Digital contact tracing in the fight against COVID-19

Hardik Gupta, William Seaton and Johannes Kolberg

AC221: Critical Thinking in Data Science
Harvard University
Spring 2020

Executive Summary

In order to contain the COVID-19 pandemic and facilitate cautious re-opening of the economy, the United States should develop new approaches to track and understand the spread of disease. One such method is digital contact tracing, using technology native to mobile smartphones to rapidly identify possible coronavirus exposure, contact susceptible citizens, and advise targeted self-quarantine measures. While the enabling technologies are ubiquitous, there are important design choices involving the engineering and policy solutions that impact privacy and civil liberties. Pandemics can lead citizens to sacrifice privacy rights for what they believe to be temporary measures, only for governments to refuse to relinquish their new powers or data. In the case of digital contact tracing, by relying on a Bluetooth-based interaction model, making the right design choices can preserve privacy while actually delivering more effective public health solutions. The United States can learn from countries impacted earlier by the novel coronavirus and who implemented various measures of digital contact tracing in response. The efficacy of the various approaches is explored in our survey of national government responses and their associated privacy costs.

After selecting a preferred design choice for a digital contact tracing application, the next question involves designing a national policy that achieves sufficient user adoption and compliance to be effective. We simulate a range of achievement across both dimensions and the impact they have on the population infection rates for a variety of scenarios. We find that app penetration of between 40-60% of the population is necessary to reduce spread of the disease to a level manageable by the hospital system, though this requires adherence to the app's recommendations of 50-60% at least. When paired with a stay-at-home order, digital contact tracing successfully contains our simulated COVID-19. The leading countries in these efforts have yet to achieve that level of penetration but are coming close after a few weeks of public encouragement. Those countries who place privacy at the forefront of public communication have seen the greatest adoption rates and highest levels of trust by their citizens. A Bluetooth-based, private-by-design model can work in the United States if policymakers can effectively coordinate a campaign focused on a single implementation and place privacy front and center in their communications.

Situation Description

Entering May 2020, the United States has passed one million cases of the novel coronavirus COVID-19 and represents a third of the world's cases.[1] More than 63,000 people have died from the disease despite stay-at-home orders in place for the past six weeks and many states have yet to "flatten the curve" by reducing the viral growth rate to an amount manageable by the hospital system. Dramatic efforts are still required to wrest control of the epidemic, but these efforts are beginning to cause their own second-order damage. The extended duration of stay-at-home orders has slowed economic activity at the fastest rate since the Global Financial Crisis of 2008 and, by some measures, since the Great Depression of the 1930s. The economy declined by 4.8% in the first quarter of 2020 with a further drop expected in the second quarter.[2] More than 30 million Americans have filed for unemployment benefits

[1] Coronavirus in the U.S.: Latest Map and Case Count - The .... Retrieved May 3, 2020, from https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html

[2] Real Gross Domestic Product (A191RL1Q225SBEA) | FRED .... Retrieved May 3, 2020, from https://fred.stlouisfed.org/series/A191RL1Q225SBEA

during the six weeks ending on April 25th 2020, the fastest rate in the nation's history.[3] The magnitude of these second-order impacts of mitigating the epidemic are causing politicians to begin arguing that the solution cannot be worse than the disease and proposing various plans to re-open the country. Public health experts have stated that any plan to reopen the United States will require tools like sufficient testing capacity and contact tracing, the latter of which is our focus.

Contact tracing is defined by the World Health Organization as the "identification and follow-up of persons who may have come into contact with a person infected."[4] It allows for an understanding of the magnitude of public health risk from exposure and a targeted method of advising exposed individuals on proper medical precautions, typically focused on self-isolation to prevent further transmission. It helps both in combating the spread of the disease and in our epidemiological understanding of it.

Contact tracing is traditionally a manual process, involving interviewing the patient about their recent travel history, listing each of the people they came into close contact with and a phone number to contact them, and following up with each contact to alert them to their exposure and advise on recommended actions. Privacy concerns exist because each patient is providing the government with a list of their known contacts and detailed records of their whereabouts. In some countries such as Singapore, providing this information is required by law if you have been tested and confirmed ill. Though it would damage containment efforts, the patient does have a choice to not reveal certain travel locations and personal contacts. Accuracy relies on the memory and truthfulness of the patient and is limited to only their personal acquaintances. If the patient was asymptomatic and within six feet of someone on a public bus, they will not know that person's contact information in order to follow up and notify them. Each interview can take an hour or more to gather this information and subsequent phone calls depend on the prompt response of exposed individuals. For diseases with high transmission rates, manual contact tracing can be too slow to keep up and provide any serious containment.

Manual contact tracing is also very expensive. Tom Frieden, former director for the Centers for Disease Control and Prevention, estimates that the United States will need to hire 300,000 contact tracers to contain COVID-19 after re-opening. David Harvey, executive director of the National Coalition of STD Directors, estimates 30,000 new contact tracers from today's 1,600 but puts the cost of these new hires at $720 million.[5] Massachusetts has taken the lead amongst the states by hiring 1,000 new contact tracers and allocating $44 million towards the initiative. Early evidential costs are large and will put a further strain on spending by the federal government. Fortunately, there are opportunities to significantly reduce both time and cost requirements.

Digital contact tracing is an opportunity to use ubiquitous mobile technology to greatly accelerate the monitoring and alerting of possible exposure incidents. It eliminates the reliance on faulty human memory and can for enrolled participants eliminate the time taken to disseminate infectious contact through that patient's network. As with most digital advances, the benefits of speed and efficiency are counterbalanced by a loss of individual privacy, with a proportion that depends on the implementation.

[3] (2020, April 30). Coronavirus-driven unemployment claims surpass ... - Politico. Retrieved May 3, 2020, from https://www.politico.com/news/2020/04/30/coronavirus-unemployment-claims-numbers-225603

[4] WHO | Contact tracing - World Health Organization. Retrieved May 3, 2020, from https://www.who.int/csr/resources/publications/ebola/contact-tracing-guidelines/en/

[5] (2020, April 13). 'We need an army': Hiring of coronavirus trackers is likely set .... Retrieved May 3, 2020, from https://www.statnews.com/2020/04/13/coronavirus-health-agencies-need-army-of-contact-tracers/

Digital contact tracing can require collecting and sharing your detailed location for as long as 28 days with a government health agency or private company. It becomes simple to identify your personal network and the strength of each connection according to the time spent in physical proximity. If data processing occurs within government IT systems, opportunity for abuse exists should an analyst process the data in ways unrelated to contact tracing. In the United States, data retention laws are limited, hence patients are unaware how long the government will retain this information once the disease has dissipated. The possibility for abuse has privacy advocates in academia and industry leaping to develop solutions that are effective, efficient, and respect individual privacy.

Technology Choices and Design Decisions

Mobile phones provide two primary methods of digital contact tracing: GPS and Bluetooth. Both come standard with most modern smartphones. GPS provides detailed locations for an individual at hyper-specific time intervals. It is commonly used in consumer applications, so there is a large population of application developers with familiarity in designing GPS-based applications. While location data is detailed, it is most useful for two-dimensional spatial analysis and can provide frequent false positives when applied to digital contact tracing. Analysts are unable to accurately evaluate vertical distances or intermediate barriers and may falsely assume two people were close enough to spread a disease when in fact they were ten floors apart. Bluetooth contact tracing relies on signal strength, specifically a calculation called the Received Signal Strength Indication (RSSI), to measure proximity and distance of two devices.[6] This signal is weakened by intervening objects and is thus less likely to create a false positive for people on the other side of a wall or on different floors. It is also a cheaper technology, so for national initiatives that must consider users without smartphones it would be more cost-effective to use Bluetooth devices.[7]

In addition to the choice of underlying technology, developers must consider how they want to develop their digital contact tracing applications. Many institutions have made the underlying code open-source and freely available. Several have partnered closely with government institutions during development or subsequently during data collection; the extent of this partnership can impact the public's perception of the application and its desire to adopt it. Storage centralization is the key decision to make when working closely with a government agency: most implementations require at minimum a central communication server for coordinating the sharing of lists with potential exposure amongst individual phones; the maximum involves the collection and storage of personally identifiable information (PII) in a central server with access provided to a number of different government agencies with varying missions.

Privacy decisions must also be made on the duration for which data is stored. Public health policy recommends 14 days of quarantine before a person can confidently assume they do not have the disease. Since COVID-19 has high asymptomatic transmission, 14 days is considered the minimum number of days that location or interaction data must be stored. Our study found a maximum of 28 days of data storage in the MIT "Private Kit: SafePaths" application.

Another design decision involves user consent: does the user have to opt-in to digital contact tracing or are they required to download an application? Some governments require application

[6] (2015, September 21). Proximity and RSSI | Bluetooth® Technology Website. Retrieved May 3, 2020, from https://www.bluetooth.com/blog/proximity-and-rssi/

[7] Difference between Bluetooth Trackers and GPS ... - Chipolo. Retrieved May 3, 2020, from https://chipolo.net/en/blogs/difference-between-bluetooth-trackers-and-gps-trackers

download for infected patients or travelers entering from abroad, but do not make it generally mandatory. Others restrict all forms of travel unless a user has downloaded the application. Some will send police to your home if you are not using the application as designed to communicate your health to the monitoring government agency.

Policy Formation in the United States

The United States' lack of a cohesive federal response has prevented a single approach from taking shape. Instead, a variety of methods have been proposed by academic research groups and private companies like Apple and Google – the largest developers of mobile phone operating systems. We explore the most prominent applications proposed by universities like Stanford, the University of Waterloo, and MIT. Their work impacted major design choices being made by Apple and Google: the integration of Bluetooth-based contact tracing into their core platforms.

MIT's "Private Kit: SafePaths"

MIT has been leading the development of the SafePaths application.[8] SafePaths stores 28 days of GPS and Bluetooth location history locally on your phone and allows you to share it with the SafePaths community and public health officials if you have tested positive for COVID-19. The project is open-sourced[9] and built with "privacy-by-design." The app compares an individual's location history to anonymized public location data of known infected patients. The comparisons are done locally on the user's phone and no data is shared unless the user approves it. When a patient tests positive, they will work with a medical professional to review their location data and publish 14 days of travel history to SafePaths' central repository.

SafePaths has targeted public health officials as a beneficiary with its associated web-tool "SafePlaces", which maps hot spots of confirmed COVID-19 cases to improve resource allocation prioritizations.[10] They also claim a secondary benefit of GPS mapping for users who can now avoid infection hotspots. Government agents are only able to access anonymized location trails of infected patients, which SafePaths says provides the added benefit of identifying public locations with frequent coronavirus exposure beyond what Bluetooth alone can provide. SafePaths discusses how health officials can redact personal locations like home or work but leaves redaction decisions to the government agent instead of the user. This leaves the concern that someone can re-identify the individual by comparing their frequently visited locations to identify their home, workplace or neighborhood.[11]

SafePaths' rejection of Bluetooth as the primary location technology appears shallow. They quote that "there are some widespread third-party apps that have hundreds, or even sometimes billions, of installations" that can "start listening to all these Bluetooth beacons that are being emitted by these

[8] COVID Safe Paths. Retrieved May 3, 2020, from https://covidsafepaths.org/

[9] tripleblindmarket/covid-safe-paths: COVID Safe Paths ... - GitHub. Retrieved May 3, 2020, from https://github.com/tripleblindmarket/covid-safe-paths

[10] Frequently Asked Questions | COVID Safe Paths. Retrieved May 3, 2020, from https://covidsafepaths.org/frequently-asked-questions/

[11] (2018, September 24). Towards matching user mobility traces in large ... - IEEE Xplore. Retrieved May 3, 2020, from https://ieeexplore.ieee.org/document/8470173

phones and can easily create the identifiable trajectories."[12] While there have been some studies that use "sniffing" algorithms to maliciously identify a user's location[13], these have typically been issues of neglect resulting in the lack of random ID generation or encryption – both common security protocols.

SafePaths has proposed an effective and decentralized method of digital contact tracing yet is ultimately judged on the basis of the necessity of specific location history in containing the virus. The anonymized heat map of infected patients can help public health officials and users target areas for containment or avoidance, but it is not clear this targeting needs to be so granular. Public resource allocation typically happens at the hospital or zip code level. Contact tracing happens at the level of individual interactions, something managed equivalently well with Bluetooth-only methods. The app designers acknowledge that location data such as commuting times will need to be manually removed from the public repository as unimportant for public health, yet this will be what the majority of GPS data can provide above someone manually listing their frequent locations. The utility benefits from collecting and utilizing GPS data do not appear to outweigh the privacy concerns.

Stanford and Waterloo's "TCN Protocol"

The most secure proposal for digital contact tracing has come from researchers at Stanford University and the University of Waterloo. The app "Covid Watch"[14] uses a decentralized, randomly generated token list to maintain a local history of interactions as measured by the strength and duration of Bluetooth signal. When a patient tests positive for the coronavirus, their private local list of interaction tokens are sent to a central server of "infected tokens" with no PII associated. The central server publishes to all participating mobile phones the full list of "infected tokens" so that local processing can compare "infected tokens" against a phone's list of interaction tokens to confirm if that particular user has had any close interactions with an infected person. At no point does the central repository or any other user receive PII that could be used to identify who is infected or who interacts with whom. This open-source design is called the "Temporary Contact Number (TCN) Protocol."[15]

In addition to recording no PII, the TCN protocol randomly generates a new contact event number every few minutes so each phone has no unique identifiers that could be used for re-identification. This prevents the prominent method of Bluetooth hacking where a physically proximate malicious actor could track a persistent Bluetooth ID to identify the broadcaster's location.

This method of background Bluetooth exchange is handicapped by policies in place with the two primary mobile operating system developers, Apple and Google. Apple's iOS does not allow persistent Bluetooth broadcasting in the background as a privacy precaution, while Google's Android does with user permission – but has unfixed bugs where repeat connections between multiple devices can cause Bluetooth to lock up.

---

[12] Transparency and Consent - By Default | Raskar, Pahwa. Retrieved May 3, 2020, from https://drive.google.com/file/d/1XM2uAWL3RyyoVTyE726a2k2F3X2xAAQ-/view

[13] (2019, July 17). How Fitbits, Other Bluetooth Devices Make Us Vulnerable to .... Retrieved May 3, 2020, from http://www.bu.edu/articles/2019/fitbit-bluetooth-vulnerability/

[14] Covid Watch. Retrieved May 3, 2020, from https://www.covid-watch.org/

[15] (2020, April 8). TCNCoalition/TCN: Specification and reference ... - GitHub. Retrieved May 3, 2020, from https://github.com/TCNCoalition/TCN

The TCN Protocol is the approach to digital contact tracing that is both fully effective for public health measures and respects user privacy. Still, Stanford computer scientist and team lead Cristina White acknowledges that the protocol has seen slower adoption by public health officials because of its lack of GPS data. "Public health agencies really don't want to do the kind of thing that we're proposing because they do want more data. But I think we're providing what the public might want."[16]

Apple and Google

The two largest mobile phone operating system developers, Apple and Google, have sole approval rights on the design of applications allowed in their respective App Stores, and therefore control the associated probability of success for any nascent method of digital contact tracing. It is therefore encouraging to see that the decisions they have made to support digital contact tracing have been impacted by privacy advocates. The companies announced a joint partnership to build into their core platforms a form of Bluetooth-based contact tracing.[17] In May, the companies will release a cross-platform API to enable apps built for their audiences to communicate with one another, preventing a situation where users are only able to connect with others using the same phone type. In the coming months, both companies will build opt-in Bluetooth-based contact tracing directly into their core platform, eliminating the need to download one of an increasing number of applications. There are several optimistic reasons for this. First, the companies have listened to public health experts and privacy advocates in choosing how best to assist in the fight against COVID-19. Second, the companies elected to make this service opt-in. Third, the companies have a combined installation base of over 3 billion smartphones worldwide. The immediate international impact of this privacy-preserving technology installed by default will pay major dividends in the fight against COVID-19 and future disease outbreaks.

A Diversity of International Approaches

Many countries have made digital contact tracing a prominent method in containing the virus. Different national cultures and the relationship between citizens and their government has led to different choices in technology, centralization, and the extent to which compliance is mandatory. The countries that best succeeded in containing the virus all laud digital contact tracing as necessary in their efforts, but the underlying approach has differed dramatically. We explore the various alternatives in a series of case studies, navigating from those nations with the most invasive privacy practices to those with the least.

China

China implemented the strictest response to the novel coronavirus, enforcing mandatory data sharing, location tracking, and restricting the movement of its citizens. The country managed the movement of its citizens by instituting a color-coded rating system delivered via a QR code across several major app ecosystems.[18] Local governments defined the rating algorithms and colors were used at public

[16] (2020, April 8). Clever Cryptography Could Protect Privacy in Covid-19 .... Retrieved May 3, 2020, from https://www.wired.com/story/covid-19-contact-tracing-apps-cryptography/
[17] (2020, April 10). Apple and Google partner on COVID-19 contact tracing .... Retrieved May 3, 2020, from https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/
[18] (2020, April 20). China's coronavirus-tracking apps use color codes ... - Fortune. Retrieved May 3, 2020, from https://fortune.com/2020/04/20/china-coronavirus-tracking-apps-color-codes-covid-19-alibaba-tencent-baidu/

checkpoints to determine whether police would permit an individual to pass and leave their restricted neighborhood. Green codes permitted unrestricted movement, yellow codes required seven days of quarantine and red codes required fourteen. Users downloaded the apps from China's major platforms Alibaba, Tencent and Baidu, and were required to share information at sign-up such as their name, national identity card number, phone number, home address, potential symptoms and travel history. Continuous data collection occurred as users were required to enter their temperature each day to maintain their health status.

South Korea

South Korea has been held up by many in the West as an exemplar response to COVID-19 from a democracy, but the details of their data use are cause for serious concern when viewed from a privacy perspective. The government emphasized transparency in metrics and diagnosis, localization of alerting, and detailed contact tracing. Once a person has a positive coronavirus test, the city or regional government will push a public notification to all local residents including personal information on the patient such as last name, sex, birth year, residential district, profession, hospital and travel history. Additionally, the contact tracers will integrate closed-circuit television (CCTV) and credit card data to gain the fullest picture of a patient's recent travel.[19]

The government has a strong legal basis for data transparency coming from frameworks made in response to the 2015 outbreak of Middle East Respiratory Syndrome (MERS). At the time, they refused to publish which hospitals were treating MERS patients until a citizen developer made a map of crowd-sourced reports and anonymous tips from hospital staff. The publication of this information combined with public backlash against the secrecy forced the government to release more information. This change was codified in 2015-2016 with notable amendments to South Korea's Infectious Disease Control and Prevention Act (IDCPA).[20] The first relevant amendment was to Article 76-2(2) of and permitted the Minister of Health and Welfare to request from the National Police Agency "location information of patients with an infectious disease and persons likely to be infected by an infectious disease" and forced any "location information provider and the telecommunications business operator" to comply with the police request. The second was to Article 6(2) and stated that "each citizen shall have the right to know information on the situation of the outbreak" and "local governments shall promptly disclose the relevant information."[21]

Studies find that South Koreans are supportive of data transparency and collection, favoring the right to know over the right to privacy during a pandemic.[22] Still, the transparency has led to a hesitation to proactively get tested, according to Choi Young-ae, the chair of South Korea's Human Rights

[19] (2020, March 26). Pervasive personal data collection at the heart of South .... Retrieved May 3, 2020, from https://blogs.thomsonreuters.com/answerson/south-korea-covid-19-data-privacy/

[20] (2020, March 16). Lessons for America: How South Korean Authorities Used Law. Retrieved May 3, 2020, from https://www.lawfareblog.com/lessons-america-how-south-korean-authorities-used-law-fight-coronavirus

[21] 영문법령 > 본문 - 감염병의 예방 및 관리에 ... - 국가법령정보센터. Retrieved May 3, 2020, from http://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=188080&chrClsCd=010203&urlMode=engLsInfoR&viewCls=engLsInfoR

[22] (2020, March 18). South Korea is reporting intimate details of COVID-19 ... - Nature. Retrieved May 3, 2020, from https://www.nature.com/articles/d41586-020-00740-y

Commission.[23] While the government tried to localize its alerts, citizen developers have built applications that gather all alerts and publicize them in a central location. Applications like Citizen Map and Citizen 100m have been downloaded by more than a million people. In response to the HRC, South Korea's CDC issued limited updated guidance on March 14th that reduced the time duration of released history according to the severity of symptoms and stated "personally identifiable information should be excluded" but re-stated its support for releasing "spatial and temporal information such as buildings and place names."[24] This was enough information to continue to support the public shaming campaigns being pursued by internet users against those patients who had been re-identified.

Poland

Poland was one of the first European countries to launch a smartphone application for digital contact tracing, mandating its download for infected patients and citizens returning from abroad. At sign-up, users can see a number of personal details auto-completed from existing government databases. The application uses GPS location data to ensure the user has remained indoors. It validates a person has not left their phone behind by requiring the user to submit a selfie within 20 minutes of receiving a random check-in text message several times per day. The application shares data with a number of government agencies and the police, which fines a total of €6,550 for breaking quarantine.[25]

Efficacy questions abound. The application was launched after three days of development off a cookie-cutter application design and crashes frequently. Exceptions exist for those who claim poor Internet connectivity or no smartphone. The app frequently freezes or fails to send the required selfie, causing stress when the time permitted and the time displayed disagree. One user reported that the police cleared him to leave quarantine while the app continued to request selfies. Poland is the only example we found that required some form of facial recognition to validate location. It is also an interesting example where implementation quality raises further privacy concerns. Even if the government guaranteed no data storage of submitted selfies, the frequency and variety of app failures implies vulnerabilities and design gaps in the app itself as well as in storage or transfers of data.

Taiwan

The country of Taiwan has received much acclaim for its handling of the coronavirus. It combined rapid response, policy flexibility, and technological innovation to contain the virus and reported no new cases on April 14th, 2020. It saw just 393 confirmed COVID-19 cases and reduced new cases to zero within 36 days.[26]

Taiwan does not use GPS to track a person's location, but instead relies on the relative signal strength of a single cell reception tower to understand if someone under quarantine is remaining at

[23] (2020, April 7). Contact Tracing Could Free America From Quarantine - The .... Retrieved May 3, 2020, from https://www.theatlantic.com/ideas/archive/2020/04/contact-tracing-could-free-america-from-its-quarantine-nightmare/609577/
[24] Updates on COVID-19 in Korea (as of 14 March) | Press .... Retrieved May 3, 2020, from https://www.cdc.go.kr/board/board.es?mid=a30402000000&bid=0030&act=view&list_no=366553
[25] (2020, April 2). Poland's coronavirus app offers playbook for ... - Politico EU. Retrieved May 3, 2020, from https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/
[26] (2020, April 14). Taiwan Reports No New Coronavirus Cases, Adding ... - NPR. Retrieved May 3, 2020, from https://www.npr.org/sections/coronavirus-live-updates/2020/04/14/834431383/taiwan-reports-no-new-coronavirus-cases-adding-to-success-in-fighting-pandemic

home.[27] If the signal strength changes dramatically, drops off, or if the cellphone begins pinging a different tower, it can be confidently assumed that the person has moved from their assigned quarantine home. In this case, first responders are dispatched to the user's home but only receive the person's name, phone number and address to minimize privacy infringement necessary for enforcement. The country cites a 1% false alarm rate[28] and is partnering directly with telecom service providers to reduce errors further.

The mandatory electronic fence is being applied to infected individuals and travelers entering from abroad, impacting both citizens and non-citizens. The police will call the phone twice a day to ensure the individual has not just left their phone at home. There have been anecdotal reports that zero phone movement will also trigger a notification to the police as another method to identify if the person has left their phone at home. Breaking quarantine results in a fine of 1,000,000 NTD (~$33,000 USD).[29]

Mandatory quarantine for patients and travelers is a strict response that most Western governments have avoided to date. This question strikes at the core of how much power is given to the government during war or pandemics. Under what circumstances should the government have the power to restrict the movement of its citizens? The answer varies by each country's cultural relationship with their government and liberal philosophy. The Taiwanese government deserves credit for restricting location tracking to those reasonably impacted by COVID-19 – instead of instituting mass surveillance, as China did – and for finding a functional alternative to blanket GPS tracking through the creative use of cell phone tower pings.

Singapore

Singapore had the first successful national implementation of Bluetooth-based digital contact tracing and became a model for other nations. The app TraceTogether was developed by Singapore's Ministry of Health and Government Technology Agency (GovTech) and has seen adoption by 20% of the city-state's citizens, over 1.1 million people.[30] Adoption was slower than desired, reaching 12% of the population on April 1 and 20% by April 30th.[31] Singapore's prime minister Lee Hsien Loong mentioned TraceTogether in an April 21st remark to the nation, imploring more citizens to download the app.[32]

TraceTogether collects a single piece of personal information – your phone number – so that health officials can contact you faster in case of suspected exposure. TraceTogether collects anonymized app analytics data to improve performance, though they only list device model and app version on their website.[33] Interaction lists are stored for 21 days before deletion and require consent given to the Minister

[27] (2020, April 8). Taiwan's digital fence technologies dra... | Taiwan News. Retrieved May 3, 2020, from https://www.taiwannews.com.tw/en/news/3912429

[28] (2020, March 31). Taiwan phone tracking system monitors 55,000 under ... - Quartz. Retrieved May 3, 2020, from https://qz.com/1825997/taiwan-phone-tracking-system-monitors-55000-under-coronavirus-quarantine/

[29] (2020, March 27). Taiwan is using a phone location "electronic fence" to help .... Retrieved May 3, 2020, from https://www.privateinternetaccess.com/blog/taiwan-is-using-a-phone-location-electronic-fence-to-help-police-track-quarantined-individuals/

[30] TraceTogether. Retrieved May 3, 2020, from https://www.tracetogether.gov.sg/

[31] (2020, April 22). Contact tracing is well underway in Asia. What can the ... - Vox. Retrieved May 3, 2020, from https://www.vox.com/recode/2020/4/18/21224178/covid-19-tech-tracking-phones-china-singapore-taiwan-korea-google-apple-contact-tracing-digital

[32] (2020, April 21). PM Lee Hsien Loong on the COVID-19 situation in ... - PMO. Retrieved May 3, 2020, from https://www.pmo.gov.sg/Newsroom/PM-Lee-Hsien-Loong-address-COVID-19-21-Apr

[33] (2020, March 20). What data is collected? Are you able to see my personal data .... Retrieved May 3, 2020, from https://tracetogether.zendesk.com/hc/en-sg/articles/360043735693-What-data-is-collected-Are-you-able-to-see-my-personal-data-

of Health before the data is publicized. They list a support website you can email to revoke your data storage consent at any time. However, Singapore does have a legal requirement that any person who tests positive and is contacted by the Minister of Health must help the department in mapping their activity and movements. TraceTogether says this legal requirement applies to location timelines and logs in physical or digital form, including presumably what the application collects.[34]

Australia

Australia is a notable example because of the rapid pace of adoption by a Western democracy. The country's app Covidsafe requests the user's age range, postcode, phone number and name, though you can provide a pseudonym.[35] The information is centrally stored on a government server and the app uses Bluetooth to record close interactions, which are stored locally on phone for 21 days. If the user tests positive for COVID-19, they can elect to share their interactions from the past 14 days with the government. The government has been explicit that police will not have access to government-stored data and this requirement will be backed up by legislation to be introduced in May to the Australian parliament. The Australian app is derived from the source code for Singapore's app, with one change that allows iPhone users to lock their phone with the app open and still have it running.

The prime minister has vocally said that the app relies on consent, is not mandatory and has spun up a public awareness campaign to encourage sign-ups. He has also stated it will be a criminal offence to refuse service or venue access to any Australian citizen who chooses not to use the app, a strong statement in defense of consent. The Australian health minister has said the government was targeting 40% adoption. In the first 24 hours after launch, over two million Australian citizens downloaded the application, around 10% of the population and 25% of the adoption goal.[36] That is the largest non-mandatory application use rate in the West and a testament to the trust citizens will place in their government when they hold privacy and security foremost in the design and communication of technology initiatives.

Germany

Germany is pursuing a decentralized Bluetooth-based approach but has arrived at this solution only after strong continental debate.[37] Its initial plan was to follow the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) Bluetooth-based design launched on April 1st.[38] The pan-European research team gained momentum early and had 10 countries committed to launching its protocol, including Switzerland and Spain, before a major privacy debate began in Europe on the extent of centralization of

[34] (2020, March 22). Can I say no to uploading my TraceTogether data when .... Retrieved May 3, 2020, from https://tracetogether.zendesk.com/hc/en-sg/articles/360044860414-Can-I-say-no-to-uploading-my-TraceTogether-data-when-contacted-by-the-Ministry-of-Health-

[35] (2020, April 30). Covidsafe app: how to download Australia's coronavirus .... Retrieved May 3, 2020, from https://www.theguardian.com/australia-news/2020/apr/30/covid-safe-app-faq-review-how-to-download-australian-government-covidsafe-tracing-download-install-ios-app-store-iphone-phone-number-google-play-android-australia-coronavirus-tracking

[36] (2020, April 27). Government's coronavirus app take-up 'amazing': Murphy .... Retrieved May 3, 2020, from https://www.canberratimes.com.au/story/6736687/covid-19-tracing-app-take-up-amazing/

[37] (2020, April 20). PEPP-PT vs DP-3T: The coronavirus contact tracing privacy .... Retrieved May 3, 2020, from https://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear

[38] pepp-pt/pepp-pt-documentation: Documentation for ... - GitHub. Retrieved May 3, 2020, from https://github.com/pepp-pt/pepp-pt-documentation

data necessary. An opposing framework called Decentralized Privacy-Preserving Proximity Tracing (DP-3T) functions similarly but only uses a central server for communication of the interaction lists of confirmed cases and processes all token generation and list comparisons on each user's phone.[39] DP-3T is similar to the TCN Protocol announced by Stanford and Waterloo in the United States.

Legally, DP-3T argues that PEPP-PT fails to follow the General Data Protection Regulation (GDPR) principle for data minimization. Over 300 European academics signed a letter stating that centralization was unnecessary and further that GPS alternatives lacked sufficient accuracy.[40] PEPP-PT researchers did themselves no favor by failing to act transparently during development. They failed to publish code or protocols for review, failed to answer questions related to decentralization at press conferences and removed mentions to alternative frameworks from its documentation as those frameworks gained momentum. Their attitude during debate led to some calling them a "trojan horse" for mass government surveillance.[41] While the spirited debate and specificity of privacy advocates is commendable, the decision behind frameworks rested ultimately on Apple and Google. As the system developers, their support for the DP-3T method and refusal to change platform rules to allow background Bluetooth tracking and transmission to an external server forced Germany's hand. As a result, following a full vote by the European Parliament, Germany and Europe are officially pursuing the most stringent privacy-preserving digital contact tracing option.[42]

Simulating Application Penetration and Compliance for Policymakers

Our qualitative study of the various implementations pursued by national governments or designed by academic institutions suggests that Bluetooth-based contact tracing solutions are at least as effective as GPS-based solutions while preserving the privacy of the user to a much greater extent. There is also a strong argument that Bluetooth solutions are more accurate, as their signal is impacted by physical barriers and vertical space, eliminating common false positives from GPS. European and American researchers have argued the privacy merits of various approaches and swayed expert opinion towards the decentralized implementation of Bluetooth interactions. While America's relative lack of data protection laws has allowed for early momentum of GPS apps like MIT's SafePaths, the announcement by Apple and Google that they will be implementing an opt-in Bluetooth digital contact tracing API will enable an installed user base so large that it cannot be ignored by public health officials. This decision solidly shifts digital contact tracing towards the most privacy preserving option as the default.

With the selection of this technology, the next concern for policymakers should be the adoption rate necessary for containment and disease management. Specifically, what is the percentage of the population that must activate digital contact tracing such that the method outpaces the virus' transmission rate? To answer this question, we turn to a quantitative assessment of the efficacy of application adoption and compliance and its impact on the spread of disease.

---

[39] Decentralized Privacy-Preserving Proximity .... Retrieved May 3, 2020, from https://github.com/DP-3T/documents

[40] (2020, April 19). Various researchers. Retrieved May 3, 2020, from https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view

[41] (2020, April 17). Europe's PEPP-PT COVID-19 contacts tracing standard push .... Retrieved May 3, 2020, from https://techcrunch.com/2020/04/17/europes-pepp-pt-covid-19-contacts-tracing-standard-push-could-be-squaring-up-for-a-fight-with-apple-and-google/

[42] (2020, March 18). TA MEF - European Parliament. Retrieved May 3, 2020, from https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf

We have developed an epidemic simulation that models migration probabilities between private and public spaces and the associated infection rate within each. On top of that, we apply varying rates of application adoption and compliance rates in a grid search to output single-day maximum population-level infection rates. This represents the top of the curve. In order to successfully manage coronavirus, the American healthcare system must have sufficient capacity to handle the maximum single day caseload. By having our simulation find that maximum, we can determine if the combination of penetration and compliance will be sufficient.

We baseline our target population infection rate using hospital capacity in New York City. The CDC estimates a hospitalization rate among COVID-19 patients of 4.6 per 100,000 patients.[43] Bloomberg calculates an existing NYC hospital bed capacity of 23,000, with another 18,333 added in recent months using emergency measures.[44] Hospital capacity planners target 85% average occupancy[45] while New York City reported in 2018 utilization rates of 79.7% and 89.7% depending on the facility type.[46] Assuming the low end of utilization, even with the emergency beds, New York City would have just 8,390 free beds for COVID-19 patients. At those rates, New York City with a 2018 population of 8.4 million would require an infected population rate less than 21% for the hospital system to manage the patient load. To see if that target infection rate was possible, we tested the efficacy of adoption and compliance rates in multiple scenarios representing varying city densities and policy decisions.

First, we simulated epidemic transmission through a city under stay-at-home orders compared against a city with unrestricted mobility. We set probability of leaving one's private residence at 35% under stay-at-home orders, as this is the mobility rate Google quotes for France, a Western country that implemented mandatory stay-at-home and so can be assumed to have similar city design as an American city and high stay-at-home compliance.[47] We set unrestricted mobility probability at 95%, applying some discount from 100% for those with limited ability to leave, such as the sick or elderly.

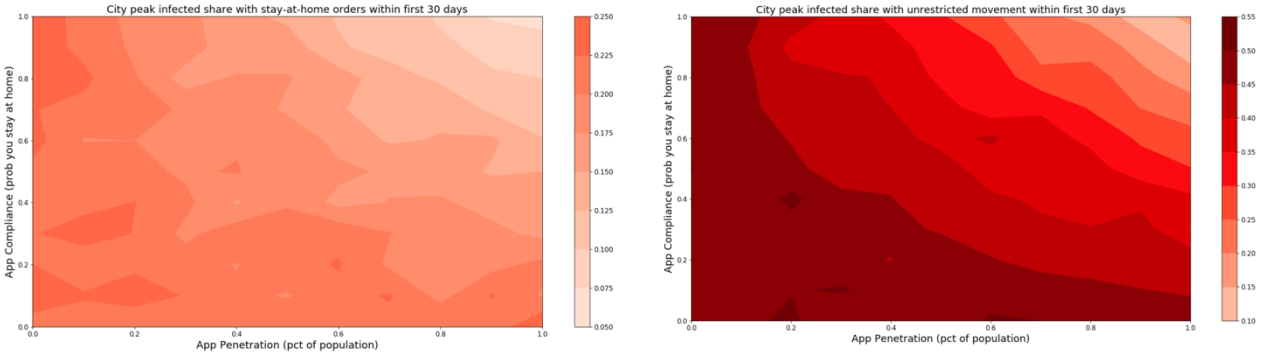

Exhibit 1: Infection Rates with Stay-At-Home orders (left) and Unrestricted Movement (right)

[43] "Hospitalization Rates and Characteristics of Patients ... - CDC." https://www.cdc.gov/mmwr/volumes/69/wr/mm6915e3.htm. Accessed 3 May. 2020.

[44] "New York Coronavirus: How Many Hospital Beds ... - Bloomberg." https://www.bloomberg.com/graphics/2020-new-york-coronavirus-outbreak-how-many-hospital-beds/. Accessed 3 May. 2020.

[45] "How Many Hospital Beds? - SAGE Journals." https://journals.sagepub.com/doi/pdf/10.5034/inquiryjrnl_39.4.400. Accessed 3 May. 2020.

[46] "Health and Hospitals – Hospital Utilization Report." https://council.nyc.gov/budget/wp-content/uploads/sites/54/2019/02/Health-and-Hospitals-Hospital-Utilization-Report.pdf. Accessed 3 May. 2020.

[47] (2020, April 17). Google, COVID-19 Community Mobility Report, France. Retrieved May 3, 2020, from https://www.gstatic.com/covid19/mobility/2020-04-17_FR_Mobility_Report_en.pdf

Our results show that stay-at-home orders remain one of the most effective means of containing COVID-19 transmission. A low probability of leaving your home reduces the maximum single-day infection rate significantly at every parameter test and nearly all levels would be manageable by the health care system. High infection only occurs in the corners where compliance or app penetration is very low. With unrestricted movement, app penetration needs to be greater than 70% and compliance above 60% to hit the requisite level.

Second, we wanted to compare application impact in various cities with differing private-to-public ratios and densities. We selected New York City (New York), Austin (Texas) and Omaha (Nebraska) as our three cities representing dense cities with high public-to-private building ratios, sprawling cities with low ratios and an averagely dense American city, respectively. We took the number of households from the United States Census Bureau. To peg our selection of "public spaces" to a shared and easily confirmable statistic, we identified the number of National Historic Landmarks present in each city. While these are not necessarily highly frequented locations, they provide an effective proxy for the public-to-private ratio we were concerned with modeling.

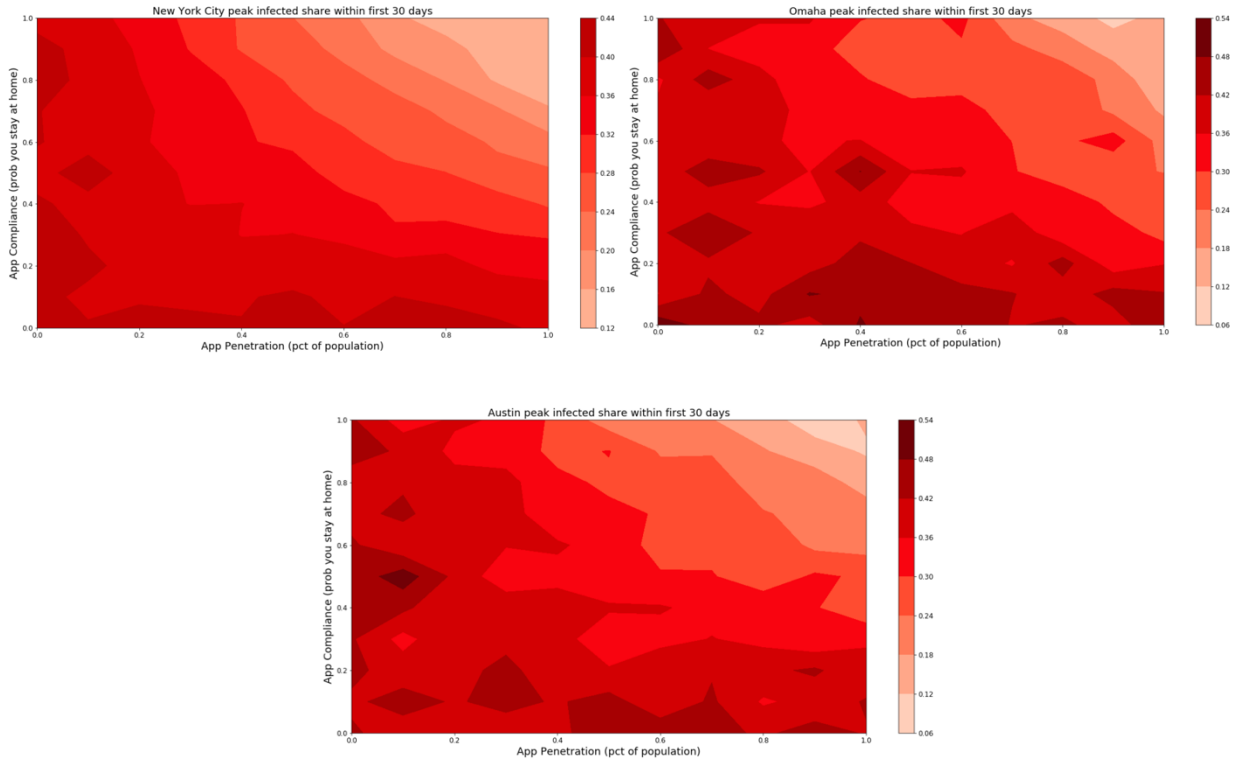

Exhibit 2: Infection Rates in cities like New York (top left), Omaha (top right) and Austin (bottom)

In a dense city like New York, with a high public-to-private space ratio, app penetration needs to be around 50% with compliance at least 60% to maintain an infected population rate near 20%. Omaha, a more average American city, would require higher app penetration near 70% but compliance can be lower at 50%. Austin, a more sprawling city comparatively, could make do with 40% penetration but still requires 60% compliance.

Concluding Remarks

Pandemics introduce threats to privacy as the tracking of citizens is core to the public health response to any outbreak. The proliferation of digital technology like smartphones has made the potential for tracking easier, but without clear design and policy choices, this tracking takes away privacy rights of a country's citizens and risks scope creep once the pandemic is contained. The argument to keep these powers in case a new pandemic appears at any time is a seductive one. Fortunately, in the response to COVID-19, privacy advocates in the United States and Europe have risen to the challenge and defined systems that accomplish public health goals while respecting user privacy. Their impact can be seen in the decisions by Apple and Google to make the strictest Bluetooth-based privacy design the default option for digital contact tracing in their underlying mobile systems.

Our quantitative study found that when travel is unrestricted fairly high rates of app penetration and compliance will be required (minimums of 40-60% and 50-60% respectively) to maintain a sufficient patient load for a hospital system. Stay-at-home orders and social distancing help dramatically in maintaining lower enough infection rates. To hit these high numbers, policymakers should follow the example of countries like Australia and Singapore and emphasize that strong privacy restraints are built into any application to encourage download and compliance. Digital contact tracing can become an incredible example where strict user privacy was maintained simultaneously as a major leap in technological innovation and capability was made to fight the deadly COVID-19 virus.