users if they were near a confirmed infected individual (e.g., HaMagen; Google/Apple infrastructure). Another CTT, the Chinese Tencent app, restricts access to public areas.[[10]](#endnote-10)

Figure 1. Timeline of Implementation of Contact Tracing Technologies in Israel



*Milestones in the application of the two Israeli contact tracing technologies, juxtaposed on a graph of the number of new daily COVID-19 cases in Israel (on a logarithmic scale).*

## The HaMagen Contact Tracing App

In Israel, two contact tracing technologies have been implemented during the coronavirus pandemic: HaMagen (“the Shield”), a contact tracing application that was developed by the Ministry of Health, and a centralized cellular tracking which is operated by Israel's General Security Services (GSS). HaMagen was deployed on 22 March 2020.[[11]](#endnote-11) The first version, HaMagen 1.0, was based on ongoing local storage of users' location data, and local matching with official data about infected people's whereabouts. In the second version, HaMagen 2.0, deployed on 28 July,[[12]](#endnote-12) BLE support was added (but without using the Google/Apple protocol).

Figure 2: Architecture of the HaMagen Contact Tracing App

A close up of a sign

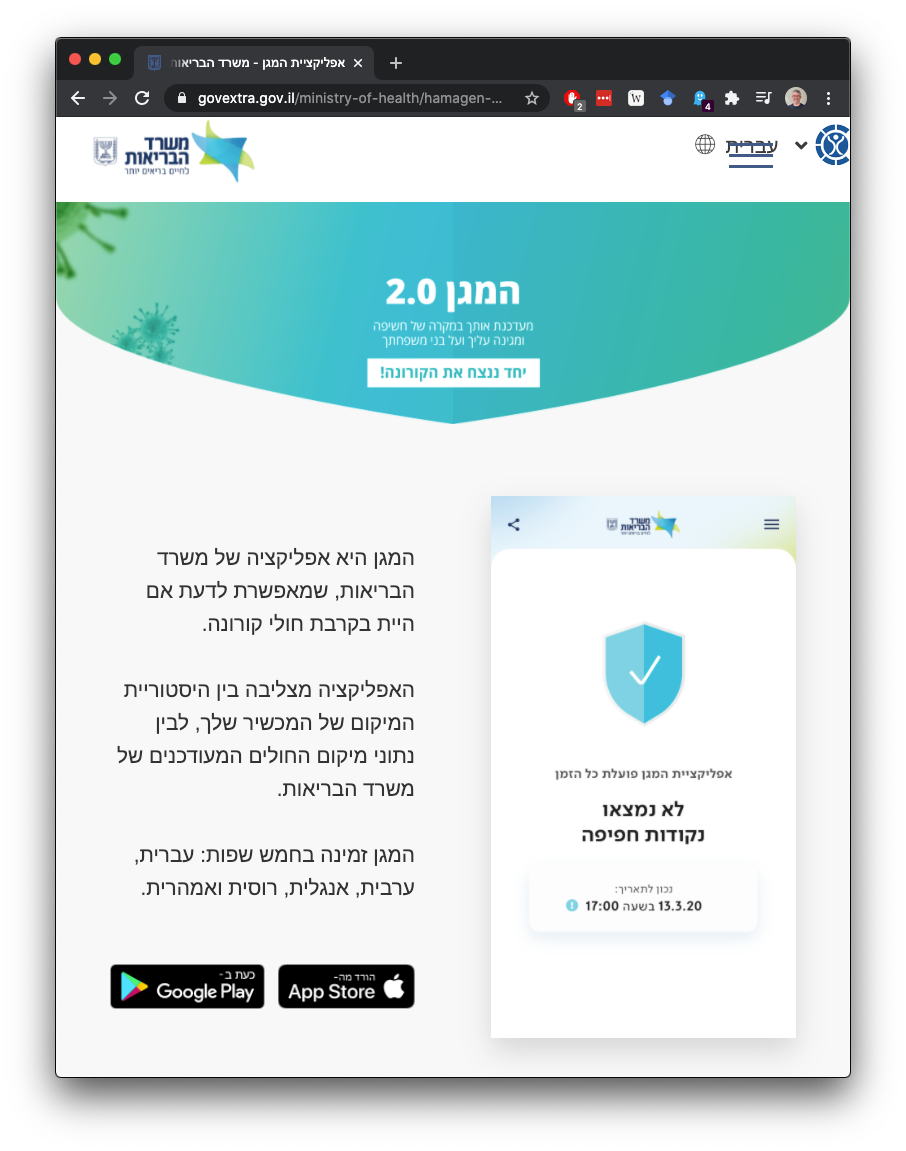
Description automatically generated

Person A is our hypothetical user, and person B is a user that was identified as COVID-19 positive.

The contact tracing process in HaMagen can be divided into two stages: ongoing data collection and handling of epidemiological isolation. Under normal circumstances, the app collects information about the visited locations (using the mobile phone’s GPS and the WiFi positioning capabilities). Beginning with HaMagen 2.0, the app also receives messages from nearby phones through BLE (Bluetooth Low Energy). These messages contain randomly assigned IDs, and theoretically cannot be used to identify the nearby phone.

When an individual is identified as COVID-19 positive, they are briefed by an epidemiological investigation team. The locations they visited within the past two weeks are fed into a simple centralized server. If the individual has the HaMagen app installed, then they can decide to upload the locations and BLE messages to the server. Each app regularly retrieves the list of locations and message IDs. If there is a match with the locations or the messages received from a COVID-19 positive person, the user is notified and is asked to contact the health authorities.

Image 1. HaMagen Website and Screenshot of the App



Links to download the app were available on the Health Ministry Website, but it was not widely promoted in the media. Even with limited exposure, about 1.5 million people have downloaded it, and 400,000 people have uninstalled it, according to the Health Ministry’s response to a Supreme Court appeal.[[13]](#endnote-13) However, the second version was only downloaded by 22,000 people, and most users have uninstalled the first version.[[14]](#endnote-14)

## GSS Cellular Tracking

The second technology, dubbed “The Tool,” is based on centralized cellular tracking operated by Israel’s General Security Services (GSS). This technology is based on surveillance of cellular companies' data centers of all of the cellular phones operating in Israel.[[15]](#endnote-15) According to news sources, it routinely collects information from cellular companies and identifies the location of the phones of all Israeli citizens through cellular antenna triangulation and GPS data, but only makes use of it with a court order.[[16]](#endnote-16) The Israeli government authorized the use of this technology for contact tracing on March 16, 2020, claiming that the GSS is the only entity that has the means to quickly and efficiently deploy contact tracing technology.[[17]](#endnote-17) Due to petitions to Israel’s high court, the government suspended The Tool on June 8, but then reinstated it under a broader legislation on July 1, 2020.[[18]](#endnote-18) On July 15, a supplementary bill was introduced that combined the use of the HaMagen app with the GSS’s tool, based on the number of new confirmed cases.

Figure 3: Architecture of the GSS Cellular Tracing Technology (“The Tool”)

Diagram, schematic

Description automatically generated

Person A is our hypothetical individual with a cellular phone and person B is a person that was identified as COVID-19 positive.

The Tool’s contact tracing process is based on constant location tracking carried out through Israel's cellular companies. As illustrated in Figure 3, every cell phone's location is tracked using a mixture of GPS locations transmitted through cellular protocols and cellular antenna triangulation. When an individual is identified as COVID-19 positive, they are briefed by the epidemiological investigation teams, and the locations they visited during the previous two weeks are fed into the Tool. According to definitions given by the health authorities, the system analyzes the location data and pinpoints individuals who were in close proximity to the COVID-positive person. Contact details for individuals identified by The Tool are then sent to the health authorities, who notify them via text message (see Image 2). The system does not let people know the location or the exact time of the proximity event.

Image 2. Text Message from the Ministry of Health



*The recipient is informed that, according to an epidemiological investigation, they have been in close proximity to a verified coronavirus patient and must enter home quarantine.*

# Privacy Analysis of the Technologies

In the short time since CCTs have been developed, we have seen several distinct architectures, with very different implications for privacy. The design of CTTs varies and can include the collection and processing of personally identifying information about people’s location, their movements, and their contacts. Some CTTs collect and process only some of these data. Such tracing has an immediate and substantial negative impact on citizens’ privacy, which may affect their trust in the government and sense of social solidarity. To analyze the potential privacy harms, we turn to a meta privacy engineering approach that analyzes the system’s data flows, protections, and potential harms.[[19]](#endnote-19) The criteria for analyzing the privacy impact are based on several fundamental questions:

* User sphere data: analyzing data gathered by the technologies and controlled by the user
* System sphere data: analyzing data gathered by the technologies and controlled by the system
* User control: whether and how users can control their personally identifiable information
* Privacy protections: includes additional privacy protections, such as policies and oversight

Table 1: Privacy Analysis of HaMagen and the GSS Tool

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technology** | **User Sphere Data** | **System Sphere Data** | **User Control** | **Privacy Protections** |
| HaMagen | Device and app history, location, Wi-Fi connection, full network access, prevent device from sleeping, change network connectivity | Locations of people who have tested positive for COVID-19 | Users can actively decide whether to install the app, contact health authorities, or share locations with the system. | Location information is not shared without user actions. Location matching is not tracked by the system. |
| GSS Tool | None: no information is stored or accessed by users | The system tracks and stores the locations of all cellular subscribers. No exact information is known about the accuracy of and additional information that is stored. | No user control over data collection. Users can appeal quarantine orders by calling the Health Ministry. | Legal obligations with GSS oversight |

The analysis of the contact tracing technologies displayed in Table 1 shows the fundamental differences between the technologies. The main difference stems from the different architectures. HaMagen keeps the data on the phone, which means that the data is saved almost exclusively in the user sphere, while the GSS tool collects locations (and possibly other information), all from the system sphere. HaMagen’s architecture, which is based on saving and matching information in the user sphere, provides users with a greater level of control. Users can decide whether to install the app, to quarantine, or to share their locations if they have tested positive for COVID-19. The GSS Tool, on the other hand, provides no level of individual control, a fact that led Israel’s Supreme Court to require direct specific legislation to authorize use of the Tool.[[20]](#endnote-20)

# Human Behavior and Deployment

The actual effectiveness of CTTs is heavily dependent on people's choices and behaviors. Effective use of voluntary CTTs requires enough people to download, authorize, and configure the applications.[[21]](#endnote-21) Users must authorize access to the exact location or to Bluetooth. Non-voluntary CTTs require citizens to carry a mobile phone on them to be effective. Therefore, to understand how useful CTTs can be in limiting the spread of COVID-19 and other infectious diseases, we need to understand the factors that impact their adoption and use. Specifically, we know that privacy concerns may negatively affect people’s willingness to use voluntary CTT solutions. Users often refrain from using or limit the permissions of mobile applications if they deviate from privacy norms.[[22]](#endnote-22) Privacy has a complex and sometimes unpredictable effect on behavioral equilibrium processes,[[23]](#endnote-23) which might lead to low adoption of CTTs, and which is likely to considerably reduce their effectiveness. To counter this problem, CTTs should be designed ex-ante to incorporate strong privacy guarantees.

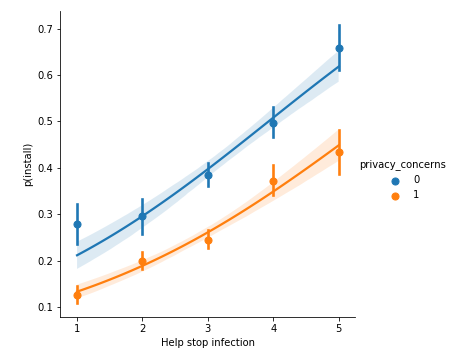
Several early studies have portrayed a contradictory picture of user attitudes towards CTT. In a survey carried out in the United Kingdom, the United States, France, Germany, and Italy, Milsom et al. have shown that 75% of all respondents declared they would “definitely install” contact tracing apps.[[24]](#endnote-24) On the other hand, of a representative sample of 2,000 people in the United States, just over 30% of Americans indicated they would download and use a mobile contact-tracing app.[[25]](#endnote-25) Contradictions have also arisen in the results of studies that evaluated the effect of privacy designs on user approaches. Li et al. used a vignette study design that did not find a relation between privacy-preserving designs and willingness to install the application.[[26]](#endnote-26) In Paradoxilly, participants preferred to install apps that use a centralized server for contact tracing, rather than designs that provided more privacy protection through decentralized architectures. On the other hand, Zhang et al. found significantly higher levels of support for apps that offer privacy protections.[[27]](#endnote-27) Similarly, Kaptchuk et al. carried out several surveys in the United States that showed how perceptions of health benefits and degree of privacy risk influence people's willingness to install contact tracing apps.[[28]](#endnote-28)

## Installations of Contact Tracing Apps

To analyze installations and attitudes towards contact tracing technologies in Israel, we conducted a survey between May 4 and May 7, 2020, that took approximately 15-minutes to complete. A total of 563 participants completed the entire survey. We used quota stratified sampling to approximate the marginal distributions of key demographic characteristics: religion/ethnicity, gender, and age.

About 32% of our respondents reported that they had installed the HaMagen application, and 9% installed and then uninstalled it. These percentages are higher than the officially reported number of 1.58 million people having installed it in Israel. One possible explanation is that our study population has more years of academic education than average. Of the rest, about 20% reported that they had not heard about the app. The rest heard about it but chose not to install it.

To analyze the factors that contribute to installing the application, we only looked at those people who have either never installed the app or who currently have it on their phones. We fitted a logistic regression model to the installation variable. The likelihood of installing the app is positively correlated with the perceived community utility of the application and negatively correlated with people’s privacy concerns. As Figure 4 shows, there is a strong positive relationship between perceived utility and the probability of installing the app. Each increase of one unit in the belief in the utility of the app increases the probability of installation by 2.3 units. Figure 4 shows this relationship. Each increase of one unit of privacy concern reduces the probability of installation by 0.6 units. Other attitudes were not found to be significant. Specifically, attitudes towards the pandemic, in general, were not found to affect installation, nor was trust in leaders significantly, or even following health instructions.

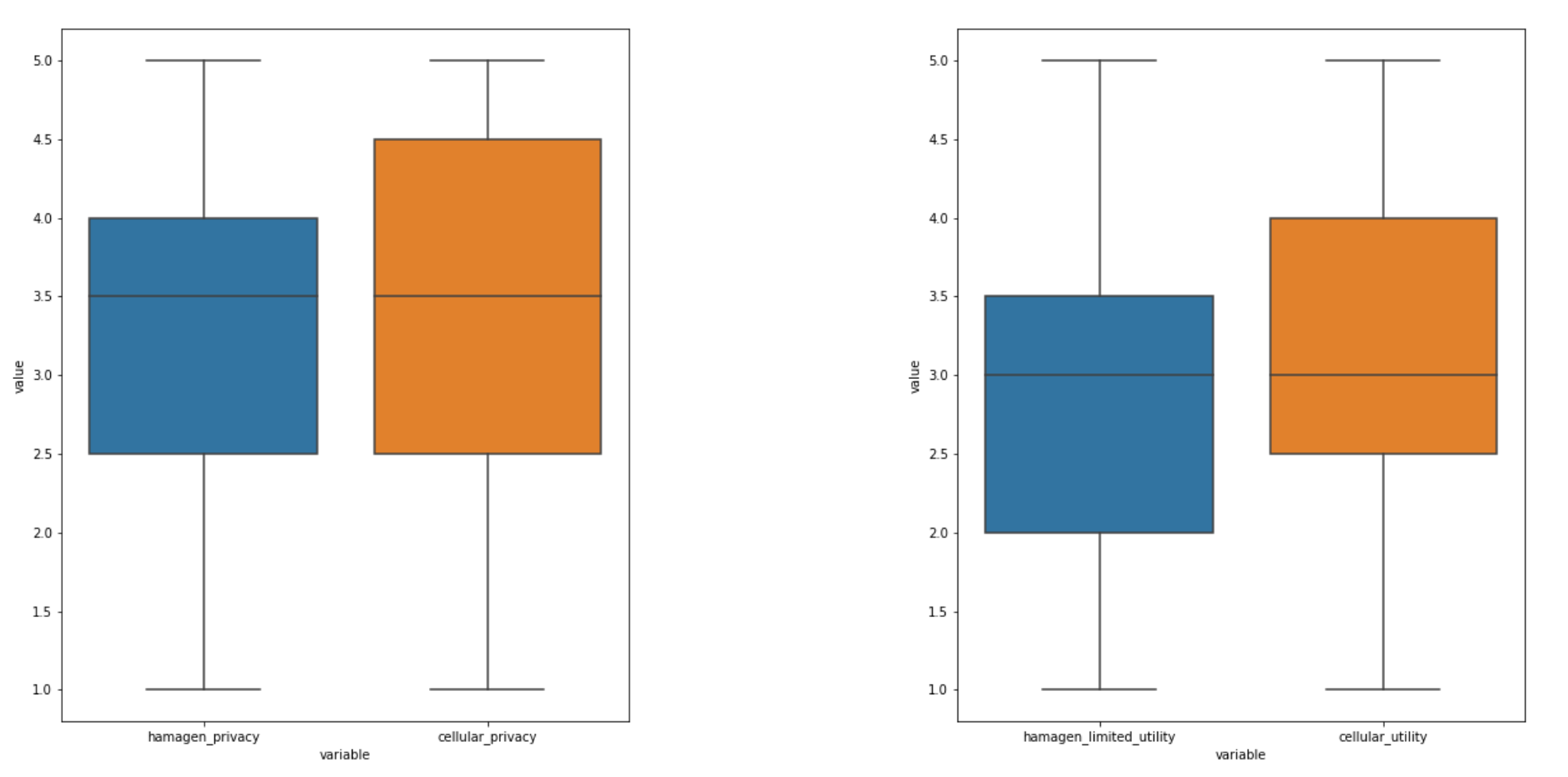
Figure 4. Perceived Utility and the Probability of Installing the App

*The effect of the general utility on the probability of installing the app, broken up by the perceived utility (higher than the median versus lower than the median).*

## Privacy and Deployment

We compared attitudes towards the contact tracing application to attitudes towards centralized cellular contact tracing technology. Overall, we did not find statistically significant differences in the approaches towards privacy between the two architectures. As Figure 5 shows (on the left), the medians and variances visually look very similar. A Wilcoxon sum test did not find significant differences (W=17499.0, p=0.15). The differences between perceived utility are statistically significant, but the effect size is rather small. As Figure 5 shows (on the right), the median utility is identical, but more participants believe that cellular tracing offers more utility (Wilcoxon sum test, W=18579.5, p=0.018).

Figure 5. Privacy Concerns and Perceived Utility



*Comparison between HaMagen and cellular tracking, with regards to privacy concerns (left) and perceived utility (right).*

These findings show that privacy perceptions are important to the installation of contact tracing apps. If we can convince people that technology does not track them and threaten their privacy, they may be more inclined to install it. However, convincing users is not easy. Users do not distinguish between privacy threats from a centralized cellular-tracking app and those from a voluntary app. This result confirms the hypothesis that the government has not communicated their privacy advantages well enough.

People have little trust in involuntary contact tracing. Their lack of trust might have real consequences, given the growing acceptance of behaviors such as avoiding carrying cell phones. If many people refrain from carrying their phones, the system’s overall accuracy would deteriorate. People also indicate low levels of trust that the government will follow through with the deletion of data that has been collected once the pandemic has abated, which may also push people to limit their cell phone use.

## Mitigating Errors

The use of contact tracing technologies in Israel sheds light on the difficulties in the many interfaces it has with individuals. The GSS Tool redeployment in July 2020 has led to revelations concerning the weakness of centralized contact tracing. During the first week of deployment, 70,949 people received text messages from the Ministry of Health notifying them that they had been in contact with a person with coronavirus and thus that they had to self-quarantine. Of them, 70,051 were identified solely by the GSS.[[29]](#endnote-29) Many individuals thought that they were misidentified as having been in contact with a person with coronavirus. Many were not told where the contact reportedly took place, and at the beginning of the redeployment there was no way to appeal the quarantine order.[[30]](#endnote-30) When an appeal mechanism was set up a few days after the deployment, the Ministry of Health Hotline was overwhelmed by phone calls. These events led to increasing acknowledgement in the media and among the public that the GSS’s tool was not as accurate and as useful as it was claimed to be.

The errors in identification and the problematic interface between the technology and the people have directly led to an erosion of trust in contact tracing and in the government’s response to the pandemic. According to the State Comptroller’s October 27 report, 3.5% to 4.7% of those told to quarantine due to the GSS’s surveillance methods contracted the coronavirus, compared with 24% of those told to quarantine by epidemiological investigations.[[31]](#endnote-31) The Tool unnecessarily sent three to eight times as many people into quarantine compared to epidemiological studies.

According to the Health Ministry, about 60 percent of the appeals against self-quarantine orders due to contact with a verified coronavirus patient were granted.[[32]](#endnote-32) The sheer number of acknowledged errors led to mistrust in the technology’s accuracy and specificity. At the same time, the lack of explanations and accountability from the GSS created a lack of engagement and a sense of resentment.[[33]](#endnote-33) News outlets have reported on calls for citizens to avoid bringing their phones to demonstrations[[34]](#endnote-34) and other public events. This failure correlates with and further contributes to a lack of trust in the authorities managing the pandemic. A survey conducted by the Israel Democracy Institute in mid-July 2020 shows a collapse in public trust towards both the prime minister and the health authorities.[[35]](#endnote-35) Health officials report that they believe that about 50% of people who are supposed to be in quarantine are ignoring their isolation conditions.[[36]](#endnote-36) The last point demonstrates the importance of public trust. Even if cellular tracking identifies all transmissions, how useful can it be if people don’t trust it?

# Conclusions

Israel has responded to the coronavirus pandemic with its ability to deploy surveillance and tracking technologies quickly. Stopping the spread of the pandemic, with its health, economic, and political implications, has become an urgent task for health authorities. Even where meaningful checks and balances exist, mass surveillance has hidden externalities. However, even though surveillance technologies may seem to be a “silver bullet” in a fight against a pandemic that spreads through interactions between individuals, our analysis here reveals a much more complicated picture.

The Israeli case study shows that even if the road to mass surveillance is a quick one, it might not lead to better outcomes. Deploying these technologies rapidly, during the uncertainty of the pandemic, led to “privacy shock,” with citizens, government, and organizations struggling to understand and assess the new informational norms. In Israel, we found that citizens have difficulties in differentiating between the HaMagen app and The Tool, even though their impact on privacy is dramatically different. Overall, we see that privacy has a substantial effect on people’s decisions to install applications and in the way they adjust their behavior to the new technologies.

The Israeli case study shows that contact tracing requires strong cooperation from citizens. People need to install applications, take their phones when they go outside, give truthful answers when briefed, self-quarantine themselves when they are asked to, and make many other diverse and difficult decisions. As attitudes towards The Tool demonstrate, when trust in the procedure erodes, people’s behavior can drive down the effectiveness of the technology. We see that Israel’s decision to rely on involuntary mass surveillance did not lead to containing the coronavirus pandemic. Privacy concerns and an erosion of trust have led people to engage in insurgent behaviors, such as leaving their phones at home and uninstalling applications. Unfortunately, these attitudes towards the GSS Tool also seem to have a spillover effect on more privacy-respectful technologies, such as the MaHagen app. Overall, the Israeli case study can be seen today, in Fall 2020, as a cautionary tale about alienating citizens while failing to reap the promised health benefits.

# References

* R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153. IEEE, 2017.
* Buch, L. Keinan-Boker, Y. Berner, E. Carmeli, R. Goldsmith, and N. Stern. Estimated frailty prevalence among israeli elderly–results from a cross sectional national survey. *Israel journal of health policy research*, 7(1):18, 2018.
* Cooperman, N. Sahgal, and A. Schiller. Israel’s religiously divided society. *Pew Research Center*, 2016.
* K. David M. Halbfinger and R. Bergman. To track coronavirus, Israel moves to tap secret trove of cellphone data, March 2020. https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone- tracking.html.
* P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi. Ask the experts: What should be on an iot privacy and security label? *arXiv preprint arXiv:2002.04631*, 2020.
* Y. Friedson. Health ministry live from the supreme court: The shin bet tracking will be extended as the lockdown is lifted, March 2020. URL https://www.ynet.co.il/articles/0,7340,L-5715439,00.html.  
  A. Grinzaig. In the request of Globes, the Supreme Court decision will be live streamed, March 2020. URL <https://www.globes.co.il/news/article.aspx?did=1001325439>.
* Johnson. Nearly 40% of icelanders are using a covid app-and it hasn’t helped much, May 2020. URL <https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/>.
* P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.  
  R. Kitchin. Using digital technologies to tackle the spread of the coronavirus: Panacea or folly. Technical report, The Programmable City Working Paper 44. 2020.
* M. Klenk, H. Duijf, and C. Engels. Ethics of digital contact tracing and covid-19: Who is (not) free to go? *Available at SSRN 3595394*, 2020.
* P. Kumaraguru and L. F. Cranor. *Privacy indexes: a survey of Westin’s studies*. Carnegie Mellon University, School of Computer Science, 2005.
* P. D. Lunn, C. A. Belton, C. Lavin, F. P. McGowan, S. Timmons, and D. A. Robertson. Using behavioral science to help fight the coronavirus. *Journal of Behavioral Public Administration*, 3(1), 2020.
* M. J. Parker, C. Fraser, L. Abeler-Dörner, and D. Bonsall. Ethics of instantaneous contact tracing using mobile phone apps in the control of the covid-19 pandemic. *Journal of Medical Ethics*, 2020.
* Pentina, L. Zhang, H. Bata, and Y. Chen. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, 65:409–419, 2016.
* Pew Research Center. Smartphone ownership is growing rapidly around the world, but not always equally. *Pew Research Center’s Global Attitudes Project*, February 2019.
* J. Tidy. Coronavirus: Israel enables emergency spy powers. *BBC News*, Mar 2020. URL https://www.bbc.com/ news/technology-51930681.
* Omer Kabir, Text Messages from the Ministry of Health: Risk of Phishing and Scamming, Calcalist, March 3rd, 2020, <https://www.calcalist.co.il/internet/articles/0,7340,L-3802839,00.html> (in Hebrew).

**Endnotes**

1. R. Jalabneh, H. Zehra Syed, S. Pillai, E. Hoque Apu, M. R. Hussein, R. Kabir, S. Arafat, and M. Azim Majumder. *Use of Mobile Phone Apps for Contact Tracing to Control the COVID-19 Pandemic: A Literature Review*, 2020. https://dx.doi.org/10.2139/ssrn.3641961. [↑](#endnote-ref-1)
2. J. Hellewell, S. Abbott, A. Gimma, N. I. Bosse, C. I. Jarvis, T. W. Russell, J. D. Munday, A. J. Kucharski, W. J. Edmunds, F. Sun, S. Flasche, B. J. Quilty, N. Davies, Y. Liu, S. Clifford, P. Klepac, M. Jit, C. Diamond, H. Gibbs, K. van Zandvoort, S. Funk, and R. M. Eggo. Feasibility of controlling Covid-19 outbreaks by isolation of cases and contacts. *The Lancet Global Health 8(4): e488–96*, 2020.

   M. J. Keeling, T. D. Hollingsworth, and J. M. Read. The efficacy of contact tracing for the containment of the 2019 novel coronavirus (Covid-19). *medRxiv*, 2020. https://doi.org/10.1101/2020.02.14.20023036. [↑](#endnote-ref-2)
3. R. Hinch, W. Probert, A. Nurtay, M. Kendall, C. Wymant, M. Hall, and C. Fraser. Effective configurations of a digital contact tracing app: A report to NHSX, 2020. URL https://cdn.theconversation.com/static\_files/files/1009/Report\_-\_Effective\_App\_Configurations.pdf?1587531217.

   L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, and C. Fraser. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, 368(6491), 2020. http://doi.org/10.1126/science.abb6936. [↑](#endnote-ref-3)
4. K. Servick. Covid-19 contact tracing apps are coming to a phone near you. how will we know whether they work? *Science*, 2020. URL https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how. [↑](#endnote-ref-4)
5. Jalabneh et al., 2020; Hinch et al, 2020. [↑](#endnote-ref-5)
6. Tracetogether: safer together join 1,600,000 users in stopping the spread of covid-19 through community-driven contact tracing, Apr 2020. URL https://www.tracetogether.gov.sg/. [↑](#endnote-ref-6)
7. R. Shaw, Y.-k. Kim, and J. Hua. Governance, technology and citizen behavior in pandemic: Lessons from Covid-19 in East Asia. *Progress in disaster science*, page 100090, 2020. https://doi.org/10.1016/j.pdisas.2020.100090 [↑](#endnote-ref-7)
8. (Israel, 2020) [↑](#endnote-ref-8)
9. C. Troncoso, M. Payer, J.-P. Hubaux, M. Salathé, J. Larus, E. Bugnion, W. Lueks, T. Stadler, A. Pyrgelis, D. Antonioli, et al. Decentralized privacy-preserving proximity tracing. *arXiv preprint arXiv:2005.12273*, 2020.

   R. Canetti, A. Trachtenberg, and M. Varia. Private colocation discovery: Taming the coronavirus while preserving privacy. *arXiv preprint arXiv:2003.13670*, 2020. [↑](#endnote-ref-9)
10. P. Mozur, R. Zhong, and A. Krolik. In coronavirus fight, china gives citizens a color code, with red flags, Mar 2020. URL <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>. [↑](#endnote-ref-10)
11. Hamagen - the ministry of health app for fighting the spread of coronavirus, Apr 2020. URL https://govextra.gov. il/ministry-of-health/hamagen-app/download-en/. [↑](#endnote-ref-11)
12. D. Globerman, Mako, <https://www.mako.co.il/nexter-news/Article-da141fa82249371027.htm>, July 28th, 2020. (in Hebrew). [↑](#endnote-ref-12)
13. (Globes, 2020; Ynet, 2020) [↑](#endnote-ref-13)
14. U. Berkovitch, Globes, <https://www.globes.co.il/news/article.aspx?did=1001343009>, September 19th, 2020. (in Hebrew). [↑](#endnote-ref-14)
15. Allison Kaplan Sommer,Israel unveils open source app to warn users of coronavirus cases, Haaretz, March 2020. URL https://www.haaretz.com/ israel-news/israel-unveils-app-that-uses-tracking-to-tell-users-if-they-were-near-virus-cases-1.8702055.

    Ronen Bergman and Ido Schwarztuch, “‘The Tool’ is Exposed: The GSS’s Secret Database that Collects Your Text Messages, Calls, and Location” [in Hebrew], Yedioth Ahranoth, March 27, 2020, https:// [www.yediot.co.il/articles/0,7340,L-5701611,00.html](http://www.yediot.co.il/articles/0,7340,L-5701611,00.html). [↑](#endnote-ref-15)
16. The General Security Service Law 5662-2002, Israeli Knesset. https://knesset.gov.il/review/data/eng/law/kns15\_GSS\_eng.pdf. [↑](#endnote-ref-16)
17. (NYTimes, 2020) [↑](#endnote-ref-17)
18. Tehilla Shwartz Altshuler and Rachel Aridor Hershkowitz, Digital contact tracing and the coronavirus: Israeli and comparative perspectives, Brookings Institute, August 2020, <https://www.brookings.edu/research/digital-contact-tracing-and-the-coronavirus-israeli-and-comparative-perspectives/>. [↑](#endnote-ref-18)
19. Toch, Eran, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, and Bruno Lepri. “The privacy implications of cyber security systems: A technological survey.” ACM Computing Surveys (CSUR) 51, no. 2 (2018): 1-27. [↑](#endnote-ref-19)
20. Globes, 2020; Ynet, 2020. [↑](#endnote-ref-20)
21. Hinch et al, 2020; Hellwell et al., 2020. [↑](#endnote-ref-21)
22. (Felt et al., 2012). [↑](#endnote-ref-22)
23. R. Cummings, K. Ligett, M. M. Pai, and A. Roth. The strange case of privacy in equilibrium models. *arXiv.* https://arxiv.org/pdf/1508.03080.pdf [↑](#endnote-ref-23)
24. L. Milsom, J. Abeler, S. Altmann, S. Toussaert, H. Zillessen, and R. Blasone. Survey of acceptability of app-based contact tracing in the UK, US, France, Germany and Italy. 2020. [↑](#endnote-ref-24)
25. B. Zhang, S. Kreps, and N. McMurry. Americans’ perceptions of privacy and surveillance in the covid-19 pandemic. 2020. [↑](#endnote-ref-25)
26. T. Li, C. Faklaris, J. King, Y. Agarwal, L. Dabbish, J. I. Hong, et al. Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in covid-19 contact-tracing apps. *arXiv preprint arXiv:2005.11957*, 2020. [↑](#endnote-ref-26)
27. Zhang et al., 2020. [↑](#endnote-ref-27)
28. G. Kaptchuk, E. Hargittai, and E. M. Redmiles. How good is good enough for covid19 apps? the influence of benefits, accuracy, and privacy on willingness to adopt. *arXiv preprint arXiv:2005.04343*, 2020. [↑](#endnote-ref-28)
29. Shwartz Altshuler and Hershkowitz, 2020. [↑](#endnote-ref-29)
30. R. Linder, Why there are so many Errors with the GSS Tracing? And What can be done? TheMarker, July 6th, 2020, <https://www.themarker.com/coronavirus/.premium-1.8973996>. [↑](#endnote-ref-30)
31. Comptroller Report, Operating Israel’s Technological Capabilities in the Coronavirus Crisis, October 27th, 2020. https://www.mevaker.gov.il/sites/DigitalLibrary/Pages/Reports/3856-2.aspx. [↑](#endnote-ref-31)
32. Jonathan Lis, About 60 Percent of Israelis' Appeals Against Quarantine Based on Digital Tracking Granted, Haaretz, July 20th, 2020. <https://www.haaretz.com/israel-news/.premium-about-60-percent-of-appeals-against-quarantine-based-on-digital-tracking-granted-1.9005554>. [↑](#endnote-ref-32)
33. Omer Kabir, Israel’s Covid-19 proximity detection app rolls out, with much criticism, Calcalist, July 29th, 2020. <https://www.calcalistech.com/ctech/articles/0,7340,L-3842371,00.html>. [↑](#endnote-ref-33)
34. Y. Yablonko, Leave your phone at home: the Soroka doctor’s post, the media storm, and the GSS cellular tracking, Globes, July 12th, 2020. (in Hebrew). https://www.globes.co.il/news/article.aspx?did=1001335497. [↑](#endnote-ref-34)
35. Tamar Hermann and Or Anabi, “Israeli Voice Index: Israel in Times of Corona,” The Israel Democracy Institute, July 14, 2020, <https://en.idi.org.il/articles/32010>. [↑](#endnote-ref-35)
36. Tal Lev Ram, Assessment: 50% of isolated people violate their quarantine conditions, Maariv, September 24th, 2020. <https://www.maariv.co.il/corona/corona-israel/Article-791800>. [↑](#endnote-ref-36)