

This site uses cookies to ensure the best viewing experience for our readers. [Read more about it](#) **Got it**

Opinion

Contact tracing apps' first task is winning the public's trust

As even seemingly benign user data can prove extremely compromising, for governments to effectively use apps to halt the spread of Covid-19, they must first prove their commitment to privacy and data security

Dov Greenbaum 08:49 26.06.20

TAGS: [Dov Greenbaum](#) [Opinion](#) [Contact Tracing](#) [Surveillance](#)
[Privacy](#)

In pre-pandemic times, Edward Snowden, a whistleblower at the U.S. National Security Agency (NSA), disclosed the extent to which the agency was tracking all civilians through [various surveillance programs](#).

While the U.S. government is supposedly prohibited from spying on citizens without a warrant, the NSA,—supported by a 1979 Supreme Court precedent and authorized under the Patriot Act, enacted following the September 11 attacks on the World Trade Center and the Pentagon—[collected billions of records containing the metadata of calls made in the U.S.](#)



Shoppers at the Machane Yehuda Market in Jerusalem during the Covid-19 outbreak. Photo: Amit Shabi

Long after this revelation, the NSA still continues to [employ a version of this program](#). However, given its increasingly diminishing operational value, [the NSA may soon opt to terminate it](#) on its own accord.

The call detail record programs, including the current paired down iteration, collect only information about the calls, including the locations of participants, the time and length of the call, or IP information. At the time of the program's exposure, even the Democratic then-President Barack Obama [suggested](#) that the public ought to be relieved that the NSA was not listening in specifically to what people say, rather just vacuuming up seemingly benign peripheral information.

However, in the world of big data, defined broadly as data that is huge in volume, fast in velocity,

However, in the name of big data, combined directly or indirectly with other data, all bits of data are effectively personal. In fact, information extracted simply from call metadata is often more informative than the content of the call itself when cross-referenced with vast amounts of data. For example, two suspicious people that consistently arrive at the same GPS coordinates, even separately and at different times could be exchanging information at designated drop sites. Several phones that are all turned off at the same time and the same place could be indicative of a clandestine meeting.

Within this reality, no matter the data's seemingly mundane appearance, citizens worldwide have reason to be wary and suspicious of their governments' efforts to develop apps that trace suspected coronavirus (Covid-19) carriers and the people they were in contact with. Privacy groups claim that even those apps employing significant privacy and security efforts still raise grave concerns.

Israel has made at least two large scale efforts in the area of contact tracing, one implemented by the Israel Security Agency (Shin Bet), the other by its Ministry of Health. The two are diametrically different. Shin Bet's attempt was reportedly designed by those within the intelligence community, with little input from the medical and epidemiology communities. Although suspended by the country's Supreme Court, Prime Minister Benjamin Netanyahu [intends to reinstate the program](#) in light of the growing number of Covid-19 cases in the country.

Under Israel's emergency regulations, technology reportedly already implemented in the fight against terrorism, was appropriated to collect data from various digital aspects of citizens' lives, including credit card transactions and phone records, to track coronavirus patients. [Shin Bet's system](#) is centralized, which means data is collected, processed, and analyzed by a central authority. Once it identifies someone as a potential carrier, it informs them of its conclusion and orders them to self-quarantine, according to the country's regulations.

In contrast, the health ministry employs [HaMagen](#), a mobile app designed by Tel Aviv-based GlobeKeeper Tech Ltd. The app is intended to be opt-in, meaning that citizens have to willingly install it on their phone to be part of the program. As with other user data-based apps, like Google's navigation app Waze, for example, the more people opt-in, the better and more reliable the results. Approximately 2 million people in Israel have installed the app thus far. However, this number is inherently capped as citizens that do not use smartphones cannot use the app.

Also, HaMagen does not report interactions between individuals and Covid-19 positive people to any centralized source, so the government does not know whether you ought to self-quarantine or not, making it your civil duty to do the right thing, as instructed by the app.

Israel is far from the first or only actor developing and deploying Covid-19 tracking apps and MIT Technology Review, a popular science magazine published by the prestigious university, offers a [dynamic database](#) on the current state of the art.

Many of the trackers mapped out by MIT Technology Review employ existing tools that are easily adapted to track people's movement. Some apps use the phones' built-in GPS systems and other location information to track Covid-19 carriers and the people with whom they interact. Other apps use standard Bluetooth technology allowing phones with the app installed to identify each other, albeit within the limited range of a Bluetooth signal.

In addition, there are a number of more advanced methods and protocols. One of the more popular systems is the Decentralized Privacy-Preserving Proximity Tracing (DP3T) protocol, developed by several European academic institutions. The protocol relies on Bluetooth to measure the proximity between coronavirus carriers, but it identifies each smartphone via a semi-random 16-byte cryptographic ephemeral identification number (EphID), uniquely but anonymously associated with the specific device.

Every time your phone encounters another phone running the protocol, the EphIDs are exchanged and logged. If a user eventually tests positive, this new information becomes associated with their EphID and is uploaded to a central server, which regularly downloads only the updated carrier information to all the nodes in the network.

However, the determination as to whether your phone has been in close proximity with a reported

disease carrier is only computed locally on your device. And, since no information is automatically sent back up to the central database, users can [choose whether to share their data with epidemiologists](#).

Privacy concerned critics have suggested, however, that even a decentralized system such as a DP3T can be attacked and these attacks can sometimes be harder to detect than it is with centralized services.

The industry-developed Apple-Google model, also known as Exposure Notification, was influenced by the DP3T model but aims to improve on it, by implementing the protocol within the operating system (OS) itself, rather than through an app where underpowered Bluetooth can lead to many false negatives from missed connections.

[The Exposure Notification application programming interface](#) (API)—the software that dictates how an app interacts with the OS—does not report user infections to a central system, it only logs encounters between two devices, leaving all operations, such as infection reporting, to be implemented by specific apps that employ the API.

This General Data Protection Regulation (GDPR)-compliant system is privacy by design, making sure apps that use the API are unable to collect any personal identification on the users themselves, unless permission is expressly granted.

The many frantic efforts to deal with the virus and its huge worldwide impact have resulted in the overlapping use of limited resources and infrastructure as jurisdictions rush to fend off the worst effects of Covid-19. We have already seen this in the medical and pharmaceutical realm with overlapping studies and vaccine efforts and we are now seeing this in the area of contact tracing apps.

For example, the U.K. poured millions into developing an app, only to [scrap it in favor of the Apple-Google protocol](#). Even North Dakota, with its relatively sparse population, [developed two competing and incompatible contact tracing apps](#), one based on the protocol created by Google and Apple and one based on the phone's location data.

Related stories:

- [How Covid-19 Might Create an Onerous Economy Inside Video Games](#)
- [How Covid-19 Can Save the World's Bee Population](#)
- [The War on Coronavirus Brings With it a Dangerous Fog](#)

No matter what contact tracing technology Israel, or any other country, ends up employing to deal with the next onslaught by Covid-19, there are many legal and ethical considerations that should be taken into account. Consent has to be provided and children ought not to be targeted without parental consent, data restrictions should be implemented to limit the retention and use of the gathered information, data security and privacy should be paramount, and there should be an educational campaign to inform the public as to the promises and pitfalls of the systems.

There are increasing cases of government overreach in the implementation of contact tracing, ostensibly justified by the pandemic. The NSA's efforts to spy on Americans were also ostensibly justified at the time, in the shadow of the September 11 attacks. But, in hindsight, such massive breaches of the public's trust hardly ever pay off.

Dov Greenbaum is a director at the Zvi Meitar Institute for Legal Implications of Emerging Technologies, at Israeli academic institute IDC Herzliya.


You Might Also Like

Recommended by

|



[About CTech](#) [Terms of Use](#) [Privacy Policy](#)

Developed by 

UI & UX by **Basch_Interactive**

Sponsored

Israel: Why Is Everyone Going Crazy Over This Inexpensive Air Cooler?
NexCooler

Place your bets: Which company will reach a Covid-19 vaccine first?

Omer Levy Appointed CFO of Binah.ai

How does a company that never turned a profit reach a valuation of \$10...

Buzz



Israel Innovation Authority eases terms for protecting institutional investors'

13.07.2020 Meir Orbach

L A B S
MEETING ROOMS
TO MEET YOUR STANDARDS

BOOK NOW



The Israeli woman who spearheads Palo Alto Networks' Managed Threat Hunting unit

24.07.2020 James Spiro



Sales conversation analytics company Gong raises \$200 million at a \$2.2 billion valuation

12.08.2020 Hagar Ravet



The cure is out there: Miniature space labs are leading to scientific breakthroughs

08.08.2020 Yoghev Carmel



Big in Japan: Israel's Binah.ai has partnered with four Japanese companies

12.08.2020 James Spiro



The constant outsider who the world's largest companies now pay millions to hack their systems

07.08.2020 Diana Bahur-Nir and Meir Orbach