Intersect, Vol 15, No 1 (2021)

Individual Health Tracking Applications in the Age of COVID-19 and Emerging Third Party Oversight

Tom Quach
Stanford University

In the 2020 decade, the most valuable commodity is no longer only our physical body, but also our brains and mental states. How do we think, and what does our digital footprint say about our future actions? In "Privacy is Power," Carissa Véliz introduces readers to a similar vein of thought, describing that with knowledge, personalities, and feelings, each person possesses "a source of power" (Véliz, 2019). "Power over others' privacy," she writes, "is the quintessential kind of power in the digital age" (Véliz, 2019). This dilemma forms a moral tug-of-war in the time of a worldwide health crisis, forcing many people to decide whether to protect personal privacy or help prevent community transmission by opting-in to a shared database for COVID-19 contact tracing. Looking through the lens of the United States's approach, I will discuss how countries globally both in Europe and in Asia such as South Korea impacted the American public's views on widespread COVID-19 tracing systems set in place and how recent data controversies continue to stir the pot on digital platforms' trustworthiness and accountability. Current situations lead us to determine how society faces future pandemics and formulate steps to reform any existing pitfalls and misunderstandings. This paper will investigate how congressional and third-party oversight are necessary in safeguarding individual information, along with expanding the system of Bluetooth-based digital contact tracing to preserve transparency and user anonymity.

Introduction

The COVID-19 pandemic shell shocked the world as a horrific reality in early 2020. By late March of that year, nearly three billion people were ordered to follow local and national lockdown orders, staying at home and avoiding interaction with friends and extended family, according to the World Economic Forum (Lacina, 2020). National governments, ranging from China to Singapore and eventually to the United States, found it necessary to begin economic recovery while maintaining public health at the forefront. Private technology companies began partnerships with city, state, and federal leaders to create algorithms to establish networks of tracking COVID-19 cases and spread across various communities. In less than a year, many digital contact tracing applications were introduced;

globally, certain countries demanded mandatory opting-in, while others attempted voluntary participation. These decisive actions by political leaders and corporations were met in part by citizens who understood and complied; on the other hand, there were also some who questioned its implementation, citing personal privacy questions and uncertainty regarding how information stored within these apps could be inappropriately accessed and exploited. More importantly, these past two years have introduced additional, emphasized calls for public health companies and private big-tech institutions that provide support to increase transparency and ethical responsibility.

It is our reality that monopolies shape the decisions of millions, if not billions, of people, by churning out advertisements based on a trove of data they collect from people's day-to-day actions online. They laser in on the most efficient way to advertise: the aggregation of individual data—whenever someone sends an input into a device, algorithms store and keep information for the long term. The more alarming actions are when the exact data are transferred to other companies to be used for consumer research, ad revenue, and targeted projects, many times without user consent and knowledge. We also need to understand those who hesitate to sign up for virtual systems to avoid getting caught in the network of data exploitation.

A Nature Medicine review article titled "Digital technologies in the public-health response to COVID-19" provides a diagram depicting the vast network of technologies used in response to the pandemic. Examples include symptom-reporting apps, data dashboards, and targeted public health messaging. However, as the authors of the report note, some initial digital tracing programs "raised concerns about privacy" and coerced participation (Budd et al. 1186). They cite countries like South Korea, where the government tracked those infected with transaction records and public surveillance, and China, a country that mandated its population to download the AliPay HealthCode app in order to construct a social scoring system—citizens deemed "too high-risk" were restricted from purchasing essentials in public. Researchers also referred to government-partnered voluntary contact tracing apps that have recently arisen, such as in Norway.

Still, the public and watchdog organizations have protested about the unclear presence of "centralized systems and GPS tracking" (Budd et al., 2020, p.1186). We can put this into the context of communities within the United States, where technologists have individually created public health software to be implemented for mass usage immediately since early-2020. With many areas across this country in some level of emergency, government officials are somewhat compelled to rush the approvals of these respective applications, often not extensively looking over hidden disclaimers of data privacy. Stanford Law and Health Policy professors Michelle Mello and Jason Wang, authors of "Ethics and governance for digital disease surveillance," agree with this outlook, noting that in a time

like this, big-tech leaders and government leaders are "working outside ordinary channels and public view" because of the need to make quick decisions (Mello, Wang, 2020, p. 952). Watching how other countries approach their mostly involuntary surveillance, combined with hearing that some of these platforms have been released under a cloak of secrecy, a portion of Americans carry with them an air of apprehension surrounding digital COVID-19 technologies. They certainly have the right to do so, but the government must find concrete ways to mend the disconnect formed from years of mistrust and controversies surrounding the major tech companies and their various platforms.

The U.S. Rollout

Like many scientists and technology enthusiasts, Mello and Wang acknowledge that there is a "growing potential to use machine learning and big data to forecast disease spread" (Mello, Wang, 2020, p. 951). They introduce multiple countries and their headway on person-to-person records and inspection, but more importantly, highlight significant areas and questions needed to be asked.

To build foundations of trust and responsibility, digital epidemiology brings forth critical ethical issues for all parties, including the government, technology companies, and ourselves, to discuss and coordinate solutions that will implant additional faith in digital trackers amidst COVID-19's health crisis. Critical steps involve "respecting privacy," "respecting autonomy," "minimizing the risk of error," and restoring "accountability" (Mello,Wang, 2020, p.952). When our country introduces a contact tracing system, the government and companies who coded the algorithm should implement key features that allow for maintaining an extremely high level of transparency with users. For Mello and Wang, they describe the crucial role of informed consent, terms and agreements, opt-in/outs, and their involvement in fostering confidence among app users. As Americans, we generally value personal freedom, privacy, and knowledge that our personal identifiable information is protected and held secret by law. With these functions clearly outlined at the beginning of logging onto these platforms, COVID-19 tracking networks then will become a more "thoughtful and transparent process" (Mello, Wang, 2020, p. 954).

When examining the data of how the United States has successfully, and at times not, rolled out its pandemic surveillance plan, we will see the truth and benefit in Mello and Wang's insights. In the "MIT Technology Review," Mia Sato summarizes the fifty states' statuses regarding their transmission prevention apps' rollouts. She emphasizes that unlike other countries, the United States did not pursue a national, coordinated effort as no national mandate was implemented. Instead, individual states “created a patchwork of systems that launched at staggered times and did not necessarily work across local borders” (Sato, 2021). Over time, software engineers, in coordination with city and state governments, refined their platforms so their applications could be utilized in broader areas than

initially. Sato references an "MIT Technology Review Covid Tracing Tracker" in her piece and demonstrates how various states have instituted features highlighted by Mello and Wang. For example, Colorado, New York, and Nevada each use their own sites, but they all rely on Bluetooth systems to collect information that is stored for a limited amount of time on individuals' phones, instead of a centralized database that aggregates hundreds of thousands of personal details. In California, Sato notes how the government-sponsored application software is “embedded in the operating system of newer iPhones” (Sato, 2021). By doing so, individuals have the critical option to opt-in or opt-out of the program simply by entering the settings app and switching the on/off button. These methods have helped increase user assurance and technology responsibility. Moreover, by consistently operating at a reasonable level of clarity, these systems provide security for users wary of data exploitation.

However, pitfalls have arisen due to companies fast tracking the production of systems that state officials can present to citizens. Both Sato and Politico's Tim Starks mention Care19, a smartphone app introduced by North Dakota and Wyoming in early April 2020. A month later, state leaders admitted the Care19 operation was involved in "sending users' location data to the digital marketing service Foursquare" (Starks, 2020). According to a third-party organization who caught the data leak, Jumbo Privacy, they wrote that Foursquare spokespeople explained their software development kit (SDK), Pilgrim, automatically synthesized people's whereabouts, and "there was no way for developers to disable this collection" (Jumbo Privacy, 2020). Though this faulty algorithmic error was eventually fixed, this instance brought to light how specific mechanics have operated without explicit user consent and knowledge—harming user trust and corporate transparency within COVID-19 digital tracking surveillance programs.

Future Solutions in Sight

As we proceed, concrete steps can immediately be taken to restore community trust. The United States is in a unique position to look at two already implemented systems around the world and improve the methods that benefit both users and medical researchers. Impacted by COVID-19 since its onset, South Korea developed a rigorous digital health monitoring network that collected information surrounding citizens’ credit card transactions, mobile phone logs, and surveillance camera footage. With over 96 percent of the population having access to daily internet access, the South Korean government formed a national mandate and enacted constant public reinforcement that encouraged widespread participation but was subject to scrutiny over the amount of personal data collected. Still, countries like South Korea say they uphold principles of public scrutiny and strong legal protections that punish data misuse and exploitation by holding daily press briefings and dispersing resources to the press (Martinez-Martin et al., 2020, p.44). On the other end of the

world, European countries utilized optional, bluetooth operated systems that prioritized users' anonymity whenever personal information was inputted, mostly operated by Google and Apple. Whenever someone was detected positive, they would insert their information into the decentralized network, which would send an encrypted signal—consisting of random numbers and letters—to a database that would check with other users' signals obtained by Bluetooth. According to TIME's Billy Perrigo, "neither you, nor the person you've come into contact with, nor the government, nor Google or Apple can deduce any personal information from that data" (Perrigo, 2020).

Domestically, we should incorporate the bluetooth-encrypted format that has come to light to preserve individual privacy among all users. Among the many positives, maintaining anonymity is perhaps the most critical for everyday citizens. The good news is that, as mentioned earlier, states have begun to utilize this model of digital health tracking. One pitfall of anonymity, however, is the inability to inform medical researchers: to address this, an option for COVID-19 positive users to specify certain symptoms and submit them to a central storage database for review to aid epidemiologists is a possibility. Furthermore, there is a need for prominent messaging, both in and outside the contact tracing apps, by certified ethicists and technology representations that explain how to manage data and precise details on what occurs after deleting the app on one's digital device. Alongside this, we should also mirror the type of public encouragement and open transparency of countries like South Korea's to increase tracing usage. The next objective, I believe, is to expand our current digital health tracing infrastructure into a standardized nationwide system that allows for cross-collaboration between different regional and state governments in the United States.

For the past few years, "tiny state cybersecurity budgets" and "stalled legislation in Congress" have halted meaningful progress around the nation in regards to personal online security and unbiased safety regulations (Starks, 2020). However, Mello and Wang outline viable ways for increased accountability that make sense to me. They say "ethicists and legal experts do not appear involved" in the decision-making and approval process, as well as the absence of oversight committees and public input (Mello, Wang, 2020, p.954). Now, in 2021, legislators should be compelled, more than ever, to enact measures that would protect everyday individuals from misuse of data by tech companies or bad actors. Monica Nickelsburg of GeekWire mentions a wave of bipartisanship in Congress that looks to ensure personal privacy and independence. "Efforts to rein in the tech industry gained momentum over the past few years," she wrote, adding that the House of Representatives, Department of Justice, federal regulatory agencies, and multiple states have investigated the activities of companies such as Facebook, Apple, Google, and Amazon (Nicklesburg, 2021). This collective concern was shown on January 21, 2021, when 17 Republican representatives delivered a letter to President Biden, which

stated that they "hope to work with [him] to... enforce [the] antitrust laws against emboldened technology monopolies."

Antitrust debates are another conversation on its own, but its core concept connects with the COVID-19 tracking and surveillance realm of thought. Ultimately, a multitude of digital applications emerging across different states are largely maintained by these exact corporations that dominate the data industry. According to VisualCapitalist's Omri Wallach, statistical graphs—with values extracted in 2020—show how Facebook earns 98.5% of its 71-billion-dollar revenue through Facebook ads, which are aggregated from millions of users every day. In addition, Alphabet received around 70% of its 162-billion-dollar total revenue through advertising streams on its services, such as Google and YouTube (Wallach, 2020). Looking into various pandemic-related healthcare software, we can see how these exact companies are in control. One major COVID screening website is Verily. According to StatNews, Verily, a recent three-year-old venture, "has operated largely out of public view." When the news organization attempted to dig more into the inner workings of the bio-health sub-company, they were alerted that "employees [who talk] to a reporter without permission is a firing offense" (Piller, C., et al, 2016). Interestingly enough, Verily is owned by the Alphabet Corporation. Although this may not explicitly be a conflict of interest, some lawmakers and experts are questioning this controversial tie. Andrew Peterson of Protocol Magazine wrote how in April 2020, a group of senators led by Bob Menendez (D-NJ) sent a letter to Verily inquiring for more answers on what the company plans to do with the information it will collect from users throughout the pandemic process. Senator Mark Warner (D-VA) also stressed that while "these tools can be a helpful part of the solution during our ongoing public health emergency, patient privacy shouldn't be sacrificed as a result" (Peterson, 2020) With congressional leaders keeping an eye on Big Tech's activities, it serves a reminder for the public to not lose sight of this prevalent issue may go on behind the scenes via backchannel operations.

International Preparedness Around Technology's Transparency and Accountability

Beyond the borders of the United States, the World Health Organization (WHO) also recently commented on the topic of preserving personal privacy and data security in the age of COVID surveillance and tracking protocols. In a joint statement with the United Nations (UN) released in November 2020, the WHO reminded the world, particularly companies who have released pandemic-prevention platforms and software to observe the lives of millions of global citizens, the importance of avoiding "infringement of fundamental human rights and freedoms" (WHO, 2020). Similar to many scientists and government officials, the WHO acknowledged the need for COVID tracking applications and their effectiveness on limiting the spread of the coronavirus strain and its

variants. Nonetheless, the organization emphasized the danger of companies utilizing the information "not directly or specifically related to the COVID-19 response," especially if programs such as digital contact tracing become the norm for future pandemic response and even day-to-day medical services (WHO, 2020).

Tied within the announcement, the WHO and the United Nations' Secretary-General outlined five bullet points that governments and technology corporations should always operate under. The WHO-UN leadership pointed to technology that is "necessary and proportionate," maintains confidentiality, proper deletion of data, and "be transparent in order to build trust" (WHO, 2020). Equally as important, the document cited the "UN Personal Data Protection and Privacy Principles" as a core resource individual governments and tech corporations should review when releasing their COVID-19 services.

The presence of such an international declaration, supported by dozens of countries and their respective governments, bolsters the cause of pushing for transparent trust and technological accountability in the realm of coronavirus response surveillance programs. To maintain a high level of responsibility, we must include the support of intercontinental governing agencies and place pressure on corporate companies and their partnering governments, leading them to commit themselves and travel on the ethically righteous path. In addition, engineers who encode algorithms for these online services need to be held accountable and must know for certain how to deactivate some features prior to public release. From then onward, we can narrow our focus down to national governments, state coalitions, and ultimately, motivated individual citizens.

The Need for Third-Party Oversight

Currently, there exists the Energy & Commerce Committee within the United States House of Representatives, which has participated in forums and webinars that discuss the critical importance of regulating software companies and safeguarding individual data and privacy from abuse and exploitation. According to the Committee's website, the legislative subgroup, headed by Chairman Frank Pallone Jr., hosted a teleconference back on May 7, 2020 that analyzed "COVID-19 testing, contract tracing and surveillance" (Energy and Commerce House Committee, 2020). Among other things, the roundtable honed in on insights that related to promoting human informational protection. Unfortunately, these conversations have not contributed to many measurable actions within these past two years, further supporting Starks' critiques on the slow-moving congressional process surrounding efforts to reshape regulation and oversight over corporations and their COVID-19 services.

This is an area where ordinary Americans can also become involved and enact objective change. Additional citizen and unbiased oversight groups, similar to JumboPrivacy, should be created to advocate for the public good and ensure that new systems are as ethical, consensual, and

transparent as possible. Publicly, tech corporations may announce that they are providing these services as an altruistic act of goodwill for humanity, but unfortunately, we cannot take them by their word. Based on historical trends and experiences of big tech's involvement in data security practices, emerging oversight committees and nonprofits, both locally and nationally, will be on the forefront of fact-checking any press releases and processes that software companies showcase.

It is imperative that countries, especially the United States, look to enact legislation that ensures the obligation to produce ethical digital services that overall benefits society. Of course, this would not be a democratic process without pushback from the Big Tech leadership themselves, who would raise concern that the government may be imposing too many regulations on independent businesses. Furthermore, multiple corporate-sponsored lobbying groups may also interfere by persuading lawmakers to oppose any government changes on technological regulations and vote "no" on bills that reach the House or Senate chambers. Therefore, the approval process may take much longer than anticipated, and will most likely require several iterations that reduce its effects before their passing. This push-and-pull stresses the need for the involvement of third-party, unbiased organizations and watchdogs to take the lead and hold these various companies accountable and trustworthy, following in the footsteps of centers such as Privacy International, which has worked to partner with civil society networks all around the globe and form a coalition of privacy advocates and researchers, including lawyers, ethicists, and technology experts. Unlike the food industry, which has the U.S. Food and Drug Administration (FDA) and the stock market, which has the Securities Exchange Commission (SEC), there is no such similar federal agency that oversees the Big Tech infrastructure. Because of this, infractions committed by Facebook, Apple, Alphabet, and others are dealt with on a case-by-case basis instead of consistent, 24/7 check-ins. With no federal technology oversight board, management bodies like Privacy International are critical in the fight to limit and prevent data exploitation, as these people can enter muddy waters that hamper involvement in the perspective of legislative involvement. The more of these oversight groups that are formed around the world, the more effective individual citizens are at inspiring systematic change, something which requires an overwhelming amount of consumers to support in order to succeed and convince these tech corporations. In coordination with the press and freelance journalists, oversight organizations would prove effective in disseminating the news to the public whenever there are breaches of responsibility and egregious management errors that may plague the digital COVID-19 scene. Once these partnerships are formed, society may even encounter a new generation of "muckrakers," groups of reform-minded writers and activists who originated during the Progressive Era (1890s-1920s) that provide citizens of "detailed, accurate journalistic accounts of political and economic violations and social hardships caused

by the power of big business" (The Editors of Encyclopaedia Britannica, 1998). These resources will be more and more useful and urgent as society recovers and begins to leave COVID-19 in the past.

Looking Forward

I understand we are currently living through an unforeseen situation that has led our government to fast-track possible solutions with technological capacities to address public health needs. As more time goes by, we will most likely witness the emergence of more in-depth peer-review networks, contracts, and more investigations into novel tracking apps, similar to what we see in other fields of science. Current limitations for contact-tracing services "require a large proportion of the population to use the app" (Budd, J., et al., 2020, p.1186). Many may view this feature as a negative, but I see it as the opposite. It serves to us as a reminder: to foster collective social good, we need a majority of people on board. If widespread skepticism persists, we will face less public cooperation due to preconceived notions. Therefore, Silicon Valley-based health monitoring companies have the incentive to provide additional transparency measures that will convince everyday Americans to log on without having to worry about privacy concerns. Inevitably, there will be another crisis that will force us to isolate. Concrete methods of trust and clear-cut responsibility should be considered and enacted now to create a future without fear of health data misuse by corporations and governments—especially amidst a global pandemic.

References

Birnbaum, M., & Spolar, C. (2020, April 18). Coronavirus tracking apps meet resistance in privacy-conscious Europe. Retrieved from https://www.washingtonpost.com/world/europe/coronavirus-tracking-app-europe-data-privacy/2020/04/18/89def99e-7e53-11ea-84c2-0792d8591911_story.html.

Budd, J., et al. (2020). Digital Technologies in the Public-Health Response to COVID-19. *Nature Medicine*, 1183–1189.

Energy and Commerce House Committee Press Release. (2020, September 2). *E&C Leaders Announce Committee Teleconference Forum on COVID-19 Testing, Contact Tracing and Surveillance on May 8*. Democrats, Energy and Commerce Committee. https://energycommerce.house.gov/newsroom/press-releases/ec-leaders-announce-committee-teleconference-forum-on-covid-19-testing.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., . . . Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science,368*(6491). doi:10.1126/science.abb6936

Jumbo Privacy. (2020, June). *Care19 Update: Foursquare allows developers to disable IDFA collection*. Jumbo Blog. https://blog.jumboprivacy.com/care19-update-foursquare-allows-developers-to-disable-idfa-collection.html.

Lacina, Linda. (2020, March 26). *Nearly 3 billion people around the globe under COVID-19 lockdowns*. World Economic Forum. http://www.weforum.org/agenda/2020/03/todays-coronavirus-updates/.

Martinez-Martin, N., et al. (2020). Digital Contact Tracing, Privacy, and Public Health. *Hastings Center Report*.

Mello, M. M., & Wang, J. C. (2020). Ethics and Governance for Digital Disease Surveillance. *Science Magazine*, *368*(6494), 951–954.

Nickelsburg, M. (2021). *Is the regulatory crusade against Big Tech over? What experts expect under Biden administration*. GeekWire. http://www.geekwire.com/2021/regulatory-crusade-vs-big-tech-facebook-google-amazon-fare-biden-administration/.

Perrigo, B. (2020, October 09). Will COVID-19 Contact Tracing Apps Protect Privacy? Retrieved from https://time.com/5898559/covid-19-contact-tracing-apps-privacy/.

Peterson, A. (2020, April 29). *Verily's COVID-19 website becomes a health data privacy battleground*. Protocol. http://www.protocol.com/verily-coronavirus-website-test-menendez.

Piller, C., et al (2016, March 28). *Verily, Google's bold bid to transform medicine, hits turbulence under a divisive CEO*. STAT News. http://www.statnews.com/2016/03/28/google-life-sciences-exodus/.

Sato, M. (2021, January 20). *Contact tracing apps now cover nearly half of America. It's not too late to use one.* MIT Technology Review.

http://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/.

Starks, T. (2020, July 6). *Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better*. POLITICO. http://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601.

The Editors of Encyclopaedia Britannica. (1998, July 20). *Muckraker*. Encyclopædia Britannica. http://www.britannica.com/topic/muckraker.

Véliz, C. (2019, September 2). *Privacy matters because it empowers us all*. Aeon. https://aeon.co/essays/privacy-matters-because-it-empowers-us-all.

Wallach, O. (2020, August 11). *How Big Tech Makes Their Billions*. Visual Capitalist. http://www.visualcapitalist.com/how-big-tech-makes-their-billions-2020/.

WHO. (2020, November 19). *Joint Statement on Data Protection and Privacy in the COVID-19 Response*. World Health Organization. http://www.who.int/news/item/19-11-2020-joint-statement-on-data-protection-and-privacy-in-the-covid-19-response.