Covid-19 Battle: Are we over-harnessing the power of data and technology to fight the pandemic?

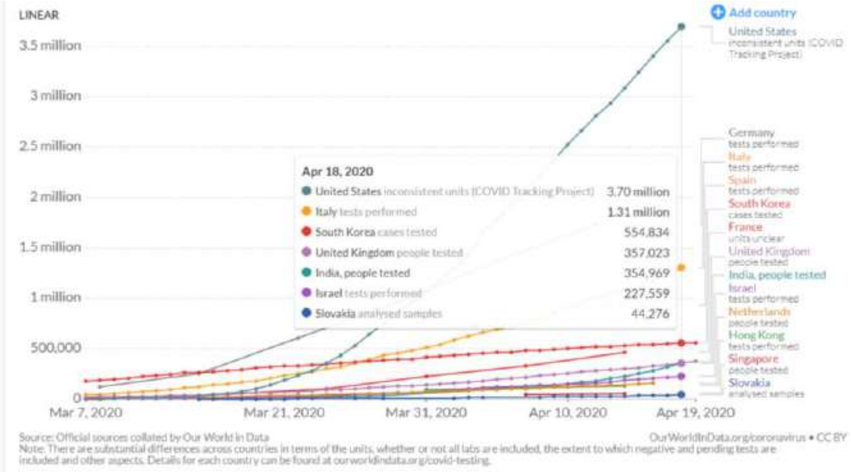
Negative technological impact by using "beyond the limits" personal data for contact tracing

Technology Vs Privacy

There is an invariable effort to find the most efficient and effective solution for fighting the global health emergency of Covid-19 (Coronavirus) faced by mankind today. In our recent article Covid-19 Battle: 4 Impactful Categories Spurring Technological Innovations, we discuss how the pandemic brings the world together to make technological innovations that would take years to accomplish if we were living in a different scenario.

But, aren't some of these technological innovations coming at a cost of personal invasion? In a Ted Connect talk, Danielle Allen (Harvard professor) stresses the need to carry-out massive, widescale testing which she further categorizes as a "smart testing" process. This process involves contact tracing or contact warning through smartphone tracking.

Figure 1: Total Covid-19 tests as on 18th April 2020



Source: Official sources collated by Our World in Data
OurWorldInData.org/coronavirus • CC BY
Note: There are substantial differences across countries in terms of the units, whether or not all labs are included, the extent to which negative and pending tests are included and other aspects. Details for each country can be found at ourworldindata.org/covid-testing.

Contact tracing is an **old-school "Sherlock" process**, where in-case of highly communicable disease—identify every sick person and who all they have met, who are potentially at the risk of being exposed to the disease. This is a continuous process until each person who may have been exposed becomes asymptomatic to stop the virus transmission. Traditionally, the process will be conducted by healthcare experts manually by gaining information from each infected person and then building the chain.

However, the advancements in technology automate this process end-to-end by enabling access to Bluetooth and location services of any individual's smartphone rather than relying on human memory. In today's world, almost every individual holds a **smartphone, with 3 billion Android and iOS users** (Podcast: The Journal)**.**

"Our analysis suggests that almost half of coronavirus transmissions occur in the very early phase of infection, before symptoms appear, so we need a fast and effective mobile app for alerting people who have been exposed. Our mathematical modeling suggests that traditional public health contact tracing methods are too slow to keep up with this virus." - Professor Christophe Fraser from Oxford University Big Data Institute

Privacy Invasion

According to Matt Hancock's (Secretary of State for Health and Social Care) letter to the NHS, *"when using data to fight Covid you do not need to comply with your duty of confidentiality anymore; Covid trumps your duty of confidentiality."*

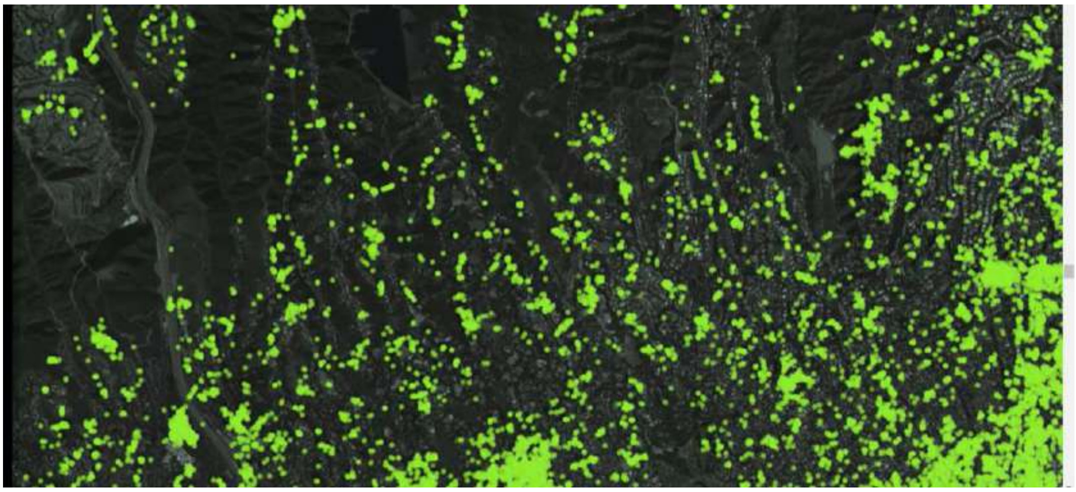
However, disclosing one's whereabouts and people connections debunks the underlying concept of privacy, civil rights, liberties, and freedom.

The danger is that measures brought in to protect citizens in exceptional circumstances, when most people accept they are needed, could outlast the current crisis, said Joseph Cannataci, the U.N. special rapporteur on the right to privacy.

Having said that, this is the need of the hour; governments have a profound obligation to prove to their citizens/societies and global communities at large that they have put the right measures in place to curb the spread. While the various government officials across the globe are asking their citizens to #stayhome #staysafe #selfquarantine, this alone is not enough. Therefore, the answer to the problem is through contact tracing applications.

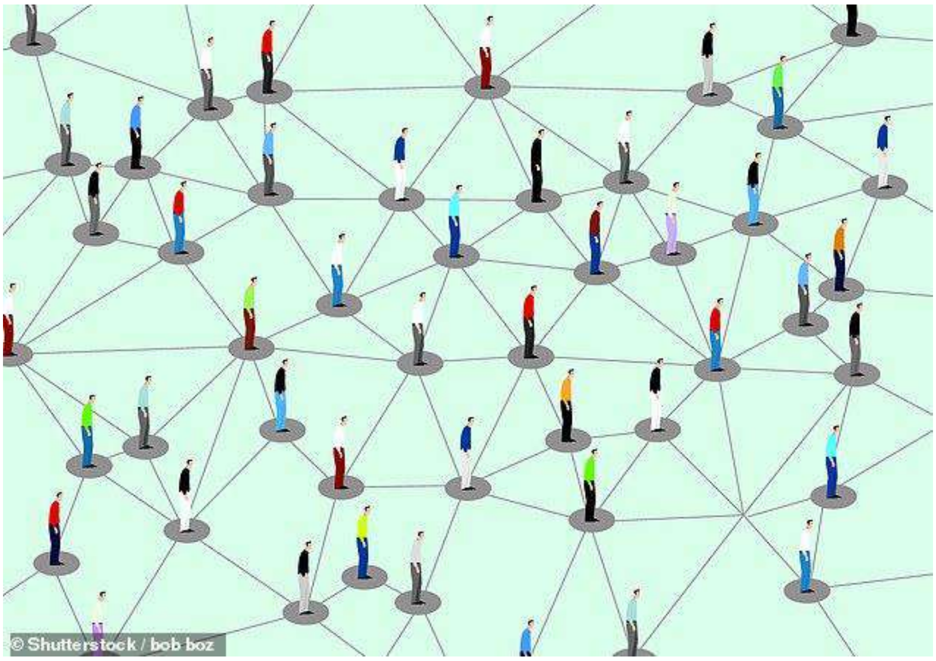
For contact tracing applications to work effectively, as discussed earlier in the article, it uses Bluetooth connection on a smartphone which then traces the signal to another smartphone. Hence, it creates links that map the number of people an individual has encountered. In addition to that, the applications track the person's location, creating a geo-trail of the places an individual has visited. Putting the two aspects together, **"who am I meeting and where am I going?"** is publicly available information (Figure 2).

Figure 2: An example of location tracking smartphones



Source: One nation, tracked (The New York Times)

In an article by Genevieve Bell in MIT Technology Review states, **“**contact tracing has this kind of history too. It was deployed at scale during World War II to manage the spread of venereal disease by American soldiers in the United Kingdom—the overlays of nationalism, power dynamics in gender relationships are all highly visible. In the 1980s in Australia, it was used to identify at-risk communities at the start of the AIDs epidemic, and gay men bore the brunt of conservative politics, religious backlash, and stigma**. The question is, can we imagine contact tracing, and other forms of data revelation, that don’t feel like a judas hole?”**



Another layer to contact tracing is when an individual declares to be tested Covid-19 positive, in that case, diagnosis is uploaded with a **“selfie”** for facial recognition to be verified by government health authorities. So, now **“how do I look?”** is also publicly available information. In some countries, these selfies are geotagged, which implies that **“from where I am clicking the selfie?”** is also tracked to ensure the person is in strict quarantine and not in contact with others.

Moreover, **Apple and Google** have come together to create a Covid-19 contact tracing solution, which the two tech giants announced on 10th April'20. Both the technology giants together dominate the operating systems of 99.3% smartphone users globally (Podcast: The Journal)**.** The intention is to create an interoperable application that works across both operating systems and removing the inconsistencies that exist in the current country-specific applications. The tool will use the Bluetooth technology and geo-location trails to trace people within 30 feet of radius, while anonymously exchanging codes to sustain the connections. **Now, imagine the scale and magnitude of data collected, processed, and managed by the two technology giants.**

The inference we can draw is that even though the data collected today to fight the pandemic is of utmost importance, the use cases it can lead to in the future will be an outcome of the data we consented to share previously. Despite the pretext that the data collected is either anonymized and/or aggregated, it still gives insights on an individual's **reactions, affiliations, religious practices, and relationships**. Thus, whether these use cases have a positive or a negative impact, it invades the fundamental right to privacy.

In an opinion-based article by The New York Times, it mentions a warning by Kelli Vanderlee, manager of intelligence analysis at the cybersecurity company FireEye stating, *"Location tracking data of individuals can be used to facilitate reconnaissance, recruitment, social engineering, extortion and in worst-case scenarios, things like kidnapping and assassination."*

Given today's scenario, the creation of such applications is crucial to identify the carriers and potential carriers of the virus, but the lack of clarity, de-limitation of data usage, and data handling are paramount concerns for the future.

Individuals, today, are ready to share their data with the **fear of whether they can be exposed to the virus**.

© Shutterstock / LP2 Studio

For example, the Hong Kong government rolled out electronic wristband synced to StayHomeStaySafe application, which alerts the authorities if a person is escaping from their compulsory home quarantines. If the same wristband and its associated technology (along with geo-tracking) are monitoring the heart rate and body temperature continuously, then it determines whether the affected needs to be shifted to a medical facility for intensive care.

But this also creates a **fear that the private data shared can create a multitude of ways in which it is manipulated for different purposes.**

Yuval Noah Harari states in his article the word after Coronavirus (© The Financial Times), *"if you can monitor what happens to my body temperature, blood pressure, and heart-rate as I watch the video clip, you can learn what makes me laugh, what makes me cry, and what makes me really, really angry. The same technology that identifies coughs could also identify laughs".*

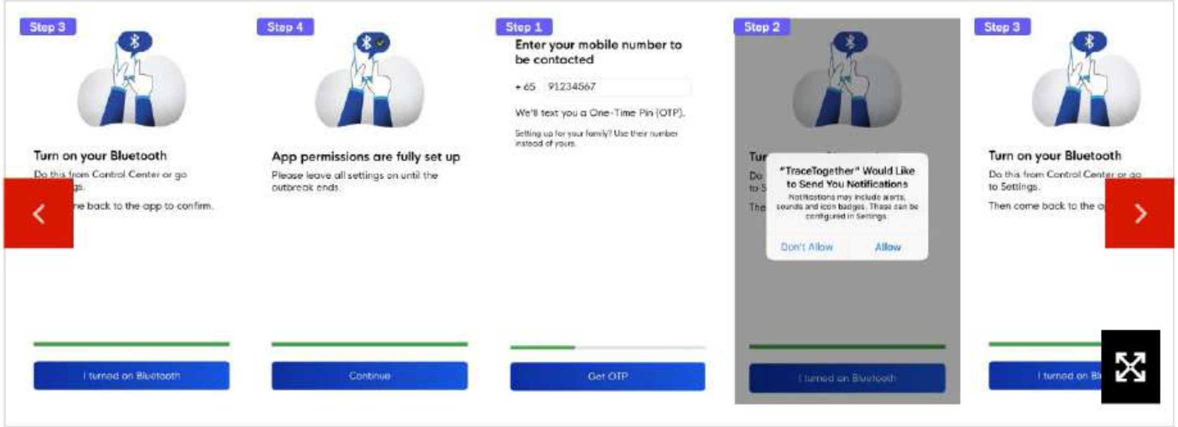
So, **who are you making powerful beyond control based on its access to such personal data? How do we determine to what extent our personal information is public and what implications it hold?**

- **Governments or regulatory bodies or ministries:** Skewing elections, managing population, pre-empting public concerns, firewall digital information, restrict opposition/ criticism, and in some cases instill fascism.
- **Technology companies:**
    - Capitalize the data by selling it to companies for the creation of customized applications, products, services, etc.
    - Use the data to predict social sentiments, relationships to create targeted social media applications
    - Predict epidemics, pandemics, war, natural disasters, geopolitical strategies, etc.
- **Individual developers and hackers:**
    - Create and sell applications through an application programming interface (APIs)
    - Hack personal accounts (emails, social media, bank apps)

Examples of country-specific contact tracing applications

Singapore's **TraceTogether** (Figure 3), it uses an individual phone's Bluetooth and traces other phones with the installed application. This tracking helps to identify the proximity of people, who has been in contact with an infected person by allowing the Ministry of Health to access the **data** on the application. The application also captures the timestamps to assess the duration of an encounter.

Figure 3: An excerpt of TraceTogether application



Step 3

Turn on your Bluetooth

Do this from Control Center or go
gs.
ne back to the app to confirm.

Step 4

App permissions are fully set up

Please leave all settings on until the outbreak ends.

Step 1

Enter your mobile number to be contacted

+65 91234567

We'll text you a One-Time Pin (OTP).

Setting up for your family? Use their number instead of yours.

Step 2

"TraceTogether" Would Like to Send You Notifications

Notifications may include alerts, sounds and icon badges. These can be configured in Settings.

Step 3

Turn on your Bluetooth

Do this from Control Center or go to Settings.

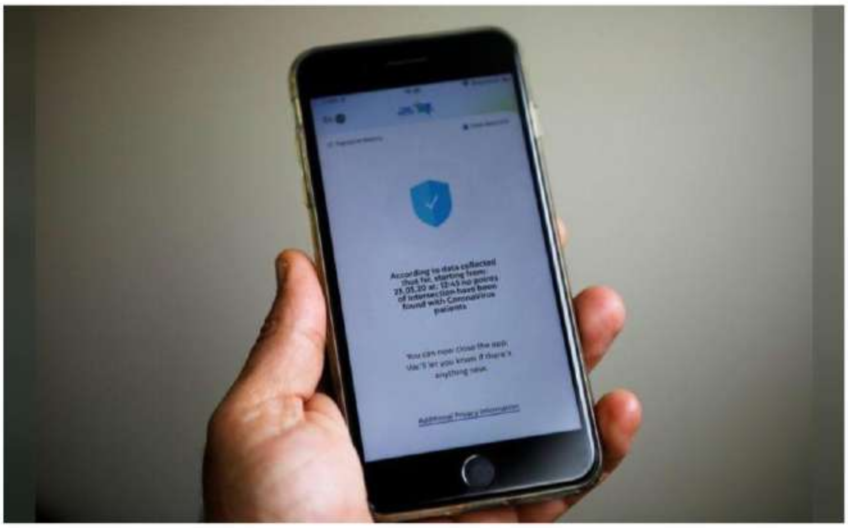
Then come back to the a

Source: Singapore Government Agency website

Germany's **Healthy Together,** is a centralized platform targeted to be downloaded by 50 million Germans and in compliance with the "German-led Pan European Preserving Proximity Tracing" guidelines (Reuters).

Israel's **HaMagen (The Shield),** it uses an individual's Bluetooth and location services to determine whether he/she has come in contact with an infected person (Figure 4). According to Israel's Ministry of Health, the app retains information about your locations solely on your device and cross-references this information with the Ministry of Health's updated epidemiological data.

Figure 4: A mobile phone image of HaMagen application



Source: Picture illustration taken on April 1, 2020. REUTERS/Nir Elias/Illustration

India's **Aarogya Setu,** it uses GPS trails along with Bluetooth functionality, which matches devices that have installed the application with its locations to trace individuals and their contacts.

South Korea launched a massive contact tracing and testing regime with the highest people per capita testing than the rest of the world— 300,000 people. South Koreans are combating this pandemic more effectively than other countries through this regime, tracing individuals through geo-location tracking and Bluetooth.

Other economies are evaluating the need for contact tracing to stem the virus, for example, National Health Service (NHS) England and UK's government is working with the Oxford University for creating such an application. Whereas, the Slovakian government has passed a law to collect geo-location data of their citizens without even asking them.

Conclusion

Well, it is scary. Despite various governments assuring and reassuring its citizens that the data collected is protected and will not be used otherwise, **ambiguity and helplessness** is a major concern.

The power of data is phenomenal, and it is fair to say that technological advancements are creating impactful solutions the world had never seen. With that, the lives of individuals are exposed whether in the light of fighting the Covid-19 pandemic or in the wake of the 9/11 terror attacks. Hence, we have done it in the past and we are doing it now because the fear is profound.

But tomorrow when lives go back to a new normal (post Coronavirus) then we will fight another war of privacy.

Despite that,

Will it be okay to consent for sharing personal information if a crisis is witnessed in the future?

While privacy experts from across the globe have raised concerns with the aftereffects of data usage, as ethical practitioners of any business, profession, company, and the industry it is paramount to institute the right measures of data privacy and security. Moreover, imbibe the responsibility of awareness among employees, partners, and consumers of measures taken for privacy.

Endnotes

https://economictimes.indiatimes.com/news/politics-and-nation/as-covid-19-cases-rise-in-india-covtech-based-surveillance-intensifies/articleshow/74876078.cms?from=mdr

https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/

https://www.governmentcomputing.com/applications/news/oxford-coronavirus-mobile-app https://www.nature.com/articles/d41586-020-00740-y

https://www.reuters.com/article/us-health-coronavirus-tracing-apps-expla/explainer-how-smartphone-apps-can-help-contact-trace-the-new-coronavirus-idUSKCN21W2I8

https://www.reuters.com/article/us-health-coronavirus-israel-apps/1-5-million-israelis-using-voluntary-coronavirus-monitoring-app-idUSKBN21J5L5

https://eng.unimelb.edu.au/ingenium/research-stories/world-class-research/real-world-impact/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia

https://eandt.theiet.org/content/articles/2020/04/contact-tracing-app-could-allow-release-from-covid-19-lockdown/

https://www.reuters.com/article/us-health-coronavirus-tech-germany/german-tech-startups-plead-for-european-approach-to-corona-tracing-app-idUSKCN21W20F

https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

https://www.theverge.com/2020/4/10/21216550/contact-tracing-coronavirus-what-is-tracking-spread-how-it-works

https://www.forbes.com/sites/bernardmarr/2020/03/23/covid-19-is-changing-our-world--as-well-as-our-attitude-to-technology-and-privacy-why-could-that-be-a-problem/#7db79d7a6dc1

https://qz.com/1836299/apple-and-google-team-up-to-fight-covid-19-with-contact-tracing/

https://iapp.org/news/a/googles-covid-19-site-raises-privacy-concerns/

https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/

https://www.cnet.com/news/covid-19-tracking-efforts-pose-a-privacy-risk-senator-says/