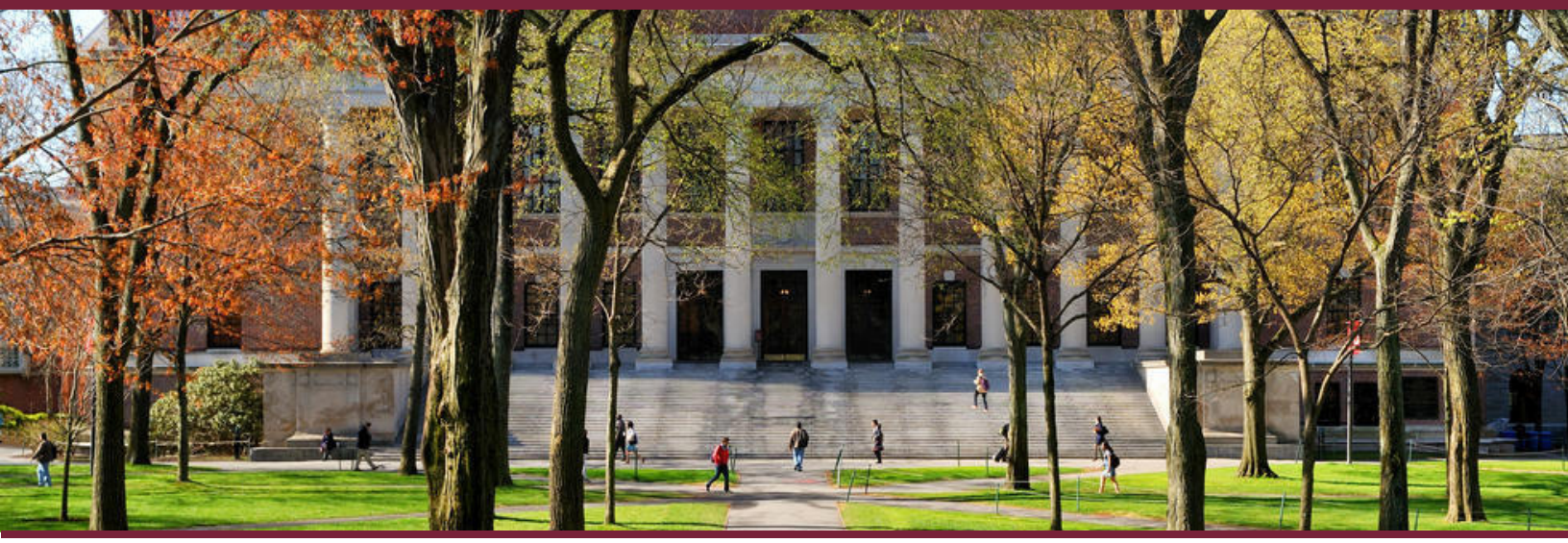
COVID-19 Rapid Response Impact Initiative | White Paper 5

Outpacing the Virus:

Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks

April 3, 2020



Vi Hart
Divya Siddarth
Bethan Cantrell
Lila Tretikov
Peter Eckersley[1]
John Langford[2]
Scott Leibrand[3]
Sham Kakade[4]
Steve Latta
Dana Lewis[5]
Stefano Tessaro[6]
Glen Weyl[7]

EDMOND J. SAFRA
Center for Ethics

Abstract

The supreme misfortune is when theory outstrips performance. You do ill if you praise, but worse if you censure, what you do not understand.

~ Leonardo DaVinci

There is a growing consensus that we must use a combined strategy of medical and technological tools to provide us with response at a scale that can outpace the speed and proliferation of the SARS-CoV-2 virus. A process of identifying exposed individuals who have come into contact with diagnosed individuals, called "contact tracing," has been shown to effectively enable suppression of new cases of SARS-CoV-2 (COVID-19). Important concerns around protecting patient's confidentiality and civil liberties, and lack of familiarity with available privacy-protecting technologies, have both led to suboptimal privacy implementations and hindered adoption. This paper reviews the trade-offs of these methods, their techniques, the necessary rate of adoption, and critical security and privacy controls and concerns for an information system that can accelerate medical response. Proactive use of intentionally designed technology can support voluntary participation from the public toward the goals of smart testing, effective resource allocation, and relaxing some of physical distancing measures, but only when it guarantees and assures an individual's complete control over disclosure, and use of data in the way that protects individual rights.

[1] Stop-covid.tech
[2] International Conference on Machine Learning
[2] CoEpi
[4] University of Washington
[4] CoEpi
[6] University of Washington
[7] RadicalxChange Foundation

Table of Contents

01	Introduction	3
02	Scaling manual processes to support smart testing and quarantine	8
03	Digitally Scaled Smart Testing	10
04	Hybrid Approaches to Smart Testing	12
05	Technology-Powered Virus Suppression and Health-Care Management	13
06	Smart testing technology	14
07	Privacy	25
08	Stigma and Harassment	24
09	Inequality and Access	30
10	Information Dissemination + Preventing Misinformation	31
11	Timeline	32
12	Conclusion	33
13	Appendix 1: Selected Existing Efforts	34
14	References	36

01 Introduction

Three months into the SARS-CoV-2 (COVID-19) pandemic, infections and deaths continue to rise globally, surpassing over 50 thousand deaths, and over one million confirmed cases as of April 2nd, and growing exponentially. The important main mitigation so far has been focused and extreme social distancing, resulting in stay-at-home orders and mandatory lockdowns in many places around the world. These measures alone can slow down the rate of infection—known as "flattening the curve"—but unless continued for many months or combined with extensive testing, tracing, and quarantine, they may only delay the same spikes in infection rates to a later date. Further, while necessary initial steps, lockdown measures have significant side effects. Massive furloughs and layoffs are rapidly spiking unemployment, with almost 10 million Americans filing for unemployment over the last two weeks. Economically, in the U.S. alone, every day of the present partial lockdown costs an estimated $10 billion—and the intangible human costs are incalculable. At the same time, the needed medical supplies, tests, provisions, and other life-critical resources are severely limited and are scaling slowly, increasing stress and anxiety at a population level. Caught between economic collapse and social disaster, many governments have responded aggressively, in some cases passing emergency decrees and expanding controls that can infringe on civil liberties and basic human rights. Concerningly, while these controls start during the pandemic, they have in some cases have been sustained long after, if not permanently.

A vaccine for the virus is currently estimated to take one to two years. Without containment, the rate of spread is bound to overwhelm the medical system, requiring an estimated 500% increase of ICU capacity to allow the pandemic to spread unchecked. Assuming this would be impossible to achieve and long-term broad containment is economically and socially unfeasible, a set of tools is required to manage the pandemic at the rate of progress that does not overwhelm the medical system.

Introduction

There is growing consensus in the public health community that to avoid this catastrophic loss of life from COVID-19, we must either have an extended (12 to 18 month) period of shelter-at-home-style policies or use technology to target quarantines more precisely. The central technological filter is biological testing: without targeting, uniform testing would need to be done at massive scale, testing up to 30% of the population per day. With efficient targeting of testing toward those most likely to have been exposed, we very roughly estimate that testing could be brought down to 1% of the population per day. Targeting such massive testing capacity efficiently will be critical to accelerating the end of the COVID-19 pandemic, saving millions of lives, preserving social stability, and saving the country hundreds of billions of dollars. The methodology required is a continual loop of testing and identification of those infected, finding those who have been in contact with COVID-positive individuals and quarantining and testing them, and finally identifying those who have recovered so they can safely work in the economy. If this process is in place, the rate of infections can be kept low enough for the medical system to cope and for the economy to continue without the lockdown.

Traditionally this testing loop has been managed manually by health-care providers through "contact tracing," where medical professionals interview the person who tests positive for the virus and contacts those who may have come into contact with a patient to alert them to quarantine and to seek a test. Dr. Anthony Fauci of the National Institutes of Health called contact tracing "the public health weapon" in a White House briefing.

Introduction

However, the COVID-19 pandemic presents a challenge even when contact tracing is used. SARS-CoV-2 has defining characteristics that make it especially difficult to keep at bay.

1. The virus is novel: there is no current defense to this version of the virus in the population, meaning no one has even partial immunity to slow down the spread. Before there could be natural herd immunity, 50 to 67% of the population would have to be infected.
2. The virus has a stealth transmission with an incubation period up to 14 days incubation period with symptoms appearing on average on day 5 after exposure. Many people can shed the virus—pass it on—even before their symptoms begin to appear. A smaller portion will process the virus asymptomatically without knowing they had it but silently passing it on. These complications make tracing those exposed and preventing onwards transmission challenging but not impossible.
3. The lethality of this virus is believed to be many times that of the seasonal flu with a high rate of mortality among the elderly and those with preexisting conditions.
4. The virus has a very high R_0, or natural rate of transmission, which represents the average number of infections generated by each COVID-positive person. According to a study published in Science, under unmitigated conditions in Wuhan, China, the R_0 was shown to be 2.36. SARS-CoV-2 is highly contagious.

To slow down the reinfection rate for this novel virus, we need novel approaches. Countries like South Korea and Taiwan showed that the use of digital technology, specifically that deployed on personal devices, can highly speed up the identification and management of the virus by empowering citizens to opt into an alert system, notifying them of possible exposure.

Introduction

While there is well-justified concern that such systems might enable mass surveillance, a variety of solutions have developed recently with intentional privacy controls incorporated. Here we discuss three complementary contact tracing paradigms and their costs and benefits:

1. Fully manual, traditional protocol scaled through large numbers of workers.
2. An encrypted peer-to-peer protocol, based on Bluetooth. We will describe different options but recommend one with most data resident on the consumer device, and with de-identified data stored on a server only when using random tokens and secure keys.
3. Location-based protocol. We will describe different options but recommend options where all personal data resides on the consumer device only.

Each of the options above has different strengths and weaknesses and all become less important if testing ramps up to a scale sufficient to test 30% of the population every day. However, adopting and obtaining wide adoption for one and probably more than one of these strategies will be critical to ensuring that the period of lockdown required by COVID-19 policies can be shortened by a month or two from what is needed to ramp up to testing at such a scale, and shortened by around a year from the period of lockdown that would be needed without other intervention. Thus, if privacy-sensitive solutions are not available, we expect that solutions that are less privacy-sensitive are likely to be adopted by countries around the world.

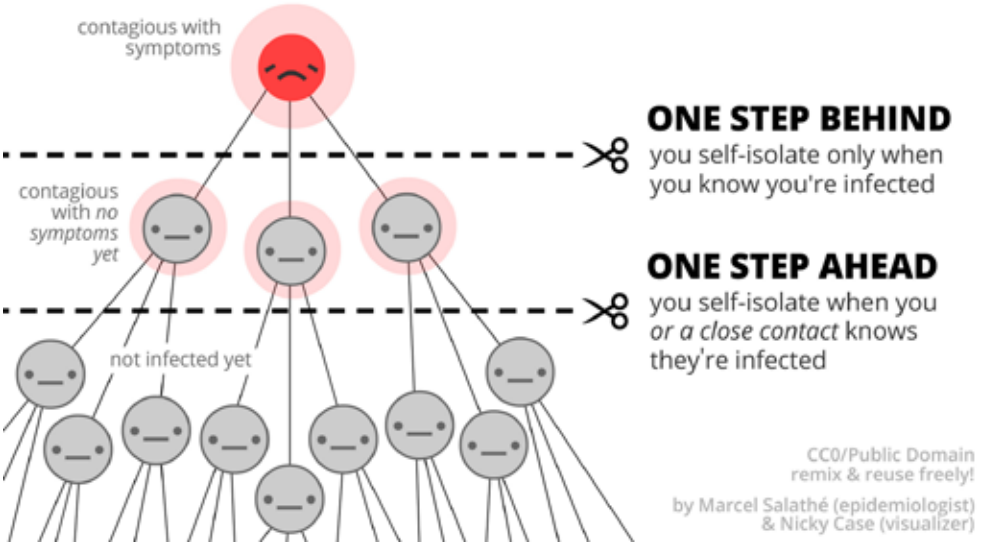
We believe it is possible to deploy a system that is voluntary, respects privacy and agency, and is resistant to fraud and abuse, while achieving the “smart” testing loop necessary to prevent another wave

Introduction

of infection or continuous lockdown. We believe it is possible to make this available within a short time-frame. And we believe that the growing global consensus around the core technology will give it the momentum to succeed.

02 Scaling manual processes to support smart testing and quarantine

Contact tracing describes a variety of techniques used to identify people who may have come into contact with a positively diagnosed person, and taking appropriate action to inform, isolate, and treat those contacts. Contact tracing is commonly used to reduce the spread of tuberculosis, measles, HIV, and other diseases. The goal of tracing is to identify and isolate not only those who are known to have a disease, but to try to get ahead of the spread of the disease by priority testing those with whom a COVID-positive person has been in close contact during the incubation period. Data shows that if only those with symptoms are identified and isolated, it will not stop the spread of the disease, as it is highly likely that they have already passed the illness to others.



Traditionally, contact tracing is done manually. It involves first testing and isolating a person who is confirmed to be carrying a virus or who is showing symptoms consistent with the associated disease. A trained health official would then interview that person to discover who they have recently been in contact with and create a list of contacts, and then go through the contact list to inform each person and repeat the process. The process includes testing and/or quarantining those contacts to watch for symptoms for the duration of the incubation period, or testing for the presence of the pathogen, if possible.

Figure 1: Using contact tracing to limit the spread of a virus. Credit: Marcel Salathé and Nicky Case.

Scaling manual processes to support smart testing and quarantine

This approach has been used in the past for outbreaks of Ebola, SARS, and HIV, and it works well when there is a small number of infected people. However, it has three big weaknesses:

1. Traditionally, manual contact tracing relies on human memory. For a highly infectious disease with a long incubation period, it becomes difficult to remember contacts and more likely that a person has spread it beyond their usual close contacts.
2. Manual contact tracing takes time. Depending on how quickly and easily a disease is spread, manual contact tracing efforts may be playing catch-up while a disease spreads beyond its scope.
3. Manual contact tracing requires trained human resources. Trained personnel are required to conduct interviews and do follow-up (Hellewell et al 2020). Our medical system does not currently have enough people for a COVID-19 scale epidemic. We estimate that up to 200,000 additional people would need to be recruited and trained.
4. Manual contact tracing has been proven insufficient to contain COVID-19 on its own, both theoretically and in practice (Ferretti et al., 2020; Bonsall et al., 2020). While contact tracing has been an integral part of the response thus far, it seems to require support from additional digital tools in order to be effective.

03 Digitally Scaled Smart Testing

For COVID-19, infections are beyond the sizes manageable with manual testing techniques used in the past, but digital testing methods have been used successfully in several countries. Both South Korea and Singapore continue to use contact tracing to effectively catch 80% of all infections before they spread too far and have not had to lock down their economies or practice extensive social distancing.

Currently we prioritize testing mostly for symptomatic individuals, but symptoms appear days and sometimes weeks after that individual becomes contagious, and probably after several chains of infection have occurred. Smart testing utilizes software to prioritize individuals who are likely to be at the highest risk of an infection based on their previous proximity to someone who has been diagnosed. Because the individuals involved are notified immediately as soon as someone in their proximity was diagnosed, this method shortens exposure risk and enables health-care providers to suppress the virus rapidly. Combined with other policies, such as priority testing of health-care workers, a smart testing policy focuses our testing resources where they can create the most public good.

Once someone is identified as SARS-CoV-2 positive, they must be able to isolate and incentivized to isolate for a minimum period of 14 days, or longer if they develop symptoms. Their contacts should also be incentivized to quarantine while they await the results of their test, and only after receiving a negative test should they resume their usual activities.

IT solutions can allow for greater privacy and cooperation than manual check-ins, at lower cost, and with reduced stigma. Combined with cultural momentum and the promise of an upcoming vaccine, we expect many people will step up and cooperate. Contact tracing can help mitigate the potential damage of noncompliance and avoid strict forms of enforcement.

Digitally Scaled Smart Testing

Widespread use of smartphones creates possibilities for smart testing that didn't exist ten years ago, and that can shore up the limitations of traditional contact tracing that make it ill-suited to fight COVID-19. There are several attributes of digitized smart testing:

1. More accurate. It no longer relies on memory to create a list of contacts.
2. Fast. A list of alerts can be created and dispatched near-instantaneously.
3. Low cost. Trained interviewers are not needed, and follow-ups can be done automatically in cases where medical care is not needed.
4. Shown to work. In places like Taiwan and South Korea, digital contact tracing has been an integral part of slowing the spread of COVID-19. At present moment, the outbreaks in those places are under control through a combination of contact tracing and other measures.

For these reasons, a consensus has grown around the need for smart testing based on digital tools (Wang et al., 2020; Cho et al., 2020; Ferretti et al., 2020).

While initially there was concern that digital contact tracing might require privacy trade-offs, in recent weeks there has been significant progress around the development of a particular Bluetooth protocol that is promising to ensure privacy controls. With this protocol, any user information would be available only to the user themselves and is not vulnerable to central hacking. This protocol has been modeled to be effective with high enough adoption rates within a given set of interacting individuals (at local, regional, national, or international scale).

04 Hybrid Approaches to Smart Testing

Using phone data to augment memory or identify high-risk individuals as part of manual contact tracing efforts has worked in several countries. Manual contact tracing can be used to supplement digital contact tracing methods in areas where app penetration is not sufficient. Where GPS location histories exist, individuals can refer to their own personal GPS data to augment their memory and provide a more accurate contact tracing interview without making this data available to anyone.

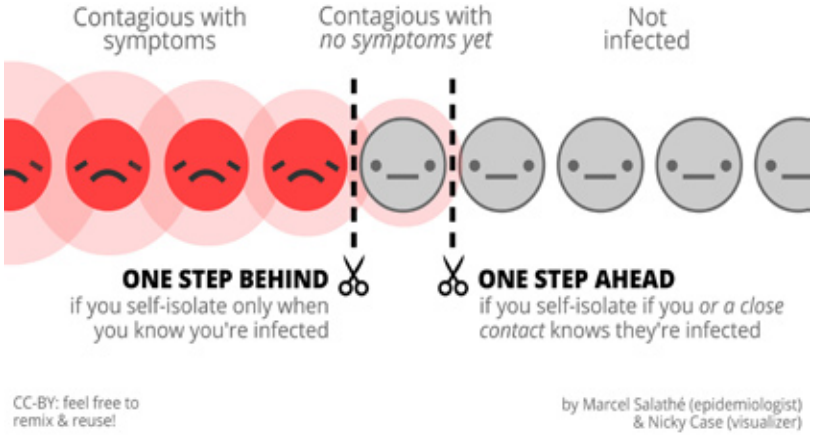
05 Technology-Powered Virus Suppression and Health-Care Management

Contact tracing, both manual and digital, can work only in the context of a functioning and well-supported health-care system. There is broad agreement that we must continue shelter-in-place policies for two to three months to buy time and reduce the number of cases. During this time, we must develop the following:

1. Increased capacity to produce protective equipment, tests, and candidate vaccines.
   a. To meet surge demand, hospital and Intensive Care Unit (ICU) capacity will have to increase to match the incoming rate of infection.
   b. Given that there are currently 5 million doctors and nurses in the U.S., we should require and properly support millions more temporary health-care workers.
   c. Most important of all, to achieve levels of disease suppression comparable to those in Asia, we must produce and administer roughly 5 million tests a day, more than 100 times the existing capacity. This requires significant increases in test production and test administration.
2. Technological solutions to help us prevent the spread of the virus and avoid a resurgence once social distancing measures are relaxed. They need to support:
   a. Digital contact tracing to enable “smart” testing that provides complete control and user privacy over their data and disclosure.
   b. Digital and biometric-secured medical records and test results accessible only to the patient themselves, to allow them the option of verifying their diagnosis.
   c. Digital tracking of medical and critical-services supply chains to help medical providers, governments, and citizens access to goods and services.

06 Smart testing technology

Smart testing relies on the broad availability of smartphones as the main device for patient identification, digital health records, and proximity tracking. To help slow viral spread, any such device must include an application that provides access to proximity tracking, identification, and medical follow-up. Such a fully-functional device would likely require a basic smartphone. For individuals with family access to a smartphone, dedicated Bluetooth-only devices with Bluetooth Low Energy (BLE) functionality, like those used by consumers to find their keys and other household items, could be produced for as little as $10 each, according to preliminary conversations the group COVID Watch has had with device manufacturers.



The higher the saturation of devices enabling selective smart testing, the more effective the suppression algorithms will be. Optimally more than 70% of the population would have these applications installed, although lower penetration could also be combined with other contact tracing interventions. One study estimates that 40% would be the minimum, while another indicates 60 to 80% would be the minimum penetration required. In the U.S., 96% of Americans (excluding undocumented immigrants) own a cellphone of some kind and 81% own cellphones, according to Pew Research, though not all are capable of running such technology. Children are another factor, and there is not enough information on how children spread COVID-19. Having smart testing functionality come standard with smartphones and other devices, with an easy and clear opt-in prompt outlining the technology and risks, would go

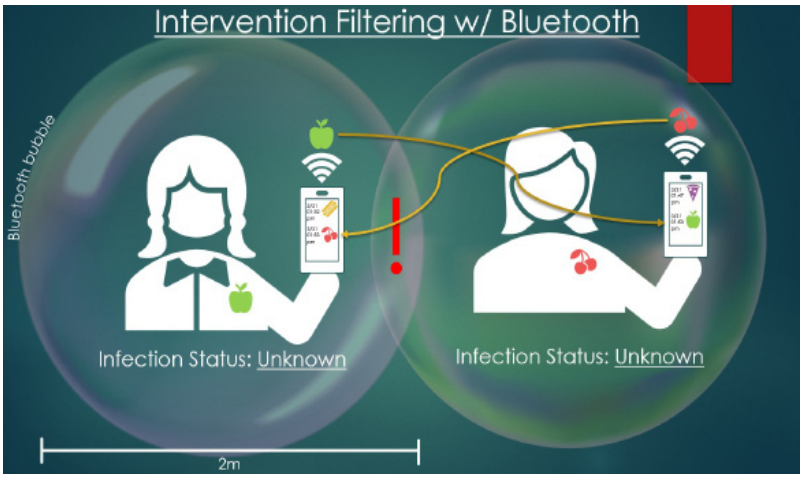
Figure 2: Using contact tracing to limit the spread of a virus. Credit: Marcel Salathé and Nicky Case.

Smart testing technology

a long way toward getting the necessary numbers of users, though probably this effort will have to be used in combination with other efforts.

The applications can utilize several algorithms in parallel to perform smart test analysis. Most core functionality relies on Bluetooth and/or GPS: he applications can utilize several algorithms in parallel to perform smart test analysis. Most core functionality relies on Bluetooth and/or GPS:

1. Bluetooth-based algorithms



Our current analysis suggests that a cell-phone peer-to-peer BLE will provide the best option for privacy-strict implementation. Bluetooth signals, broadcast from individual's phones, can be used to detect proximity to other individuals. These signals are used to talk to devices nearby (such as those estimated to have been within virus shed distance for a specified duration) and store an anonymous token from those devices.

Bluetooth has an accuracy advantage over GPS for in-person contacts. Bluetooth works reliably underground, indoors, and in motion, and will detect only those within a certain 3D radius, rather than everyone at the same GPS coordinates, which may involve people in very distant parts of the same building. This is especially useful to avoid inundating the system with false positives, while missing actual

Figure 3: Using Bluetooth signal to detect and exchange secure tokens with nearby people. Credit: M Eifler.

Smart testing technology

Bluetooth-based algorithms

contacts entirely when multi-story buildings or underground transit is involved. Bluetooth has a privacy advantage over GPS because the only information involved is contact tokens, which can be cryptographically secured in a way that is less vulnerable to de-anonymization than location histories.

Bluetooth does have a functional disadvantage in the case of surface transmission, as it can tell only whether you've been directly close to another device running the Bluetooth proximity protocol, not whether you are somewhere that an exposed person may have been recently. With Bluetooth alone, there is no way to account for hotspots of transmission or to create warnings for areas that are in need of decontamination. However, as the time window for surface transmission is tight, probably three days at the most (and shorter if surfaces are regularly decontaminated), the usefulness of identifying hotspots would be dependent on the ability to act within that time frame.

We've seen three basic Bluetooth architectures implemented or proposed, with varying degrees of centralization.

a. Centralized Warnings with Rotating Hashed Centralized ID

- Users are given a random ID known to central authority.
- Everyone broadcasts a hashed version of their ID, which changes every 15 minutes or so.
- Everyone records the IDs of those near them.
- Upon diagnosis, user sends central authority the IDs they recorded.
- Central authority can identify who has been exposed by checking whether hashes of centrally known IDs match, and contact them for follow-up.

Smart testing technology

Bluetooth-based algorithms

Security risks include government abuse, as well as the vulnerabilities of having a centralized database of personal medical information. We believe these risks are unnecessary compared to other architectures. However, this system is at least robust against third-party eavesdroppers, to whom the IDs appear as random noise. Such a system, TraceTogether, has been deployed in Singapore.

b. Decentralized Warnings, Decentralized Rotating Randomness

- Everyone broadcasts their own, self-made tokens that change constantly, and keeps a list of what they're sending out.
- Everyone nearby records everyone else's tokens.
- Upon diagnosis, user sends out the tokens they recorded to everyone else through broadcast, using a central server as a relay only.
- Everyone checks if those tokens are their tokens.
- If there is a match, they know they have been exposed.

This architecture may strain devices as massive lists of numbers must be checked individually by every person's phone. It also relies on people self-reporting their diagnosis in a way that cannot be verified, and so may be more at risk for abuse and exploitation.

This architecture does not rely on a central authority, and so it is not vulnerable to mass surveillance or data breach. However, it may be vulnerable to third-party attacks similar to DDoS attacks, where many messages are sent to overwhelm the system, rendering it

Smart testing technology

Bluetooth-based algorithms

nonfunctional. It may also be possible to triangulate and identify individuals as the distribution source of a particular ID (though we are uncertain of this).

c. Central Server, Decentralized Rotating Pseudorandomness

- Everyone creates their own random token-generator, and uses it to broadcast randomized tokens rotated at a recurring frequency.
- Every nearby device records every token they receive from other nearby devices.
- Upon diagnosis, user sends their token generator to a central server.
- Tokens generator is broadcast across the network to all devices.
- Everyone checks the affected token generator to see if it generates tokens that matches the tokens they've been exposed to.

While a central server is still used, there is no way for the central authority to identify what information belongs to whom. This mitigates the risks of centralization, while still allowing for benefits such as test verification, incentives, and reasonable bandwidth requirements. This approach allows a spectrum of options for token-generator key lifetime, from fully persistent to

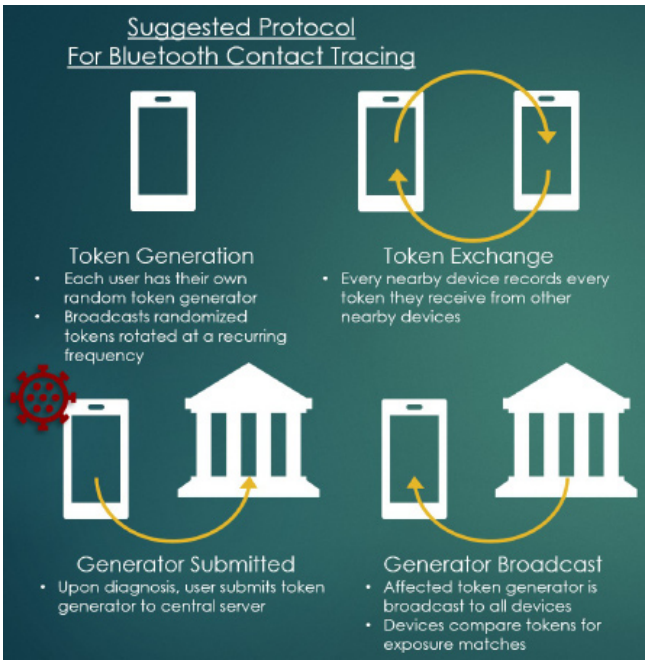


Figure 4: Suggested Protocol for Bluetooth Contact Tracing. Credit: M Eifler.

Smart testing technology

Bluetooth-based algorithms

single-use token-generator keys, with the latter being identical to option B.

Special care will have to be taken to audit the algorithm to prove it correctly prevents reconstruction of the pseudorandom generator from its output.

A particular open-source implementation of this last option, called the CEN Protocol, is being developed and adopted by COVID Watch, CoEpi, ito, and others. We recommend this style of implementation for Bluetooth as having the strongest privacy protections, including patient confidentiality.

Implementation challenges for current Bluetooth-based designs currently include challenges such as devices that cannot easily connect if both have the Bluetooth-enabled app running in the background. All other combinations of Apple, Android, background, and foreground currently work together. At least one developer in communication with the CoEpi/COVID Watch team has determined how to exchange keys between two Apple devices in the background, and the CoEpi/COVID Watch team is actively working to reproduce this method in open-source code.

Another challenge is integrating test verification. It would be possible for users to verify test results in a secure way using verification codes provided by a health authority; however, this requires coordination and cooperation with that authority, which may take time. Thus, we recommend efforts in this direction be explored and prototyped quickly. While such efforts are underway, voluntary symptom-sharing can serve many of the same purposes, and enable beta testing and pilot-scale deployment of the contact tracing/exposure matching technology.

2. GPS and WiFi-based systems

Mobile location data, which includes GPS, cell tower triangulation, and WiFi access point triangulation, can be used to create a location history for an individual, and those histories can be compared to other location histories to check for potential interactions.

The largest advantage of mobile location records is that a significant proportion of phones are already recording location data, either to Google Maps Timeline or encrypted local storage on iOS devices, or both. This allows users to install an app today and receive warnings about exposures that may have happened in the preceding week or two, and perhaps most importantly, allows those who test positive to install an app after that diagnosis.

Mobile location has an advantage over Bluetooth when it comes to tracking surface transmission, as it can be used to warn users to avoid certain areas. However, it is less accurate at identifying whether two people have been at the same place at the same time.

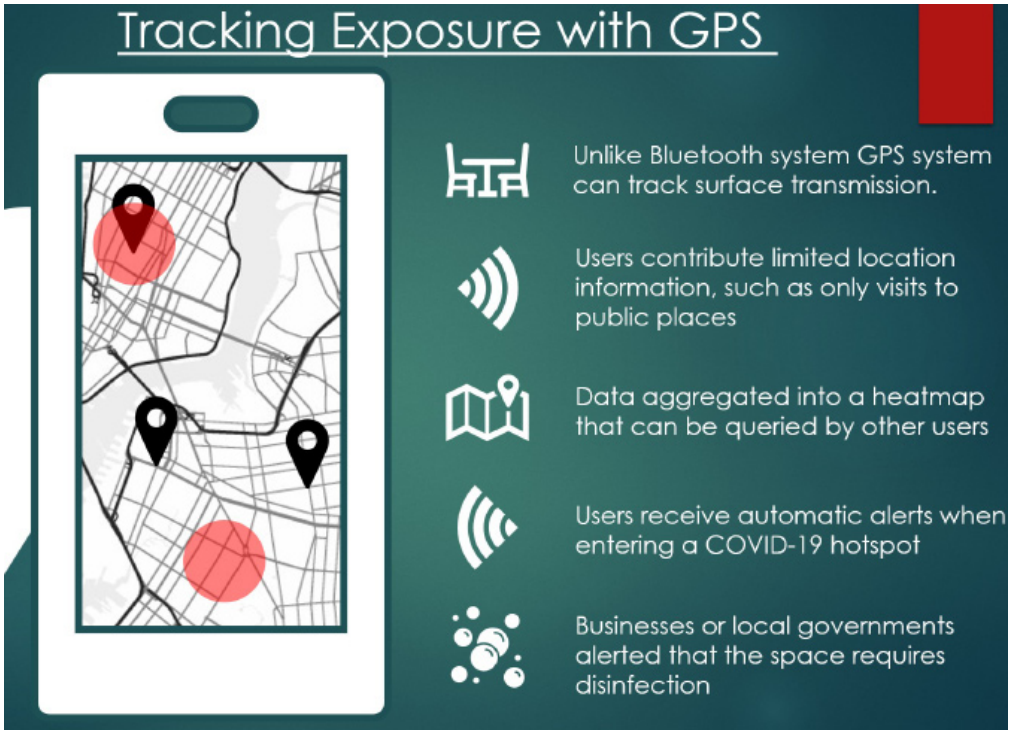


Figure 5: Methods of tracking exposure with GPS. Credit: M Eifler.

Smart testing technology

GPS and WiFi-based systems

Importantly, GPS traces have a significant security disadvantage in that location information is higher dimensional and therefore harder to anonymize correctly (though all forms of anonymization are subtle and fallible). A database of people's location histories would be easy for central authorities to abuse, and would also make a tempting target for hackers and bad actors.

It is possible to mitigate security risks through cryptographic methods and encrypted computation; however, the advantages over Bluetooth are few and the trade-offs high. We have seen a few projects that started with a GPS system switch over to Bluetooth more recently as the trade-offs became clear. We caution against the wide adoption of tracking systems that send GPS location histories to be stored in a centralized database, as they are high-risk and unnecessary.

However, there are methods by which groups are using location history to aid in Smart Testing and Smart Warnings without requiring histories to be stored externally:

a. Location History as a Memory Aid for Manual Contact Tracing Interviews

Users can track their location history on their own device, in a way that never leaves their device (or using platforms that may already be recording it, such as Google Maps Timeline or fitness apps), and use this information for their own personal reference during a contact tracing interview. Because the long incubation period of Covid-19 is a barrier to accurate contact tracing interviews, there may be significant improvements if someone can refer to their own history and tell an interviewer only the information that is relevant to tracing contacts, without having to provide unnecessary or specific location information.

b. Heatmaps using Limited, Aggregated Data

Users can contribute limited location information, such as only visits to public places, that gets aggregated into a heatmap that can be queried by other users. Automatic alerts can be given to users entering a COVID-19 hotspot, or used to alert businesses or local government that the space requires disinfection.

Done carefully, it is theoretically possible to anonymize the data in a way that, combined with limited queries, would make it impossible for a third-party bad actor to reconstruct personal data. Any system claiming to anonymize data should be carefully audited. However, there may still be some risk that the authority handling the centralized data could reconstruct some personal information through deanonymization techniques. It is, however, a strict improvement over public heatmaps that have been used elsewhere.

Combined Approaches

Several proposals for apps for smart testing include both a Bluetooth and GPS component, to gain the accuracy and security of Bluetooth for contact warnings while also making use of the unique capabilities of GPS for limited functionality. Apps may also include additional features such as incentives, general alerts, health information, and digital health services.

Increasingly, groups are moving toward similar Bluetooth architecture as one part of a suite of smart testing approaches. While the right Bluetooth architecture can be made to provide secure access, some apps may also include functionality that sends other information (such as personal information and GPS data) to external servers, for example to public health authorities for analysis. Some of these additional functionalities may not be as secure-access based; however, the common Bluetooth architecture will allow the tracing functionality of these apps to inter-operate, so that people may choose an app with high privacy standards and still receive the benefits of being part of a highly adopted system. The following table provides a comparison of Bluetooth and GPS systems in different degrees of centralization.

Smart testing technology

Combined Approaches

	Fully Decentralized	Mixed	Centralized
Bluetooth	Fully peer-to-peer: each user broadcasts and receives self-made tokens, recording interactions. Positive tokens are disseminated by diagnosed users to peer network. No centralized database stored at all. (Ex. Phase III Private Kit:Safe Paths)	Users create and broadcast their own constantly changing random IDs. COVID-positive users send their token generator to a centralized server, which broadcasts the generator for cross-checking. Centralized authority holds no identifiable individual data on users. (Ex. Covid Watch)	User ID is assigned by a central authority. ID interactions are recorded locally. COVID-positive users send their IDs to the central authority, populating a database. Users that intersect with these pings are notified. (Ex. TraceTogether Singapore)
GPS	Cryptographic methods such as private set intersection or secure multi-party computation may allow fully or mostly decentralized mobile location notification algorithms.	GPS is used as a memory aid for manual contact tracing interviews. Users are in full control of information shared, avoiding unnecessary information transfer, but tracing data is collected by a central authority.	Users submit GPS paths to a centralized database. COVID-positive users mark their paths as such. Individuals can cross-check the database to see if their paths have intersected with COVID-positive users.

07 Privacy

No technical solution can absolutely guarantee privacy. Experimentation and oversight will be crucial to make a realistic assessment of possible vulnerabilities. For example, other apps installed on a phone may try to listen in on a tracing application and send data to a third party, or someone may deduce who exposed them to the virus simply because they have had minimal outside contact and took notes that allow them to pinpoint specific exposure points. That being said, our hope is that a system can be developed that has fewer privacy failure-points than traditional manual contact tracing and more privacy protections than GPS location-based tracking, and that allows people to opt in based on a realistic understanding of the risks.

In order to drive voluntary adoption, it needs to be clear to people that a technical solution will actually help solve the problems they're experiencing and witnessing around them. Without a centralized decision maker providing a coordinated response that includes both containment of the illness and support—both for those diagnosed as positive and for those struggling in other ways due to the cascading effects of the pandemic—these tools will not be adopted, and will not be able to collect sufficient data for smart testing.

The decision to "turn on" the technologies described in this document must come from an agency like the CDC, which has the charter and necessary expertise, with oversight from regular channels. During this process, it is crucial that the technology is respectful of privacy, so that people are protected from excessive data collection and potential loss of agency, particularly in the long term. Privacy controls that include fully voluntary use, robust data security, de-identification, verifiable retention, and more are necessary to protect society and to enable trusted adoption. Once government measures are put in place for civilian surveillance, it is very difficult to roll back those measures. Thus, much care will have to be taken to ensure data collection is proportionate, fully justified, and has a fixed

Privacy

end date (Gostin, Hodge, and Wiley 2020), and that all adoption is opt-in, with no consequences for not using the proposed technology.

Historically, manual contact tracing methods have had privacy issues due to lack of confidential data management, causing harm—largely to already vulnerable populations. There is reasonable concern that digital contact tracing systems could introduce similar harm at large scale. However, while keeping this in mind, we believe that a respectful design with robust security and transparent, enforced data management can enable safe implementations of smart testing.

Existing concerns and responses include the following:

- Civil rights group Privacy International has been tracking emergency measures taken in the response to coronavirus. Engagement with civil society groups such as PI throughout the process is crucial to ensuring long-term outcomes are not overly affected by emergency measures taken.
- The ACLU writes on the privacy trade-offs of government location tracking and suggests ways in which even voluntary sacrifices of privacy may backfire, including disincentivizing testing and endangering public trust. They identify the lack of consensus from health officials that government collection of location data is necessary, and recommend that if such measures are taken then it is done with consent, with minimal data sharing, with data deleted as soon as it is unneeded, and that no effort is made to de-anonymize anonymized data.

Privacy

Existing concerns and responses include the following:

- Previous ACLU literature on individual rights in times of pandemics, particularly white papers written during the H1N1 outbreak, focused on maintaining public trust in public health authorities and encouraging public cooperation in efforts to mitigate disease. They highlight the need to avoid a law enforcement-based, punitive approach to containment, which can be highly damaging and have far-reaching consequences for citizen wellbeing and trust. They also highlight the false dichotomy of "trading liberty for security" while acknowledging that, in the case of infectious diseases, extensive government power may need to be leveraged in a way that trumps individual rights—but only when science supports the need for these measures, and only in a contained and time-bound fashion.
- Commitment to protecting civil liberties in times of national crisis is emphasized in the ten points "In Defense of Freedom at a Time of Crisis," signed after 9/11 by diverse organizations, from Amnesty International and the Electronic Frontier Foundation to Phyllis Schlafly's Eagle Forum and Grover Norquist's Americans for Tax Reform. This is particularly crucial in not deepening existing class, gender, and racial divides by deploying surveillance technology in a national security context.
- The Electronic Frontier Foundation writes that governments have not made a clear case that mass location surveillance is necessary to contain COVID-19. They ask that proposals be foremost necessary and proportionate, with safeguards that include "mandatory expiration when the health crisis ends, independent supervision, strict anti-discrimination rules, auditing for efficacy and misuse, and due process for affected people."
- Hu Yong, professor at Peking University and internet pioneer, wrote on the public health vs. privacy trade-offs in China's response to the virus and outlines three pillars: (1) treat public interest concerns as exceptions to the protection of privacy, rather than routines; (2) if it is necessary to restrict privacy for the sake of public interest, we must establish appropriate guarantees for basic civil rights and personal interests in this process; and (3) insist on fair use of information at all times (especially secure storage and deletion of information after use).

Privacy

Children are especially relevant as they are effective carriers of COVID-19 yet rarely fall ill. Because children are less likely to request testing based on symptoms and more likely to spread it to others asymptomatically, their considerations for contact tracing may be fundamentally different than for adults.

- A WHO joint report on China mentions that children have largely been identified only through contact tracing of households—perhaps household tracing, rather than individual tracing, is an option here.
- In several countries, laws related to data collection treat minors differently, depending on region and their age.
- While it may not be appropriate to collect data from children, it still might be possible to collect minimal contact tracing data locally, or through institutions such as schools, to be accessed only in the case that a child tests positive.

These valid and varied concerns must be addressed in the built technology—moving away from a location-based GPS system to a decentralized Bluetooth protocol may be the first step in this process, as well as working closely with civil society groups in development, testing, and deployment of any proposed applications.

08 Stigma and Harassment

Relevant dangers of tracing applications include social stigma and harassment of individuals, potential boycott of businesses, and racial or ethnic targeting, especially as the pandemic has highlighted existing racial and socioeconomic disparities. The same dangers exist where there is any possibility of information being exposed through abuse, misuse, or hacking. There is a need to protect against already vulnerable groups being further open to negative consequences due to the proposed applications (Raskar et al., 2020).

Fear may also prevent adoption—particularly broadcasting fear, which is public fear that individual health status and location history may be broadcast to others, as has happened in Singapore and South Korea. While the intention in these countries was to de-identify the data before it was broadcast as a preventative notification, the nature of the data makes that extremely challenging. Individuals were identified and harassed, and businesses targeted for boycotts. This could cause people with symptoms to avoid testing or tech adoption for fear of retaliation due to these privacy concerns.

Care must be taken not only to create a system people are willing to participate in at first; it must also be truly secure and privacy-preserving over the long term, so that failures will not cause a mass rejection of the technology, leading to a resurgence of COVID-19.

09 Inequality and Access

Many citizens may not own devices that have the necessary technical capabilities for these applications, or that can hold charge for extended periods of location or Bluetooth sharing. There are also vast swaths of rural (and, to a lesser extent, semi-urban) America that don't have consistent or sufficient broadband access. It is vital that we not only get a certain percent adoption, but that that percentage is spread across populations. If 100% of some communities use a tracing app, but other communities feel alienated by it, don't have the necessary devices, cannot get signal, or are afraid of government overreach, we may have a situation where the virus can more easily get a foothold in certain communities, further increasing existing inequalities and creating an atmosphere of stigma and disparity. A possible solution being pursued by COVID Watch is the idea of using external Bluetooth devices, which are relatively inexpensive, to enable expanding the system into areas where there are few smartphone users.

10 Information Dissemination + Preventing Misinformation

Tracing and containment must work hand in hand with building trust in institutions and governance bodies to increase adherence, and to make enforcement more of a social enforcement possibility than a top-down security effort. This can come only through a concerted effort at consistency, transparency, and scientific accuracy in messaging from institutional players, with practical guidelines and clear recommendations.

Centralized monitoring is most effective when coupled with a well-informed population that can do the right thing absent of tracking, as we have seen in both Taiwan and South Korea. Evidence in crisis communication scholarship recommends speed, honesty, and credibility, in addition to empathy, and highlights the need to promote useful individual actions and decisions. Using tailored messages through multiple, trusted platforms is also beneficial. Risk communication guidelines by the WHO highlight the importance of balancing risk with solutions that are practical, viable, and accessible, without which users may reject risk and not take appropriate tracing or containment measures.

Contact tracing applications have the potential for misuse or incorrect usage, which can spark panic, as users mistakenly assume they are at high risk due to incorrect information or incomplete understanding of exposure timelines. Trustworthy, consistent, and accessible messaging is crucial to mitigate these risks and ensure safe adoption of public-health promoting practices, without which contact tracing cannot function.

11 Timeline

The basic version of digital contact tracing through Bluetooth is lightweight and simple enough for a small team of engineers to implement fully within a few weeks, as has already been done by groups around the world. Beyond that, there is a high ceiling for additional functionality, interfaces, testing, and review.

We hope to see many different apps developed that use the same open-source back-end protocol for the Bluetooth component, allowing people a choice of what other functionality or interfaces appeal to them. Secure options for using location information are being explored right now, and in the coming two months standards can be developed and tested.

It is critical to integrate with a central health authority, with time barriers being more political than technological. It may take time to agree on a protocol for providing test verification codes that can securely provide confirmation of test status without revealing personal information.

It is also critical to have oversight to develop and enforce privacy guidelines for these technologies and continually review the impact in real-world situations. This will also take time to develop, and the process will be ongoing.

12 Conclusion

There are strong arguments for using digital contact tracing in combination with other technological interventions to battle COVID-19, and reasons to believe that large-scale privacy sacrifices are not necessary to make this technology work.

Specifically, there is significant momentum around Bluetooth protocols that use decentralized IDs with cryptographic protections, sent through a central server that itself has no ability to decrypt personal information from the transmissions. It seems likely that some form of this will be developed as an inter-operable standard that enables one form of digital contact tracing. In addition, there are other digital contact tracing technologies being explored and developed, including GPS heatmaps, focused public service announcements, and memory-augmentation for traditional interviews. While privacy and civil liberties must be preserved in building out these technologies, it is worth continuing to develop secure, privacy-respecting implementations to use in combination with other methods.

Contact tracing methods must work alongside other efforts to expand our testing and health-care capacity, produce and allocate supplies, and develop a safe vaccine. These methods must be deployed in conjunction with transparent, consistent, and accurate communication to citizens, and large-scale social and economic programs to ensure that lives and livelihoods, particularly those of the most vulnerable, are safeguarded.

During the coming months of lockdown, there is time for various groups to develop technology that is secure, preserves privacy to the greatest extent possible, and works between apps and devices, which in combination with other measures, can allow us to ease social distancing, slowly lift lockdowns, and return to fully participating in our economy and our society.

13 Appendix 1: Selected Existing Efforts

We know of a dozen efforts in development, and most are undergoing rapid changes. We include this list to show the breadth of efforts being undertaken and the options being explored, understanding that within the coming days the fundamental architecture of some of these efforts may shift, and that many existing efforts are not included.

Trace Together: This is the app used in Singapore, and has been shared with various governments as implementations progress. Bluetooth is used to log contacts and sent in to a central authority, which checks for matches and informs users. This app relies on Singapore's Ministry of Health (MOH) to collect data from diagnosed carriers and share it with contacts. MOH enforces cooperation of contacts who must provide information to assist manual contact tracing efforts.

Private Kit: Safe Paths, MIT: A previously described plan used GPS, which now includes the COVID Watch/CoEpi Bluetooth implementation. A paper on this is forthcoming.

Covid Watch, Stanford: This proposed system uses Bluetooth for contact tracing as well as GPS to create an anonymized heatmap of high-risk areas. With the right architecture and limitations, it may be possible to use GPS information to create a heatmap with low privacy risk, as individual paths are not traceable, though details would be needed to assess risk. Bluetooth is used to collect logs of contacts, and when a user is diagnosed, they send data in to a central database. If they are verified as diagnosed, their tokens are sent to other users who check for a match.

CoEpi.org: Working with Covid Watch on the open-source Bluetooth library and CEN Protocol for compatible Bluetooth-based contact tracing apps. This system uses decentralized contact matching and exposure alerting system that focuses on individual end-user symptom reporting, in order to allow for rapid deployment as a general wellness app providing immediate benefit to small communities of close contacts without requiring FDA EUA or integration with public health systems.

Appendix 1: Selected Existing Efforts

Alipay Health Code add-on to WeChat in China: This app is voluntary to use but centralizes information. It color codes areas as green-orange-red, uses a QR code, and scans at subway entrances. The app uses a central database, supposedly using AI to issue color codes.

South Korea: This government system warns of possible contact with infection, and sends text messages containing personal information about diagnosed carriers to inform citizens. There are concerns that breaches of privacy disincentivize testing or reporting symptoms.

UK government and University of Oxford: These entities are currently building an app relying on public volunteering of location data, which would be associated with the NHS. Specific architecture is forthcoming.

Thailand: National Broadcasting and Telecommunication Commission provided a SIM card to every foreigner and Thai who had travelled from countries that have been designated as "high risk" for COVID-19 infections (at the time, China, Hong Kong, South Korea, Italy, and Macau). The app will track the phone's location position for 14 days and alert authorities if it leaves the designated quarantine area.

Spain: The Madrid government launched a free app to track COVID-19 cases similar to those developed in Asian countries such as South Korea, China, and Taiwan.

14 References

ACLU. 2001. “In Defense of Freedom at a Time of Crisis.” https://www.aclu.org/other/defense-freedom-time-crisis.

Allen, Danielle, et al. 2020a. “Securing Justice, Health, and Democracy against the COVID-19 Threat.” March 20, 2020 (corrected March 24, 2020). https://ethics.harvard.edu/justice-health-white-paper

Allen, Danielle, et al. 2020b. “When Can We Go Out?: Evaluating Policy Paradigms for Responding to the COVID-19 Threat.” March 25, 2020. https://ethics.harvard.edu/when-can-we-go-out.

Atkeson, Andrew. 2020. “What Will Be the Economic Impact of COVID-19 in the US? Rough Estimates of Disease Scenarios.” NBER Working Paper 26867, March 2020. https://www.nber.org/papers/w26867.

Austin, Lucinda, and Yan Jin. 2015. “Approaching Ethical crisis Communication with Accuracy and Sensitivity: Exploring Common Ground and Gaps between Journalism and Public Relations.” *Public Relations Journal* 9 (1). http://www.prsa.org/Intelligence/PRJournal/Vol9/No1/

Bakker, Marije H., et al. 2018. “The influence of accountability for the crisis and type of crisis communication on people’s behavior, feelings and relationship with the government.” *Public Relations Review* 44 (2): 277–86. https://doi.org/10.1016/j.pubrev.2018.02.004

Bonsall, David, Michael Parker, and Christophe Fraser. 2020. “Letter to the Editor: Sustainable Containment of COVID-19 Using Smartphones in China: Scientific and Ethical Underpinnings for Implementation of Similar Approaches in Other Settings.” Working Paper, 2020. https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Policy%20forum%20-%20COVID-19%20containment%20by%20herd%20protection.pdf

Cho, Hyungchoon, Daphne Ippolito, and Yun William Yu. 2020. “Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs.” *arXiv*, March 25, 2020. https://arxiv.org/abs/2003.11511

COVID Watch. 2020. COVID Watch website. https://covid-watch.org/, 2020 (accessed April 1, 2020).

Doremalen, N., et al., 2020. “Aerosol and Surface Stability of SARS-CoV-2 as Compared with SARS CoV-1.” New England Journal of Medicine, letter to the editor, March 17, 2020. https://www.nejm.org/doi/full/10.1056/NEJMc2004973

References

Ferretti, Luca, et al., 2020. "Quantifying dynamics of SARS-CoV-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing." *medRxiv* preprint, March 12, 2020. doi: 10.1101/2020.03.08.20032946.

Gamhewage, Gaya. 2020. "An Introduction to Risk Communication." WHO. https://www.who.int/risk-communication/introduction-to-risk-communication.pdf?ua=1

Gostin, Lawrence O., James G. Hodge Jr., and Lindsay R. Wiley. 2020. "Presidential Powers and Response to COVID-19." *JAMA Network*, posted March 18, 2020. https://jamanetwork.com/journals/jama/fullarticler/2763423

Heath, Robert L. Jaesub Lee, and Lan Ni. 2009. "Crisis and Risk Approaches to Emergency Management Planning and Communication: The Role of Similarity and Sensitivity." *Journal of Public Relations Research* 21 (2): 123–41.

Hellewell, J., et al., 2020. "Feasibility of Controlling COVID-19 Outbreaks by Isolation of Cases and contacts." Lancet Glob. Health 8, e488–e496. February 28, 2020. https://www.ncbi.nlm.nih.gov/pubmed/32119825

Kok, Gerjo, et al., 2017. "Ignoring theory and misinterpreting evidence: the false belief in fear appeals." *Health Psychology Review* 12 (2): 111–25. https://doi.org/10.1080/17437199.2017.1415767

Lanier, Jaron, and E. Glen Weyl. 2020. "How Civic Technology Can Help Stop a Pandemic: Taiwan's Initial Success Is a Model for the Rest of the World." *Foreign Affairs*, March 20, 2020. https://www.foreignaffairs.com/articles/asia/2020-03-20/how-civic-technology-can-help-stop-pandemic.

Raskar, R., I. Schunemann, R. Barbar, K. Vilcans, J. Gray, P. Vepakomma, S. Kapa, A. Nuzzo, R. Gupta, A. Berke, et al. 2020. "Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic." *arXiv* preprint, March 19, 2020. https://arxiv.org/abs/2003.08567.

Romer, Paul, and Alan Garber. 2020. "Will Our Economy Die From Coronavirus?" *New York Times*, March 23, 2020. https://www.nytimes.com/2020/03/23/opinion/coronavirus-depression.html.

Sohrabi, Catrin, et al. 2020. "World Health Organization Declares Global Emergency: A Review of the 2019 Novel Coronavirus (COVID-19)." *International Journal of Surgery* 76: 71–76. https://umsu.ac.ir/uploads/1_1480_19_190.pdf

Tidy, Joe. 2020. "Coronavirus: Israel Enables Emergency Spy Powers." *BBC News*, March 17, 2020. https://www.bbc.com/news/technology-51930681

References

Walker, Patrick G. T., et al. 2020. "The Global Impact of COVID-19 and Strategies for Mitigation and Suppression." Imperial College COVID-19 Response Team, March 26, 2020. https://www.imperial.ac.uk/media/imperial-college/medicine/sph/ide/gida-fellowships/Imperial-College-COVID19-Global-Impact-26-03-2020v2.pdf

Wang, C. Jason, Chun Y. Ng, and Robert H. Brook. 2020. "Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing." *JAMA Network*, posted March 3, 2020. https://jamanetwork.com/journals/jama/fullarticle/2762689

Weyl, Glen, et al. 2020. "Mobilizing the Political Economy for COVID-19." Edmund J. Safra Center for Ethics, Harvard University, White Paper, March 26, 2020. https://drive.google.com/file/d/17kGMznpxIuUPdP3icqXkxIsqqQ0sTtY7/view.

WHO. 2020. "Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)." https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf