TIP
Tech Informed Policy

JUNE 11, 2020

COVID-19 RAPID TECHNOLOGICAL BRIEFING

The differences between contact tracing and exposure notification

Produced by

Taylor Owen, Policy Lead, Beaverbrook Chair in Ethics, Media and Communications, Director of the Centre for Media, Technology and Democracy, and Associate Professor in the Max Bell School of Public Policy, McGill University

Derek Ruths, Tech Lead, Director of the Network Dynamics Lab and Associate Professor of Computer Science, McGill University

Stephanie Cairns, Research Assistant

Sta Kuzviwanza, Research Assistant

Sara Parker, Research Assistant

Sonja Solomun, Research Director, Centre for Media, Technology and Democracy, McGill University

Kate Gilbert, Graphic Designer

Centre *for* MEDIA, TECHNOLOGY *and* DEMOCRACY

network dynamics @mcgill
measuring and predicting large-scale human behavior

ABOUT TIP

Tech Informed Policy (TIP) is an initiative spearheaded by two leading McGill researchers—Dr. Derek Ruths, Director of the Network Dynamics Lab and Associate Professor of Computer Science, and Dr. Taylor Owen, Beaverbrook Chair in Ethics, Media and Communications, Director of the Centre for Media, Technology and Democracy, and Associate Professor in the Max Bell School of Public Policy. TIP aims to demystify the technology underlying critical policy issues and to provide valuable, tech-based recommendations to Canadian policymakers.

For enquiries, please contact Derek Ruths.

Glossary of Terms

Application Programming Interface (API): An API provides a framework for developers to create their own programs. It is a collection of potential operations that programmers can develop to suit their needs.

Bluetooth: A wireless technology used to transmit data between devices in a close range.

BLE: Bluetooth Low Energy (BLE) has a very low power consumption and is ideal for transmitting small amounts of data periodically.

Central Server: A computer system that provides services to multiple users. A server may also store and control access to data or other resources.

GPS: Global Positioning System (GPS) uses satellites to determine the latitude and longitude of an object.

ID: A contact ID is a series of randomized characters broadcasted by a user's device throughout the day. Upon encountering another user, their IDs are exchanged and then stored in their respective contact logs. If a user later tests positive for COVID-19, their IDs from the previous 14 days are cross-referenced with those in other contact logs, so users who came into contact with the infected user can be notified.

Token: A token generates each user's contact IDs. With EN, the user's device creates a new token every day, which then generates IDs that are broadcast throughout the day. With CT, the server creates a new token every day, and that token then generates IDs for every connected device.

EXECUTIVE SUMMARY

The purpose of this rapid response briefing is to provide an overview of the differences between contact tracing and exposure notification, and outline the current options for these technologies. We summarize the technical differences between the two approaches, and review the security and privacy risks, adoptability, and feasibility of three technologies:

1. GPS-Based Contact Tracing
2. Bluetooth Low Energy (BLE) Based Contact Tracing
3. BLE-Based Exposure Notification (Apple/Google model)

Should the federal government implement or endorse a contact tracing or exposure notification technology, this briefing recommends Bluetooth-based exposure notification. Federal decision-making will require a careful balance between public health and safety, technological capacity, and privacy protection. COVID-19 apps require the collection of vast amounts of data; this can compromise personal privacy and increase security risks, as individuals may be more easily identified or have their personal information (particularly sensitive health information) exposed. Location data of any kind is highly sensitive and can never be fully anonymized; even de-identified[1] location data can be used to re-identify[2] individuals, often from only a few data points.[3] In addition to securing privacy, strong data protection is an integral mechanism for ensuring public trust and adoptability. The capacity of any pandemic response technology should be rigorously weighed against its democratic impact and possible unforeseen (mis)uses.

MODEL	DEFINING FEATURES	EVALUATION
GPS Contact Tracing	Collects exact location data Tracks outbreaks	**Feasibility: Low** Inaccurate GPS results likely **Security/Privacy: Bad** High risk of user re-identification; app vulnerable to hacking
BUY-IN: UNLIKELY		
Bluetooth Contact Tracing	Collects general location data Bluetooth records encounters Central server notifications	**Feasibility: Low** App only works when open **Security/Privacy: Mediocre** Some risk of user re-identification; app vulnerable to hacking
BUY-IN: POSSIBLE		
Apple/Google Exposure Notification	No location data collected Bluetooth records encounters Individual device notifications	**Feasibility: High** App works continually **Security/Privacy: Good** Low risk of user re-identification; app not vulnerable to hacking
BUY-IN: LIKELY		

ISSUE

Manual contact tracing, the process of identifying exposed individuals who have come into contact with diagnosed individuals, has been shown to be effective in containing outbreaks of Ebola,[4] SARS,[5] and tuberculosis.[6] In the past weeks, digital contact tracing has been employed by some countries with the aim of preventing resurgences of COVID-19 outbreaks or monitoring infected and high-risk persons. However, countries like Australia[7] and Singapore[8] have since reported that digital contact tracing apps have not been effective.[9] Exposure notification, the process by which users are notified if they have come in contact with an infected individual, has gained popularity following Apple/Google's roll out of a Bluetooth exposure notification framework. Exposure notification claims to better protect users' privacy and security than digital contact tracing, which could encourage a higher adoption rate. Understanding the differences between digital contact tracing and exposure notification and their risks can help inform which technologies to endorse, develop, or restrict.

CONTACT TRACING VS EXPOSURE NOTIFICATION

Both digital contact tracing and exposure notification rely on GPS or Bluetooth Low Energy (BLE) technology on individuals' smartphones to notify users who were in the proximity of someone who was diagnosed with infection. High adoption rates are critical; an estimated 60% of residents must download and use the app for virus-curbing efforts to succeed.* [10] There is currently limited evidence of countries meeting adequate adoption rates without mandated use.[11] They key difference between the two approaches is that contact tracing is centralized, while exposure notification is decentralized. In contact tracing, a central body, such as a government health agency, has access to the data collected by the app, enabling them to track outbreaks. With user consent, this information can also be used to further epidemiological research.

In an exposure notification model, users are likewise informed if they have come in contact with an infected individual, but no central body has access to this information. This puts the responsibility for how to respond to exposure (by self-isolating, getting tested, or self-reporting) in the user's hands. Exposure notification is less invasive and more secure, but it also makes uniform responsiveness and compliance less certain. Expert reviews of contact tracing and exposure notification have found several technical limitations of these models, including imprecision in detecting 'contact' and in detecting distance between people, which could lead to high numbers of false positives and false negatives.[12] Any application is thus best mobilized in conjunction with other public-health policies. For exposure notification in particular, the individual compliance to an alert suggesting self-isolation for instance, would depend upon users' proximity to essential resources[13] and other conditions of employment[14] and home life.[15]

* This points to a larger problem of digital exclusion; those who have smartphones and the digital skills to use the application correctly will be differently affected than children without cellphones, the elderly, and those from low income households (including users with inconsistent access to internet and/or data plans).

OPTIONS

1. GPS-BASED - CONTACT TRACING

What is it?

In a GPS model, users' location data is shared with health authorities in order to help control outbreaks. This model prioritizes information gathering at the expense of privacy protection.

How does it work?

The app shares users' anonymized location information with health authorities.** If a user tests positive for COVID-19, health authorities can plot their movements, notify other users who have recently visited the same locations, and disinfect public spaces as needed.

What does it accomplish?

Users are notified if they have frequented a potentially infected area. As the virus has been shown to linger on surfaces,[16] this method is potentially more effective than simply notifying users if they have come in close proximity with an infected individual. The GPS model also provides health authorities with specific location data, enabling them to monitor outbreaks as they occur.

Who's doing it?

Qatar and India are among the countries to have incorporated GPS into their digital contact tracing efforts. Qatar's mandatory app uses both GPS and Bluetooth for contact tracing through a central database. A major security flaw identified by Amnesty International (and since remedied) would have allowed malicious actors access to highly sensitive personal information, including the names, national IDs, health status, and location data of more than a million users.[17] India's mandatory app allows users to check whether someone in their area is infected. Privacy experts quickly identified a fundamental failing in its design: hackers can easily pinpoint who reports a positive diagnosis.[18]

Some US states are embracing location-tracking as well. Utah's app reported an adoption rate below 2% one month after deployment.[19] North Dakota has two apps[20]—an exposure notification app incorporating Apple/Google's API which is still in development, and a location-based app which has been sharing personal data with private companies.[21] The risks to security, reliability, and functionality[22] of a state-by-state approach are a caution to other countries considering similar solutions.

Privacy and security

Centralized GPS models may open up potential data misuses since they collect massive volumes of data and afford governments and/or primary authorities—who are not infallible to data and security breaches[23]—greater access to that data than other models. Collecting the location data needed to plot user movements and using a centralized server to store and process information can significantly compromise user anonymity.[24] Location data is typically considered a special legal category with unique protections[25] since it can be used to identify a user's home, workplace, or school, revealing highly sensitive identifying information regarding a person's professional, political, religious, or sexual orientations.[26] Even aggregated location datasets present privacy challenges to the public.[27] Centralized models may be especially prone to "mission creep" or unintended uses of collected data,

** As outlined above, location data can never be fully anonymized. Any subsequent reference to anonymized data in this briefing should not be understood in absolute terms (see "Privacy and Security" below).

which can damage the effectiveness of the apps and belie public trust and adoption rates. Centralized models are contingent on the assumption that only a “trusted authority” will be using sensitive data without misuse, with no possible guarantees.[28] [29]

Social buy in

The use of GPS and location data to track and surveil populations has been shown to directly violate users’ privacy and cause undue harm and discrimination, especially toward vulnerable groups.[30] The sensitive nature of health-related data and the scale of its collection in this context would likely exacerbate known risks. The lack of anonymity inherent to location data, coupled with a growing distrust of technology companies,[31] implies that such an app would be met with skepticism if not outright condemnation. The susceptibility to hacking of existing international GPS-based apps outlined above might further motivate Canadians to reject a GPS model.

Feasibility: low

Apple and Google have banned developers from using GPS in conjunction with their BLE model (see: Section 3. Bluetooth Low Energy - Exposure Notification). Even if this were not the case, the technology would be prone to numerous false positives. GPS pinpoints location by using only latitude and longitude, so it does not account for height. This could lead to numerous false positives, as a GPS-reliant application would deem users to be in close proximity, even if they were numerous floors away from each other in a high rise building.

2. BLUETOOTH LOW ENERGY (BLE) BASED CONTACT TRACING

What is it?

The app uses BLE to signal nearby devices. When two devices come into close proximity, they exchange anonymized IDs (long sets of randomized characters) which are then stored in contact logs on their individual devices. Upon diagnosis, users may voluntarily upload their contact logs, along with their general location (e.g. first half of their postal code), to a central server, allowing health authorities to track outbreaks and alert other users if they have come into contact with an infected individual. Variations of this model are possible; for instance, artificial intelligence (AI) may be used to predict a user’s unique risk.

How does it work?

The following describes a standard contact tracing model, based on the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) protocol.[32]

Set up – A central server maintained by health authorities periodically generates a global secret token. This token generates a list of IDs (long strings of randomized characters) for each individual app to broadcast throughout the day.

Stage 1 – Encounter logging: using BLE, apps ping each other when two devices come in close proximity. The apps exchange IDs and record the encounter in their contact log, along with metadata like the time and signal strength (which correlates with the physical distance of the devices).

Stage 2 – Infection reporting: Pending manual verification of positive diagnoses by health authorities, infected users will be encouraged to upload their contact log (with its associated metadata) to the central server. The server verifies the list of contacts using an algorithm to reduce false positives. The server will then communicate with individual devices, and users will be notified of potential infection through their device. Users may also be asked to provide their location, through either approximate (half a postal code) or more exact measures, both when reporting a diagnosis and upon notification of possible infection. This data is what allows health authorities to track the spread of the virus.

An app that uses Artificial Intelligence (AI) would determine the probability that a user is infected based on their locations, interactions, and other risk factors. If a user is deemed by the algorithm to be high risk, the app would recommend testing. The test results would be used to "train" the app to more accurately predict users' risk of contracting COVID-19. The use of AI would demand massive amounts of personal data beyond contact logs or general location. Users would likely be asked questions about their medical history, age, and behaviour.

What does it accomplish?

Bluetooth contact tracing produces similar results to GPS contact tracing: notifying users of possible infection and giving health authorities and epidemiologists access to information that could be used for infection tracking.

Who is using it?

The UK will launch a Bluetooth contact tracing app in June, having rejected Apple/Google's approach.[33] Privacy campaigners are gearing up for a legal challenge in response to Public Health England's revelation that personally-identifiable data collected by the UK's manual contact tracing system will be retained for 20 years.[34] Data retained by the app will additionally be studied using AI not only to advance epidemiological research but also to provide users with individual risk assessments.[35] France also recently launched its own contact tracing app,[36] while the majority of other European nations endorsed Apple/Google.[37] While both countries employ a centralized framework with contact logs being uploaded to a central server, only the UK's app collects location data (partial postcode).

Technology, security and privacy experts have raised significant concerns about both apps. In France, 471 cryptography and security researchers (77 of whom are directly affiliated with Iria, the French app's developer) have emphasized the privacy vulnerabilities inherent to both contact tracing and exposure notification and called for greater transparency and oversight for the app.[38] Singapore's Bluetooth app, praised for its rapid deployment and apparent initial success, has only been downloaded by 25% of residents,[39] with many citing privacy concerns[40] and poor functionality since the app only works on Apple devices if it is kept open at all times.[41]

Privacy and security

Over 300 academics across 26 countries strongly argued against a centralized contact tracing model, jointly outlining its vulnerability to security breaches, massive data collection, and possible surveillance after the pandemic, given inadequate legislative protections.[42] This kind of "mission creep" (unintended app use or data abuse) could exert an overextension of government power and surveillance. Moreover, since contact logs are uploaded to the server, malicious actors would only need to target the central server. IDs generated by global tokens stored in the server could be decrypted to re-identify the users listed in the logs. To successfully perform contact tracing, authorities must request location information. Since even general, area-based location data can readily re-identify users, authorities will have access to highly sensitive identifying information. Experts have also warned that such apps could result in security threats and potential for wrongful surveillance of users' devices since Bluetooth signal is openly broadcast.[43]

For apps using additional AI technology in their models, privacy and security risks are greater. AI-based apps require large amounts of users' personal data, including location, age, and health data. The privacy of the user may then be more easily compromised, as the larger volume of data may make it easier for a user to be identified.

Social buy in

Although Canada's Health Minister has indicated that some regions are reluctant to endorse a nationwide app,[44] surveys have revealed broad public support for an undefined contact tracing or exposure notification app. Two separate polls have reported favourability rates as high as 80%.[45] [46] A KPMG poll has even found that a majority of respondents (60%) would willingly forfeit their privacy to stop COVID-19, though nearly all believe the app should balance privacy with public safety.[47]

Until an app is officially endorsed, this support remains untested and likely contingent on the app's usability and on the public and expert-level discourse surrounding its risks. The aforementioned 300 security experts claim that this model would be directly perceived as an invasion of personal privacy by the public of 26 different countries.[48] As it is impossible to fully safeguard the app from malicious actors or ensure total anonymity, citizens may be reluctant to expose their information, potentially compromising adoption rates. This is the case in Australia,[49] Norway,[50] and Singapore,[51] all reporting low adoption rates despite receiving initial praise as successful models of rapid adoption.

Feasibility: low

Apple has blocked the use of background Bluetooth when data collected by an application is moved off the device,[52] so any platform using a centralized server will be infeasible. Alberta's application, ABTraceTogether, is indicative of this problem: the application can only work when the phone is open on the app,[53] and therefore has little ability to accurately trace contact. Various countries, including France, have asked Apple to lift the ban, but Apple has refused to do so.***

3. BLE-BASED EXPOSURE NOTIFICATION (APPLE/GOOGLE MODEL)

What is it?

Like in contact tracing, the app uses BLE to signal nearby devices. But, unlike in contact tracing, each user's contact log is stored only on their individual device. Only the anonymized tokens of those diagnosed are uploaded to a central server. This model aims to minimize privacy risk through better data protection.

*** This points to an important policy question regarding the need for sunset provisions (time limitations for law and policy) to safeguard the already demonstrable inability to overturn private decision making about public health and security. While current technical decisions support wider adoption now, public policy will need to safeguard future re-purposing.

How does it work?

The following describes Apple/Google's exposure notification model,[54] which is based on the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) protocol.[55]

Set up – Unlike in contact tracing where the server creates global tokens, each individual app periodically generates a new secret token. This token is used to spawn IDs that the app broadcasts to nearby devices.

Stage 1 – Encounter logging: When two users approach each other, their devices exchange IDs over BLE. These IDs, along with metadata like physical distance and time, are stored in the users' respective contact logs. Encounter logging is an identical process in both BLE contact tracing and exposure notification models and is laid out in Apple/Google's API.

Stage 2 – Infection reporting: Like with contact tracing, a central server is maintained by health authorities and a user may voluntarily upload a report upon diagnosis. However, this report does not contain their contact log, but only their tokens from the previous 14 days. Other devices download the report, use the tokens to generate the same IDs as the original device, and then compare the IDs to those stored in their logs. A user who has come into proximity with an infected person is thus notified of this encounter without health authorities ever accessing contact logs. The implementation details of Stage 2 are left to individual app developers.

What does it accomplish?

The application notifies users when they have come into contact with someone who has tested positive for COVID-19. Users are then encouraged to self-report this potential contact to the relevant health authorities. While exposure notification does not provide health authorities with data about movement patterns like contact tracing, an exposure notification app ensures a greater degree of user privacy and autonomy over their health information. As users are encouraged to self-report their infection or possible exposure, epidemiological research is still possible, if clear opt-in is provided for users to share specific data for clearly defined epidemiological purposes.[56]

Who is using it?

Switzerland[57] and Italy[58] have deployed apps incorporating this framework. While 70% of Swiss residents intend to download their country's app,[59] only 44% of Italians[60] say they will probably or certainly download theirs. Other European countries, including Germany, Latvia and Estonia,[61] are preparing to roll out their own Apple/Google-based apps in the coming weeks. Several US states and a total of 23 countries have requested[62] Apple/Google's API.

Privacy and security

Decentralized models are heavily endorsed by global technology companies, who are not without private interests. They have also gained widespread popularity among independent experts.[63] Decentralized exposure notification does not require contact logs nor location data to ever be centrally stored, limiting governments and health authorities access to users' personal information. Instead, contact logs remain on individual devices, and location data is never recorded. Decentralization increases security by lowering the risk of security breaches and attacks on distributed devices. If a malicious actor hacked one device and procured its contact log, the IDs in the log would be undecipherable without first obtaining each user's secret tokens. As these tokens are generated and stored on individual devices an attacker would need access to thousands of devices. Likewise, an attack on the central server where tokens of infected users are uploaded would still require access to individual devices in a given area in order to identify a user's contacts. In a decentralized model, security breaches are less convenient, but not impossible.[64]

Social buy in

Theoretical support exists for an unspecified Bluetooth-based app, as presented in Section 2 (Bluetooth Low Energy - Contact Tracing). A new study conducted by Ryerson University suggests that a small majority of Canadians even support a mandatory exposure notification app in workplaces and when accessing public services like public transit.[65] Exposure notification systems, with their emphasis on privacy, will likely be better able to capitalize on that initial public trust and foster sufficiently high adoption rates.

While decentralization addresses security and privacy more thoroughly than other available options, research has shown it remains open to potential abuse of and risks to verifiability.[66] Voluntary exposure notification apps could also produce numerous false alerts, thereby affecting the reliability of the app.[67] False positives can arise with any option discussed, but exposure notification may lead to low-risk alerts because of the lesser degree of health authority intervention in distributing exposure notifications. These warnings may eventually undermine the perceived efficacy of the app and affect continued use and adoption.[68]

Countries adopting the Apple/Google API will need to contend with the power they delegate to private companies over public health and security, especially as companies have already rejected demands from other federal governments relating to contact tracing.[69] Since clear terms of use and explanation of data collection is the mandate of individual developers, governments using the Apple/Google API must ensure companies comply with strict provisions of use and purpose, data governance, and privacy protections. The power of the government against tech monopolies will undoubtedly affect public opinion and may affect adoption rates, especially considering Canadian citizens' vocal rejection of Google's Sidewalk Labs.[70] Social buy-in of any option is also directly influenced by the inclusion of a testing phase before complete deployment. This would allow governments to remedy and learn from any issues that may be unforeseen until actual use.

Feasibility: high

An exposure notification application following the Apple/Google model circumvents Apple's ban on background Bluetooth, and can therefore be downloaded on devices using iOS.[71] The API has already been requested by 23 countries for their own national exposure notification apps.[72]

REFERENCES

[1] Valentino-devries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik. “Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret.” The New York Times, December 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[2] Thompson, Stuart A., and Charlie Warzel. “Twelve Million Phones, One Dataset, Zero Privacy.” The New York Times, December 19, 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[3] Montjoye, Yves-Alexandre De, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. “Unique in the Crowd: The Privacy Bounds of Human Mobility.” Scientific Reports 3, no. 1 (2013). https://doi.org/10.1038/srep01376.

[4] “Contact Tracing.” World Health Organization, July 23, 2015. https://www.who.int/csr/disease/ebola/training/contact-tracing/en/.

[5] “Severe Acute Respiratory Syndrome (SARS) - Multi-Country Outbreak - Update 26.” World Health Organization, July 24, 2015. https://www.who.int/csr/don/2003_04_10/en/.

[6] “Contact Tracing Methods for Tuberculosis.” Contact tracing methods for tuberculosis. Accessed June 8, 2020. https://www.cochrane.org/CD013077/INFECTN_contact-tracing-methods-tuberculosis.

[7] Taylor, Josh. “NSW Is Unable to Use Covidsafe App’s Data for Contact Tracing.” The Guardian, May 19, 2020. https://www.theguardian.com/australia-news/2020/may/19/nsw-and-victoria-are-unable-to-use-covidsafe-apps-data-for-contact-tracing.

[8] “Why Aren’t Singaporeans Using the TraceTogether App?” South China Morning Post, May 18, 2020. https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether.

[9] Burgess, Matt. “Coronavirus Contact Tracing Apps Were Meant to Save Us. They Won’t.” Wired, May 1, 2020. https://www.wired.co.uk/article/contact-tracing-apps-coronavirus.

[10] Robert Hinch et al., *Effective Configurations of a Digital Contact Tracing App: A report to NHSX*, Oxford: Oxford University, 2020, 1, https://drive.google.com/file/d/1uB4LcQHMVP-oLzIIHA9SjKj1uMd3erGu/view.

[11] For instance, Australia has reported only a 14% adoption rate of their app COVIDSafe: Hogan, Stephanie. “What Is Contact Tracing? Here’s What You Need to Know about How It Could Affect Your Privacy.” CBC News, May 14, 2020. https://www.cbc.ca/news/canada/coronavirus-covid-19-contact-tracing-app-1.5558512.

[12] Ada Lovelace Institute, *Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis*. London: Ada Lovelace Institute, April 26, 2020 https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf.

[13] Deparle, Jason. “The Coronavirus Class Divide: Space and Privacy.” The New York Times, April 12, 2020. https://www.nytimes.com/2020/04/12/us/politics/coronavirus-poverty-privacy.html.

[14] Valentino-devries, Jennifer, Denise Lu, and Gabriel J. X. Dance. “Location Data Says It All: Staying at Home During Coronavirus Is a Luxury.” The New York Times, April 3, 2020. https://www.nytimes.com/interactive/2020/04/03/us/coronavirus-stay-home-rich-poor.html.

[15] Nicole Bogart, “Advocates scramble to help domestic abuse victims as calls skyrocket during COVID-19”, CTVNews, May 3, 2020, https://www.ctvnews.ca/health/coronavirus/advocates-scramble-to-help-domestic-abuse-victims-as-calls-skyrocket-during-covid-19-1.4923109.

[16] “Coronavirus Disease - Answers.” World Health Organization. Accessed June 8, 2020. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/coronavirus-disease-answers?gclid=EAIaIQobChMI9fmnmMXy6QIVA43ICh0hcAIwEAAYASAAEgKVzvD_BwE&query=how+long+does+it+stay+on+surfaces.

[17] “Major Security Flaw Uncovered in Qatar’s Contact Tracing App.” Amnesty International. Accessed June 8, 2020. https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/.

[18] Greenberg, Andy. “India’s Covid-19 Contact Tracing App Could Leak Patient Locations.” Wired. Accessed June 8, 2020. https://www.wired.com/story/india-covid-19-contract-tracing-app-patient-location-privacy/.

[19] Sonnemaker, Tyler. “Utah Reportedly Spent Nearly $3 Million on a Contact Tracing App That Less than 2% of the State’s Population Has Downloaded.” Business Insider, May 20, 2020. https://www.businessinsider.com/utahs-275-million-contact-tracing-app-few-downloads-report-2020-5.

[20] Johnson, Bobbie. “The US’s Draft Law on Contact Tracing Apps Is a Step behind Apple and Google.” MIT Technology Review, June 2, 2020. https://www.technologyreview.com/2020/06/02/1002491/us-covid-19-contact-tracing-privacy-law-apple-google/.

[21] Fowler, Geoffrey. “One of the First Contact-Tracing Apps Violates Its Own Privacy Policy.” The Washington Post, May 21, 2020. https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/.

[22] Greenberg, Andy. “State-Based Contact Tracing Apps Could Be a Mess.” Wired. Accessed June 8, 2020. https://www.wired.com/story/covid-19-contact-tracing-app-fragmentation/.

[23] "Personal Information Belonging to 144,000 Canadians Breached by Federal Departments and Agencies." CBC News, February 14, 2020. https://www.cbc.ca/news/politics/privacy-breach-canada-1.5457502.

[24] Montjoye, Yves-Alexandre De, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. "Unique in the Crowd: The Privacy Bounds of Human Mobility." Scientific Reports 3, no. 1 (2013). https://doi.org/10.1038/srep01376.

[25] Gray, Stacey. "A Closer Look at Location Data: Privacy and Pandemics." Future of Privacy Forum, March 25, 2020. https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/.

[26] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)

[27] Sly, Liz. "U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging." The Washington Post, January 29, 2018. https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html.

[28] "Examples of Abuse." Privacy International. Accessed June 8, 2020. https://privacyinternational.org/examples.

[29] Bennett, C. and Gebhart, G. (2020, May 12). Governments Shouldn't Use "Centralized" Proximity Tracking Technology. Electronic Frontier Foundation (EFF). https://www.eff.org/deeplinks/2020/05/governments-shouldnt-use-centralized-proximity-tracking-technology.

[30] "Data Harm Record." Data Justice Lab, December 9, 2017. https://datajusticelab.org/data-harm-record/.

[31] Edelman, *Edelman Trust Barometer 2020*, 2020, https://cdn2.hubspot.net/hubfs/440941/Trust%20Barometer%202020/2020%20Edelman%20Trust%20Barometer%20Global%20Report.pdf?utm_campaign=Global:%20Trust%20Barometer%202020&utm_source=Website.

[32] "Pan-European Privacy-Preserving Proximity Tracing." PEPP-PT. Accessed June 8, 2020. https://www.pepp-pt.org/.

[33] Chowdhury; Matthew Field; Margi Murphy, Hasan, Matthew Field, and Margi Murphy. "NHS Track and Trace App: How Will It Work and When Can You Download It? ." The Telegraph, June 8, 2020. https://www.telegraph.co.uk/technology/2020/06/08/nhs-app-trace-track-coronavirus-download/.

[34] Sabbagh, Dan, and Alex Hern. "Privacy Group Prepares Legal Challenge to NHS Test-and-Trace Scheme." The Guardian, May 31, 2020. https://www.theguardian.com/world/2020/may/31/privacy-campaigners-prepare-legal-challenge-to-uks-test-and-trace-scheme.

[35] Burgess, Matt. "There's a Big Row Brewing over the NHS Covid-19 Contact Tracing App." Wired, May 10, 2020. https://www.wired.co.uk/article/nhs-contact-tracing-app-data-privacy.

[36] "France Rolls out Covid-19 Tracing App amid Privacy Debate." France 24, June 2, 2020. https://www.france24.com/en/20200602-france-rolls-out-covid-19-tracing-app-amid-privacy-debate.

[37] "Europe pins hopes on smarter COVID-19 contact tracing apps", CNA, June 4, 2020, https://www.channelnewsasia.com/news/world/covid-19-europe-contact-tracing-apps-apple-google-12804606.

[38] Michel Abdalla et al., "Mise en garde contre les applications de traçage", April 26, 2020, https://attention-stopcovid.fr/.

[39] Heijmans, Philip and Yoolim Lee, "Singapore Considers Wearable Tech Devices For All to Trace Virus", June 5, 2020, https://www.bloomberg.com/news/articles/2020-06-05/singapore-rules-out-mandatory-use-of-contact-tracing-app.

[40] Sim, Dewey and Kimberly Lim, "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?", South China Morning Post, May 18, 2020, https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether.

[41] Cook, James, "Singapore plans wearable device after problems with its contact tracing app", June 5, 2020, https://www.telegraph.co.uk/technology/2020/06/05/singapore-plans-wearable-device-problems-contact-tracing-app/.

[42] Kaafar, Dali et al., "Joint Statement on Contact Tracing", April 19, 2020, https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view.

[43] Masoodi, M.J., Andrey, S., Bardeesy, K. & Choudhry, Z. (2020, June 8). *Race to Trace: Security and Privacy of COVID-19 Contact Tracing Apps*: 10 https://www.cybersecurepolicy.ca/racetotrace; Angwin, J. (2020, April 14); Will Google's and Apple's COVID Tracking Plan Protect Privacy? The Markup. https://themarkup.org/ask-the-markup/2020/04/14/will-googles-and-apples-covid-tracking-plan-protect-privacy.

[44] Aiello, Rachel, "Plans for single COVID-19 contact tracing app facing resistance: health minister", CTV News, June 1, 2020, https://www.ctvnews.ca/politics/plans-for-single-covid-19-contact-tracing-app-facing-resistance-health-minister-1.4963895.

[45] Thomas, Jesse, "Coronavirus: Survey suggests majority of Canadians would use contact tracing app to curb spread", Global News, May 29, 2020, https://globalnews.ca/news/7004213/coronavirus-poll-canada-contact-tracing-covid-19/.

[46] Gunn, Andrea, "Poll shows broad public support for contact tracing apps to fight COVID-19", The Guardian (PEI), May 8, 2020, https://www.theguardian.pe.ca/news/canada/poll-shows-broad-public-support-for-contact-tracing-apps-to-fight-covid-19-447687/.

[47] "Majority of Canadians would sacrifice personal privacy if it helped stop COVID-19, finds KPMG in Canada survey", Cision, May 14, 2020, https://www.newswire.ca/news-releases/majority-of-canadians-would-sacrifice-personal-privacy-if-it-helped-stop-covid-19-finds-kpmg-in-canada-survey-891920008.html.

[48] Kaafar, Dali et al., “Joint Statement on Contact Tracing”, April 19, 2020, https://drive.google.com/file/d/1OQg2dxPu-x-RZzETIpV3lFa259Nrpk1J/view.

[49] Taylor, Josh, “How did the Covidsafe app go from being vital to almost irrelevant?”, The Guardian, May 23, 2020, https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant.

[50] Findlay, Stephanie. “Coronavirus Contact-Tracing Apps Struggle to Make an Impact.” Financial Times, May 18, 2020. https://www.ft.com/content/21e438a6-32f2-43b9-b843-61b819a427aa.

[51] Sim, Dewey and Kimberly Lim, “Coronavirus: why aren’t Singapore residents using the TraceTogether contact-tracing app?”, South China Morning Post, May 18, 2020, https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether.

[52] Fouquet, Helen, “France Says Apple Bluetooth Policy Is Blocking Virus Tracker”, Bloomberg, April 20, 2020, https://www.bloomberg.com/news/articles/2020-04-20/france-says-apple-s-bluetooth-policy-is-blocking-virus-tracker?sref=CrGXSfHu.

[53] Toy, Adam, “Alberta’s contact-tracing app only works on iOS when phone is unlocked, app running in foreground”, Global News, May 4, 2020, https://globalnews.ca/news/6898691/ab-trace-together-contact-app-alberta-covid-ios/.

[54] “Privacy-Preserving Contact Tracing - Apple and Google.” Apple, https://www.apple.com/covid19/contacttracing.

[55] “Decentralized Privacy-Preserving Proximity Tracing -- Documents.” GitHub, 28 May 2020, https://github.com/DP-3T/documents.

[56] “Decentralized Privacy-Preserving Proximity Tracing -- Documents”, GitHub, 28 May 2020, https://github.com/DP-3T/documents.

[57] Kelion, Leo, “Coronavirus: First Google/Apple-based contact-tracing app launched”, BBC News, May 26, 2020, https://www.bbc.com/news/technology-52807635.

[58] “Italy launches COVID-19 contact-tracing app amid privacy concerns”, Reuters, June 1, 2020, https://www.reuters.com/article/us-health-coronavirus-italy-app/italy-launches-covid-19-contact-tracing-app-amid-privacy-concerns-idUSKBN2383EW.

[59] “Poll: 70% of residents back ‘SwissCovid’ tracing app”, SWI, May 25, 2020, https://www.swissinfo.ch/eng/covid-19_poll--70--of-residents-back--swisscovid--tracing-app/45783230.

[60] “Italy launches COVID-19 contact-tracing app amid privacy concerns”, Reuters, June 1, 2020, https://www.reuters.com/article/us-health-coronavirus-italy-app/italy-launches-covid-19-contact-tracing-app-amid-privacy-concerns-idUSKBN2383EW.

[61] “Europe pins hopes on smarter coronavirus contact tracing apps”, Reuters, June 4, 2020, https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKBN23B1OA.

[62] “Apple-Google contact tracing tech launches, with 23 countries seeking access”, Reuters, May 20, 2020, https://www.reuters.com/article/health-coronavirus-apps-tracing/apple-google-contact-tracing-tech-launches-with-23-countries-seeking-access-idUSL1N2D21BB.

[63] Smart, Nigel, “Joint statement on Contact Tracing”, GoogleDocs, April 19, 2020, https://drive.google.com/file/d/1OQg2dxPu-x-RZzETIpV3lFa259Nrpk1J/view.

[64] Cyphers, B., Gebhart, G., “Governments Shouldn’t Use “Centralized” Proximity Tracking Technology”, Electronic Frontier Foundation, May 12, 2020, https://www.eff.org/deeplinks/2020/05/governments-shouldnt-use-centralized-proximity-tracking-technology.

[65] Masoodi, M.J., Andrey, S., Bardeesy, K. & Choudhry, Z. (2020, June 8). *Race to Trace: Security and Privacy of COVID-19 Contact Tracing Apps*: 10 https://www.cybersecurepolicy.ca/racetotrace.

[66] Soltani, A., Calo, R., Bergstrom, C., “Contact-tracing apps are not a solution to the COVID-19 crisis,” Brookings, April 27, 2020, https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[67] Ibid

[68] Ibid

[69] Hern, A., “France urges Apple and Google to ease privacy rules on contact tracing”, The Guardian, April 21, 2020, https://www.theguardian.com/world/2020/apr/21/france-apple-google-privacy-contact-tracing-coronavirus.

[70] Carter, A., Rieti, J. “Sidewalk Labs cancels plan to build high-tech neighbourhood in Toronto amid COVID-19”, CBC, May 7, 2020, https://www.cbc.ca/news/canada/toronto/sidewalk-labs-cancels-project-1.5559370.

[71] Newton, C., “Why countries keep bowing to Apple and Google’s contact tracing app requirements”, The Verge, May 8, 2020, https://www.theverge.com/interface/2020/5/8/21250744/apple-google-contact-tracing-england-germany-exposure-notification-india-privacy.

[72] “Apple-Google contact tracing tech launches, with 23 countries seeking access”, Reuters, May 20, 2020, https://www.reuters.com/article/health-coronavirus-apps-tracing/apple-google-contact-tracing-tech-launches-with-23-countries-seeking-access-idUSL1N2D21BB.