9-2-2020

Secure Digital Contact Tracing Methods Are Necessary for Slowing Down COVID-19

Rania Ansari

Rania Ansari

Pop Culture Intersections

September 2, 2020

Secure Digital Contact Tracing Methods Are Necessary for Slowing Down COVID-19

COVID-19 has horrified the world with its grasp, totaling 23 million cases and 850k deaths worldwide and they continue to rise.[1] Of those cases, the US holds the highest total worldwide with 6 million cases and 183k deaths.[1] As death tolls and cases rise, so do tensions among government agencies and its people. With a novel virus such as COVID-19, people are torn about what to do during this pandemic and the repercussions that may follow. In previous outbreaks and pandemics, contact tracing was used as a means of slowing down the viral spread by tracing an infected person's contacts. This is usually done by volunteers; people willing to put their lives on the line in order to preserve public health. This is not a luxurious job. In fact, many countries struggle with equipping enough people for the job as the available workforce is extremely limited. For one, it is difficult to recruit enough volunteers that are willing to work with the risk of infection. Even further, it takes critical time to teach volunteers how to properly contact trace, critical time that most certainly means life or death for some individuals. Additionally, in-person contact tracing requires for the infected party to remember all the places they visited and the people they encountered. Of course, these recollections are not always completely accurate.[2]

---

[1] "COVID-19 Map - Johns Hopkins ...." Accessed September 1, 2020. https://coronavirus.jhu.edu/map.html.

[2] "Liberia: Ebola contact tracing lessons inform ... - UN News." Accessed September 1, 2020. https://news.un.org/en/story/2020/04/1062582.

As a response, many countries have begun taking safety precautions using modern technology. An example of this is contact tracing applications, which are created to alert and inform those who come into close contact with someone exposed to the coronavirus. Countries like Singapore and South Korea have already incorporated technology such as digital contact tracing into citizen's daily lives. Both countries have rolled out nationwide applications using an individual's digital footprint as a means of tracking where they have been and who they have come in contact with.[3] Some countries have even taken it further, incorporating data surveillance (or tracking users whereabouts), with police in Kerala, India, even going as far as tapping phones of COVID-19 patients (and tracking their call detail records).[4]

However, many are frightened of possible hazardous implications of safety measures, such as contact tracing, and data surveillance, bringing privacy concerns to the front line. The cybersecurity of these safety measures is brought into question, as risks of hacks and security breaches are leveled. Additionally, many wonder at what point these security measures infringe upon citizen's privacy, with some questioning the government's lack of transparency, such as the collection of personal call records or location tracking without the user being aware. In fact, in Norway, the government released a smartphone contact tracing app that was met with privacy complaints and abundant with security problems. The app has now been formally placed on an

---

[3] "In defence of digital contact tracing: human rights, South ...." Accessed September 1, 2020. https://www.emerald.com/insight/content/doi/10.1108/IJPCC-07-2020-0081/full/html.

[4] "Surveillance state': Congress on Kerala tapping phones of ...." Accessed September 1, 2020. https://www.hindustantimes.com/india-news/surveillance-state-congress-on-kerala-tapping-phones-of-covid-patients/story-haTF6ttrq8FQCmZZsRiECM.html.

interim ban in the country as the risks of increased surveillance outweighed the app's unproved public health benefits at the time.[5]

As some countries are becoming increasingly overrun with cases, they must weigh the pros and cons of such apps. Because the U.S. alone holds a majority of the world's cases, leading all countries in the total number of cases and fatalities presented by John Hopkins University, it is quite concerning that we have not begun to consider using contact tracing technologies. Additionally, America's public trust of the government continues to fall rapidly, which is due to a multitude of reasons, such as past security breaches that are difficult to stomach. Human rights groups argue that such apps place millions of citizens under unnecessary privacy danger, exposing risks of stalking, scams, identity theft, or even, as seen in some countries, oppressive government tracking, all of which sabotage public health benefits and citizen's trust in the government. It is not hard to understand why some Americans are apprehensive about incorporating safety efforts that involve data analytics and surveillance.[6] Primarily, many people are concerned with what their personal data could be used for if left in the wrong hands and whether the government would protect those basic human rights. And rightfully so.

Because of past instances such as security breaches ranging from NSA security leaks to personal voter data exposure, which will be discussed later on in this paper, citizens do have the right to be understandably uncertain about trusting the government. However, I wish to make it clear that the novel coronavirus pandemic calls for urgent, necessary, and effective safety

---

[5] "Norway halts coronavirus app over privacy concerns | MIT ...." Accessed September 1, 2020. https://www.technologyreview.com/2020/06/15/1003562/norway-halts-coronavirus-app-over-privacy-concerns/.

[6] "Trust and Distrust in America - Pew Research Center." Accessed September 1, 2020. https://www.pewresearch.org/politics/2019/07/22/trust-and-distrust-in-america/.

methods, including data analytics, surveillance, and Artificial Intelligence. In fact, the contact tracing apps discussed have been proven to be effective with research studies from academic journals and epidemiological models justifying this. Further, this advanced technology and application should **not** infringe on basic human rights. It is possible for apps such as these to be implemented properly and efficiently while ensuring personal data protection and privacy. By outlining the history behind America's mistrust of their own government and current misinformation from the government, it will be made clear why so many citizens are hesitant to go full throttle on technology that uses data so personal such as location, contacts, and even (in some cases) credit card information. Analyzing other countries' applications of digital contact tracing and the effectiveness will help us gain insight into how these apps will positively help the battle against the coronavirus. Delving into how these contact tracing apps work specifically, we can obtain a more educated perspective on the advancements being made in technology to safeguard user privacy, such as apps that can "scramble" the data being accumulated. I will also outline the current safety regulations in place and possible future guarantees that developers and corporations can make in order to assure consumers that their data is protected and not being misused.

In light of this pandemic, tensions are already high. While other countries have begun flattening their curve, America has continued to rise extremely rapidly in cases. Going from 69 daily cases on March 5th to 77.3k on July 16th is a tremendous leap.[1] Therefore, it is evident that something drastic must be done to circumvent more cases and fatalities of innocent people. Analyzing other countries' responses to this immense threat of public health and the results demonstrate that digital contact tracing is one protocol that can indeed aid in slowing down the

coronaviruses path of devastation. The information provided in this paper should, additionally, make it easier for those who are worried about contact tracing and their rights to understand exactly what is implied by the phrases “digital contact tracing” and “data privacy.” Personal information is of concern and crucial importance to everyone who has intellectual data, therefore, it is only sensible to want to protect it. Furthermore, it is imperative to emphasize that public safety should not put basic human rights such as privacy and cybersecurity at risk. With current regulations and talks of further precautionary measures to be placed on developers and technology companies, it is most definitely possible to incorporate a contact tracing app that is efficient, effective, and still maintains basic data protection and consumer privacy.

In order to understand why Americans are so skeptical to trust their own government, it is important to examine the history of mistrust, specifically in data breaches and lack of transparency with the public. In studies by the Pew Research Center and CBS News polls, researchers found that Americans perceive trust in Washington as rapidly shrinking.[6] Especially now during this pandemic, with fake news and false information being spouted directly from the White House, many Americans are distrusting public health officials and local leaders. A large reason for this is due to the false claims that come directly from the top of leadership. Statements from our very own president like: “the U.S. has done far more testing than any other nation, by far” and “we've taken the most aggressive actions to confront the coronavirus” give many people, who are not willing to conduct further research, false hope.[7] In March (when this statement was said) the U.S. had tested 418,810 individuals for coronavirus, the highest total of any country.[7] Before this, South Korea had the highest total of 357,896 tests.[7] While the U.S. has

[7] "Coronavirus: Five Trump claims fact-checked - BBC News." Accessed September 1, 2020. https://www.bbc.com/news/world-us-canada-51818627.

done more testing in total than any country, the population of America is around 328 million. South Korea's population? About 51 million.

Undeniably, the false accusations from the government concern citizens. When claims such as those that are blatantly biased and skewed in favor of a certain party, it leaves many wondering whether the government is fighting for the public's safety or is promoting another more sinister agenda. Especially now, as elections are nearing, there seems to be a direct focus on the politicization of the coronavirus pandemic. Yet, it is never ethical for public health/safety and user privacy protection to be political. Still, in America's history, we see a long battle between government transparency and the people's trust in the country's leaders. These recurring issues are a part of what sparked the privacy debates of surveillance and tracing apps.

The problem stems much deeper than this, though.

In 2013, National Security Agency contractor Edward Snowden blew the lid off U.S. government surveillance methods.[8] On June 5, 2013, The Guardian in Britain published the first story based on Snowden's leaks.[7] It revealed that a secret court order was allowing the U.S. government to get Verizon to share the phone records of millions of American citizens.[7] Later stories disclosed other backend snooping and how U.S. and British spy agencies had accessed information from the world's telephone and internet traffic.[7] Incidences like this one, permanently changed how the public viewed and trusted their own government. Issues regarding personal privacy and infringements upon human rights emerged, showcasing the amounting evidence for the public to be wary about the government's lack of transparency. In fact, Edward

[8] "Edward Snowden, the NSA, and the US Surveillance State." Accessed September 1, 2020. https://www.independent.org/publications/tir/article.asp?id=1053.

Snowden's revelations about NSA's telephone metadata collection program triggered an uproar in the U.S., eventually culminating in the 2015 passage of the USA Freedom Act—legislation that supporters claimed would "end" the kind of mass surveillance Snowden had exposed to the world.[9]

However, this is not the only case of extensive data leaks occurring. In 2015, a whitehat hacker (or ethical computer hacker) uncovered a database sitting on the Web containing various pieces of personal information related to 198 million American citizens registered to vote, later being described as the largest US voter data leak.[10] UpGuard cyber-risk analyst Chris Vickery told FORBES he found a multitude of voter data, including names, home addresses, phone numbers, dates of birth, party affiliations, and logs of whether or not they had voted in primary or general elections, dating back to 2000.[10] He said, "Our society has never had to confront the idea of all these records, all in one place, being available to anyone in the entire world for any purpose instantly."[9] Vickery supplemented, "That's a hard pill to swallow. It crosses the line."[9] It was later discovered in 2017 that over 1.1 terabytes of "entirely unsecured personally identifiable information" (PII) were exposed on behalf of the RNC.[11] To put this into context, just 1 terabyte

---

[9] "From Snowden to Schrems: How the Surveillance Debate has ...." Accessed September 1, 2020. https://login.libproxy.scu.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1904774769%3Faccountid%3D13679.

[10] "191 Million US Voter Registration Records Leaked In ... - Forbes." Accessed September 1, 2020. https://www.forbes.com/sites/thomasbrewster/2015/12/28/us-voter-database-leak/.

[11] "The RNC Files: Inside the Largest US Voter Data ... - UpGuard." Accessed September 1, 2020. https://www.upguard.com/breaches/the-rnc-files.

can store 6.5 million document pages (or 1,300 physical filing cabinets of paper).[12] Situations like these, even if unintentional, make it hard for the people to wholeheartedly put their trust in the government to do what is right in times of crises, and even make it difficult to believe that the government has the public's best interests at heart.

During times of crisis, it is not unusual for the government to ramp up security. After the 9/11 terrorist attacks in 2001, the U.S. government passed the Patriot Act in order to "enhance domestic security" as quoted by Tina Ebenger in her article "The USA PATRIOT Act: Implications for Private E-Mail."[13] As a means of increasing security, the government inherently negated several privacy protections for citizens. She says, "One of the means to accomplish this was to give law enforcement increased authority for the surveillance, interception, and disclosure of private e-mails."[12] Often times during public crises, privacy rules are relaxed in turn for greater protection against considerable threats, and such was the case in 2001.

After the 9/11 attacks, there was time to debate the law and deliberate over the government's surveillance powers. However, in the case of this pandemic, there is not enough time. The total cases and deaths are rapidly rising. Countries like China, Singapore, and South Korea have already used increased surveillance to help control the spread of the coronavirus and limit the death toll. The Chinese government is requiring that citizens use software that automatically decides if a person must be quarantined based on contagion risk. Similarly, South Korea is using a combination of smartphone location data, surveillance camera footage, and

---

[12] "How much is 1 TB of storage? - Dropbox." Accessed September 1, 2020. https://www.dropbox.com/features/cloud-storage/how-much-is-1tb.

[13] "The USA PATRIOT Act: Implications for Private E-Mail: Journal ...." Accessed September 1, 2020. https://www.tandfonline.com/doi/abs/10.1080/19331680801978759.

credit card data to trace those infected and their movements, delivering this information to the public.[3] And Singapore's government has launched a COVID-19 live dashboard to provide up to date information, contributing transparent data on each confirmed case including the age, sex, and occupation of each person who has tested positive for the virus.[13] It also shares places they have recently been to and when they sought medical help. It also reveals when they were hospitalized and when they were discharged. In fact, this site has been commended by other countries. According to Open Gov Asia, "it is believed that no other country has recorded such accurate data, and relentlessly tracked and traced every contact possibly linked to infected patients like Singapore has. No country has released as much detailed information about its coronavirus cases as the city-state."[14]

Still, these intrusive methods have yet to be introduced to America which has more cases and deaths than these both China, South Korea, and Singapore *combined*. Currently, Apple and Verily are partnering with state and federal governments to amass a collection of patient data on their symptoms, recent travel, location, age, and underlying health conditions.[15] Microsoft and many other technology startups are also conducting digital screening to collect similar information.[14] This news was met with concern as several democrats in the U.S. Senate have contacted Apple CEO Tim Cook and Verily CEO Andy Conrad, asking how the companies intend to use the information they plan to collect, and whether they will agree to refrain from

---

[14] "The importance of contact tracing in Singapore and the role ...." Accessed September 1, 2020. https://opengovasia.com/the-importance-of-contacttracing-in-singapore-and-the-role-technology-plays/.

[15] "Apple, Google Announce Joint COVID-19 Contact Tracing Tech." Accessed September 1, 2020. https://time.com/5819235/apple-google-smartphone-tracking-coronavirus/.

using the user data for commercial purposes. In the letter to Apple, which was signed by Sens. Bob Menendez and Cory Booker of New Jersey, Richard Blumenthal of Connecticut, and Kamala Harris of California, they affirm"Americans should not have to trade their privacy at the expense of public health needs."[16] As these discussions about security and consumer privacy arise, other possible complications of implementing these safety measures are brought to light. Jay Stanley, a senior policy analyst for the ACLU, says a lack of adequate privacy protections would impair consumer usage. He also states that "location tracking apps are limited by the accuracy of the data and uneven distribution of smartphones among richer and poorer segments of the population, which could pose equity issues."[17] While many Americans have cell phones, there are still unequal disruptions of *smartphones* which are fundamental to downloading apps and using certain location features. In fact, according to the Pew Research Center, 81 percent of Americans own smartphones, leaving a large portion of citizens who do not.[18] These numbers also impact different demographic groups as well, with some placed at disproportionate rates. With this in mind, it would require additional services or products to take into account as many Americans as possible. However, digitally tracing individual contacts is still significantly better than human contact tracers as they are often subject to constraints such as limited volunteer

---

[16] "COVID-19 Highlights New Privacy Challenges for BigTech ...." Accessed September 1, 2020. https://www.dwt.com/blogs/privacy--security-law-blog/2020/04/covid-19-privacy-challengers-for-big-tech.

[17] "Will we give up privacy for security after Covid-19? - STAT." Accessed September 1, 2020. https://www.statnews.com/2020/04/08/coronavirus-will-we-give-up-privacy-for-security/.

[18] "Mobile Fact Sheet - Pew Research Center." Accessed September 1, 2020. https://www.pewresearch.org/internet/fact-sheet/mobile/.

availability, inaccurate data, and risks of viral infection. Thus, using digital contact tracing can still unquestionably help automate the tracking process to be more efficient and accurate.

However, many people argue that apps like contact tracing alone could not cut off the transmission of the virus completely. Hannah Clapham, an epidemiologist at the National University of Singapore says, "It's very appealing—that you have an app that does all this work." [19] In fact, she and others claim that an app can not replace human contact tracers. "I worry that we think it's going to save us."[18] Furthermore, researchers emphasize that these apps must reliably estimate distance, based on the strength of the received signals from smartphones, in order to demonstrate effectiveness.[18] While conducting a test of Singapore's nationally administered TraceTogether app, computer scientists Douglas Leith and Stephen Farrell at Trinity College Dublin found flaws. Their study showed "that when people sat across a table, the received signals were much weaker if their phones were in their pockets versus on the table."[18] They caution that "the imprecision could lead to both missed encounters and false alarms," in other words, these possible flaws that these apps have can lead to inaccurate contact detection.[18]

Nonetheless, many countries have proven the use and effectiveness of technologies such as contact tracing in containing COVID-19. In a study conducted by doctors from the medical journal *The Lancet,* it was found that isolation strategies and contact tracing techniques combined would result in a reduction in the transmission of the coronavirus. They concluded that "self-isolation *and* contact tracing would be more likely to achieve control of severe acute

---

[19] "Can phone apps slow the spread of the coronavirus? | Science." Accessed September 1, 2020. https://science.sciencemag.org/content/368/6497/1296.

respiratory syndrome coronavirus 2 transmissions."[20] In another study also from *The Lancet,* researchers found that "optimizing testing and tracing coverage and minimizing tracing delays, for instance with app-based technology, further enhanced contact tracing effectiveness, with the potential to prevent up to 80% of all transmissions."[21] Moreover, after studying 391 COVID-19 patients and their 1,286 close contacts in China, researchers stated that their data analysis showed the effectiveness that contract tracing and isolation had in slowing the spread of COVID-19 (they did note that the overall impact was highly dependent on the number of asymptomatic patients).[20]

Researchers also confirmed that contact tracing reduced the time between viral detection and isolation in patients. The Center for Infectious Disease Research and Policy (CIDRAP) reported: "Patients identified through symptom-based surveillance were identified and isolated, on average, 4.6 days after symptom onset (95% CI, 4.1 to 5.0). Contact tracing reduced this time to 2.7 days (95% CI, 2.1 to 3.3)."[22] With this information in mind, it is safe to conclude that some form of technological contact tracing is proven to be effective when helping stop the spread of COVID-19. Even if not 100% accurate all the time, contact tracing apps can help significantly slow the spread of COVID-19. On a similar note, human contact tracers are also not 100% accurate all the time, yet they are still effective. With technology like these apps in place, the risk of human contact tracers becoming infected diminishes and more data can be compiled

---

[20] "Effectiveness of isolation, testing, contact tracing, and physical ...." Accessed September 1, 2020. https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30457-6/fulltext.

[21] "Epidemiology and transmission of COVID-19 in 391 cases ...." Accessed September 1, 2020. https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30287-5/fulltext.

[22] "Study: Contact tracing slowed COVID-19 spread in China ...." Accessed September 1, 2020. https://www.cidrap.umn.edu/news-perspective/2020/04/study-contact tracing-slowed-covid-19-spread-china.

at faster rates. Countries like Singapore and South Korea have efficiently slowed the contagion of the virus using safety measures including contact tracing apps, with New Zealand having gone 100 days with no community coronavirus transmission.[23]

Since one of the most critical concerns of digital contact tracing is the intrusiveness (if not done without the proper security measures), researchers are working to develop ways of collecting data without compromising personal privacy and data. "The Massachusetts Institute of Technology has teamed up with Facebook, Mayo Clinic, and other organizations to create an app that collects information using a technique known as differential privacy, a way of publicly sharing information gleaned from a data set without identifying the individuals whose activities are represented."[16] The app works in a way to *scramble* the data provided so that the information can not be connected to the individual, therefore eliminating the concern of the user being identified. The data would also be encrypted to ward off potential hackers from accessing any important and private information. They are also focused on ensuring that the app does not give the government constant access to private user data. Nevertheless, these safety measures do rely on consumers' willingness to make use of their online and cell phone data for the benefit of public health.

Taking the fact that researchers are trying to develop new technologies to protect data into consideration, many may still be concerned about where that information goes from there and whether the government and corporations are using consumer data for usages other than public safety. The question then arises: how can Americans trust that the government and corporations are not going to misuse the data collected from these contact tracing apps?

---

[23] "New Zealand goes 100 days with no COVID-19 transmission ...." Accessed September 1, 2020. https://www.livescience.com/new-zealand-100-days-no-covid-19.html.

Currently, there are a few regulations that are in place in order to protect consumer data misusage. For example, the California Consumer Protection Act (CCPA) prohibits the "use [of] personal information collected for additional purposes without providing the consumer with notice."[16] In other privacy legislation, there are similar precautions placed to limit what companies can and can not do without user discretion.[16] Additionally, the CCPA does not contain any exceptions to its conditions, specifically for public interest use purposes.[16] However, this does not leave many companies with necessary guidelines on the legality of contact tracing data collection. The group of senators who sent Apple and Verily letters serve as a reminder that basic privacy requirements should construct product and application development.[16] In her article, "COVID-19 Highlights New Privacy Challenges for BigTech, Lawmakers," Rachel R. Marmor outlines a specific legal guideline for what she calls "data protection assessments."[16] She includes that the assessments should:

- Evaluate the benefits of the data collection, use, and disclosure against the risk of harm to the individual;[16]
- Enforce data minimization during product development by documenting the necessity of each data element collected to achieving the business purpose;[16]
- Analyze the data collection, use, and disclosure practices against the organization's privacy policy; and[16]
- Evaluate whether any special security measures need to be taken in light of the sensitivity of the data at issue.[16]

With this in mind, it is essential for legislatures and tech companies to work together in order to compile a comprehensive list of safety regulations to be applied when contact tracing apps come

into the market. By following the guardrails listed, it is possible to implement a powerful app that still certifies personal information and privacy.

The U.S. currently has the most deaths and cases in the *whole world.*[1] With this pandemic getting progressively worse and multiple countries having already implemented digital precautions to fight the pandemic, specifically contact tracing, many wonder when the U.S. will follow. For many Americans, like myself, we are concerned with the country's perspective on this novel virus. Many citizens are uneducated about the dire implications of this pandemic on public health and even further uneducated on the topic of digital contact tracing. It is undeniably alarming to give up personal information such as our phone location to track whereabouts and who we recently came into contact with, especially with the trend of a lack of transparency with the government and its people. Thus, it is paramount that regulators and developers create products that verify safety and protect personal information. Further, with the proper regulations and guardrails in place, contact tracing applications can be implemented in the U.S. with great assistance in slowing the pandemic's national (and global) reach.

The bottom line is that thousands of people are dying every day due to this virus, and it is a global responsibility to stop the spread. These safety measures are of the utmost importance to public health. In fact, Michelle Mello, a health law professor at Stanford University, weighs that some precautions are arriving too late to make a difference. She says, "We kind of blew it on surveillance, it's pretty late in the game to be getting into that now, you really can't stand these things up in the middle of a pandemic," implying that data surveillance to prevent the viral spread is too late; America is past the point of prevention. However, it is definitely possible to stop the spread of coronavirus. Since the U.S. is experiencing extremely high rates of cases and

deaths, it is imperative that we analyze the risks and gains of safety measures and enforce them as soon as possible. I want to emphasize the fact that, although I realize the uneasiness to trust the government with important information such as data privacy, the pandemic will not slow down if we do not treat it. In fact, experts predict that by December, if America's response remains the same, the U.S. death toll will reach 300,000.[24] The same IHME (Institute for Health Metrics and Evaluation) model predicts that the coronavirus is on track to be the third leading cause of death in the U.S.[24] A huge part of the coronavirus's reach is its ability to infect such a large number of people in such little time. In order to change the course of America's future, we must use a digitally based contact tracking system that follows all safety and legal guardrails, preferably an app that collects information from individuals and notifies them if they have come into contact with someone who was infected. From then on, quarantining is necessary to prevent any further viral contagion. As stated before, usually, people must wait until symptoms appear to realize that they may be sick and then isolate themselves, which, on average takes 4.6 days.[22] With contact tracing implemented, that number can be lowered to 2.7 days, which in turn reduces the amount of time for possibly infected individuals to expose others to the virus, and as a result, slowing down COVID 19's infection rate.

From here on, the coronavirus is only going to take more lives. At some point, we must realize that what we are currently doing is *not enough*. 850 thousand people in the world have died. 183 thousand Americans have died. How many more must give their life in order for us to implement safety precautions to help slow the spread of COVID 19. With the technology

---

[24] "IHME Model Projects Nearly 300,000 COVID-19 Deaths By ...." 6 Aug. 2020, https://www.npr.org/sections/health-shots/2020/08/06/900000671/300-000-deaths-by-december-9-takeaways-of-the-newest-covid-19-projections. Accessed 1 Sep. 2020.

available for us today, we must understand that it is possible to successfully execute safety measures like contact tracing in a way that would thoroughly protect the intellectual property of consumers. Using effective methods such as digital contact tracing has been proven to work in many countries and has even been used in previous pandemic outbreaks. Far too many people have died from this virus for us to simply sit around and "hope" that what we are doing it enough. It is not. In order for Americans to even have a fighting chance at defeating COVID 19, safe and cyber-secure precautions like contact tracing (digital and others) must be used now.

Bibliography

Aizenman, Nurith. “300,000 Deaths By December? 9 Takeaways From The Newest COVID-19 Projections.” NPR. NPR, August 6, 2020. https://www.npr.org/sections/health-shots/2020/08/06/900000671/300-000-deaths-by-december-9-takeaways-of-the-newest-covid-19-projections.

Andrej, Zwitter and Oskar J. Gstrein. "Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection." *Journal of International Humanitarian Action* 5, no. 1 (Dec 2020). http://dx.doi.org.libproxy.scu.edu/10.1186/s41018-020-00072-6.

Beúsekom, Mary Van. “Study: Contact Tracing Slowed COVID-19 Spread in China.” CIDRAP. University of Minnesota, April 28, 2020. https://www.cidrap.umn.edu/news-perspective/2020/04/study-contact-tracing-slowed-covid-19-spread-china.

Bi, Qifang, Yongsheng Wu, Shujiang Mei, Chenfei Ye, Xuan Zou, Zhen Zhang, Xiaojian Liu, et al. “Epidemiology and Transmission of COVID-19 in 391 Cases and 1286 of Their Close Contacts in Shenzhen, China: a Retrospective Cohort Study.” *The Lancet Infectious Diseases* 20, no. 8 (April 27, 2020): 911–19. https://doi.org/10.1016/s1473-3099(20)30287-5.

Brewster, Thomas. “191 Million US Voter Registration Records Leaked In Mystery Database.” Forbes. Forbes Magazine, December 30, 2015. https://www.forbes.com/sites/thomasbrewster/2015/12/28/us-voter-database-leak/.

Bryner, Jeanna. “New Zealand Goes 100 Days with No COVID-19 Transmission.” LiveScience. Purch, August 10, 2020. https://www.livescience.com/new-zealand-100-days-no-covid-19.html.

Butler, Alan and Fanny Hidvegi. "From Snowden to Schrems: How the Surveillance Debate has Impacted US-EU Relations and the Future of International Data Protection." Seton Hall Journal of Diplomacy and International Relations 17, no. 1 (15, 2016): 55-80. https://login.libproxy.scu.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1904774769%3Faccountid%3D13679

“Coronavirus - Liberia: Ebola contact tracing lessons inform COVID-19 response.” *African Press Organization* (April 2020). ProQuest. https://news.un.org/en/story/2020/04/1062582.

“COVID-19 Map.” Johns Hopkins Coronavirus Resource Center. John Hopkins University, 2020. https://coronavirus.jhu.edu/map.html.

Ebenger, Tina. "The USA PATRIOT Act: Implications for Private E-Mail." *Journal of Information Technology & Politics* 4, no. 4 (05, 2008): 47-64. doi:http://dx.doi.org.libproxy.scu.edu/10.1080/19331680801978759

Firth, J.A., Hellewell, J., Klepac, P. et al. “Using a real-world network to model localized COVID-19 control strategies.” *Nat Med* (2020). https://doi.org/10.1038/s41591-020-1036-8.

Gurman, Mark. “Apple, Google Announce Joint COVID-19 Contact Tracing Tech.” Time. Time, April 10, 2020. https://time.com/5819235/apple-google-smartphone-tracking-coronavirus/.

“How Much Is 1 TB of Data Storage?” Dropbox. Dropbox. Accessed September 1, 2020. https://www.dropbox.com/features/cloud-storage/how-much-is-1tb.

Kucharski, Adam J, Petra Klepac, Andrew J K Conlan, Stephen M Kissler, Maria L Tang, Hannah Fry, Julia R Gog, et al. “Effectiveness of Isolation, Testing, Contact Tracing, and Physical Distancing on Reducing Transmission of SARS-CoV-2 in Different Settings: a Mathematical Modelling Study.” *The Lancet Infectious Diseases*, June 16, 2020. https://doi.org/10.1016/s1473-3099(20)30457-6.

Lee Rainie, Scott Keeter And Andrew Perrin. “Americans' Trust in Government, Each Other, Leaders.” Pew Research Center - U.S. Politics & Policy. Pew Research Center, August 17, 2020. https://www.pewresearch.org/politics/2019/07/22/trust-and-distrust-in-america/.

Marmor, Rachel. “COVID-19 Highlights New Privacy Challenges for Big Tech, Lawmakers." *Intellectual Property & Technology Law Journal* 32, no. 6 (June 2020): 5-7. EBSCO. https://www.dwt.com/blogs/privacy--security-law-blog/2020/04/covid-19-privacy-challengers-for-big-tech.

Munger, Michael. "No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State." The Independent Review 19, no. 4 (Spring, 2015): 605-609.

https://login.libproxy.scu.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1671113540%3Faccountid%3D13679.

O'Neill, Patrick Howell. "Norway Halts Coronavirus App over Privacy Concerns." MIT Technology Review. MIT Technology Review, June 17, 2020. https://www.technologyreview.com/2020/06/15/1003562/norway-halts-coronavirus-app-over-privacy-concerns/.

O'Sullivan, Dan. "The RNC Files: Inside the Largest US Voter Data Leak." UpGuard. UpGuard, March 11, 2020. https://www.upguard.com/breaches/the-rnc-files.

Pew Research Center. "Demographics of Mobile Device Ownership and Adoption in the United States." Pew Research Center: Internet, Science & Tech. Pew Research Center, June 12, 2019. https://www.pewresearch.org/internet/fact-sheet/mobile/.

Reality Check Team. "Coronavirus: Five Trump Claims Fact-Checked." BBC News. BBC, March 26, 2020. https://www.bbc.com/news/world-us-canada-51818627.

Ross, Casey. "Will We Give up Privacy for Security after Covid-19?" STAT. STAT, April 8, 2020. https://www.statnews.com/2020/04/08/coronavirus-will-we-give-up-privacy-for-security/.

Ryan, Mark. "In defence of digital contact tracing: human rights, South Korea and Covid-19." *International Journal of Pervasive Computing and Communications* (Aug 2020). https://doi.org/10.1108/IJPCC-07-2020-0081.

Sagar, Mohit. “The Importance of Contact Tracing in Singapore and the Role Technology Plays.” OpenGov. OpenGov, March 17, 2020. https://opengovasia.com/the-importance-of-contact-tracing-in-singapore-and-the-role-technology-plays/.

Servick, Kelly. “Can Phone Apps Slow the Spread of the Coronavirus?” Science. American Association for the Advancement of Science, June 19, 2020. https://science.sciencemag.org/content/368/6497/1296.

Tripathi, Ashutosh, ed. “'Surveillance State': Congress on Kerala Tapping Phones of Covid Patients.” Hindustan Times, August 13, 2020. https://www.hindustantimes.com/india-news/surveillance-state-congress-on-kerala-tapping-phones-of-covid-patients/story-haTF6ttrq8FQCmZZsRiECM.html.