Parnell, Caroline

Hester

CEPC0911

11 July 2020

# The Individual vs. The Collective Whole: Balancing Digital Privacy with Public Health During the COVID-19 Global Pandemic

## Introduction

The COVID-19 pandemic of 2020 marks the first major widespread global health emergency of the information age. The world is by no means stranger to disease outbreaks. In the past decade alone, the public faced Ebola and Zika virus; however, these outbreaks remained relatively localized. Ebola remained for the most part in West Africa [(“Ebola Virus Disease,” n.d.)](https://www.zotero.org/google-docs/?b1b8dE) and Zika in Brazil [(“Zika Virus Disease,” n.d.)](https://www.zotero.org/google-docs/?A7iOG4). Neither compares to the scale of the coronavirus outbreak. Analysis using the CDC’s Pandemic Severity Assessment Framework [(Reed et al., 2013)](https://www.zotero.org/google-docs/?W8L2sf), suggests that the risk and transmission rates of the virus are comparable to that of the 1918 Spanish Flu [(Freitas, Napimoga, & Donalisio, 2020)](https://www.zotero.org/google-docs/?EeuhGu). Added to the world’s growing dependence on technology, the coronavirus outbreak provided the perfect opportunity for public health officials to look to use information and communications technology as a means to educate the public and also enhance public health measures. One of the most significant ways in which technology is being used is the experimental adoption of digital contact tracing and exposure notification. In other words, tracking citizen’s movements through their personal digital devices and notifying them and medical officials if they are exposed or come in contact with another citizen who has tested positive. Such digital contact tracing has been vital to flattening the curve in many Eastern Asian countries such as South Korea, who slashed it’s daily new cases by over 95% [(“Daily Confirmed COVID-19 Cases and Deaths,” n.d.)](https://www.zotero.org/google-docs/?bBAU4i) from its peak on February 29. In the United States, however, the virus is still spreading at an alarming rate. Dr. Anthony Fauci remarked, the United States is facing a “serious problem,” as the United States soared past 150,000 deaths [(CDC, 2020)](https://www.zotero.org/google-docs/?V0CS6I). As other countries are seeing some success against the virus using digital contact tracing, one might wonder whether implementing such measures is a possibility for the struggling United States.

## Methods

A qualitative analysis was used to compare the fourth and fifth amendments of the United States Constitution against digital contact tracing plans of countries who were able to effectively flatten the curve of coronavirus cases in order to determine whether digital contact tracing models would be feasible or if it would contradict American ideals of privacy. The analysis used digital contract tracing plans from both China and South Korea as comparators. These states were chosen because they have each demonstrated a reduction of new cases per day of greater than 94% from their respective peaks to July 29, 2020. Coronavirus case data was harvested from Our World in Data (“Daily Confirmed COVID-19 Cases and Deaths,” n.d.). These states were also chosen because they have each launched digital contact tracing programs to help quell the spread of the coronavirus. Additionally, they represent two distinct styles of government, in order to capture measures implemented by both a more authoritarian regime and a democratic government. Information from the International Organization for Standardization (ISO) (“QR Traffic Light to Help Stop COVID-19,” n.d.) was used to gather details about the QR traffic light system implemented by Chinese officials, and information about South Korea’s Corona 100m app, including the number of downloads and how it works, was found in an article in the Harvard Business Review (Huang, Sun, & Sui, 2020) as well as an interview with the creator of the app in a CNN Business (Business, n.d.) article. These digital contact tracing models were then compared to the US law as laid out in the United States Constitution (“The Constitution of the United States,” 2015) and in the Bill of Rights (“The Bill of Rights,” 2015), which were both found in the National Archives, as well as former supreme court rulings regarding the fourth and fifth amendments. These articles and transcripts were found using Brown’s online library and Google Scholar and then filtered based on relevancy to the topic after an initial skim.

## Theory

Due to the individualist climate in the United States, it is unlikely that data sharing would be widely accepted by the American public despite its potential benefits in fighting the deadly war against the virus. Countries in Eastern Asia, in contrast, have a more accepting culture when it comes to putting the common benefit over their own individual rights or preferences. This is a possible explanation for the success of their digital contact tracing against the spread of the virus, as citizens are willing and able to sacrifice the privacy of their personal digital devices for a seemingly “greater good”. A team of ethicists at Harvard suggested that COVID-19 is a profound threat to American democracy [(Stanger, Tabarrok, & Tretikov, n.d.)](https://www.zotero.org/google-docs/?77mEJw). If this is the case, then researchers need to dig deep into the actions taken by democratic nations who have seen success against the spread of coronavirus to determine how the United States can act effectively against the pandemic.

## Results

While the word privacy is never explicitly stated in the Constitution or Bill of rights, the fourth and fifth amendments to the United States Constitution lay the groundwork for an American’s right to this privacy. Historically, the Supreme Court of the United States has attached great importance to the concept of personal privacy. In 1886, Justice Clark addressed the fourth and fifth amendments in *Boyd v United States*: “[The fourth and fifth amendments] apply to all invasions on the part of the government and its employees of the sanctity of a man’s home and the privacies of life.” (Krauss, 1977). In *Katz v United States*, Justice Harlan stated that the fourth amendment provided citizens with “a reasonable expectation of privacy,” (“U.S. Reports,” n.d.). In 2003, a bipartisan push to defend the Privacy Act stated that under the US Constitution, commercial companies would not be permitted to sell personally identifiable information to the federal government (Law, 2003). South Korea’s “Corona 100m” app, which collects data from public government sources, notifies users of any diagnosed COVID-19 patient within a 100-meter radius along with the patient’s date of diagnosis, age, gender, nationality, and that patient’s prior locations (Huang, Sun, & Sui, 2020). Under the Privacy Act in the United States, such qualifying data would be classified as personally identifiable information because someone could hypothetically determine the “anonymous” patient’s identity. In China, the QR Traffic Light system is a widespread government software being used to stem the spread of the virus. It works by assigning codes on a traffic-light principle: red, yellow, and green codes corresponding to high, medium, or low-risk states, respectively. Red codes are assigned to confirmed or suspected patients and yellow codes to persons who have been in contact with them. Citizens’ phone QR codes are scanned at entrances to public spaces, so in order to gain admittance, they must have a green code (“QR Traffic Light to Help Stop COVID-19,” n.d.). China’s QR system doesn’t directly share private information with the public, however, it’s system works by tracking people’s movements through their phone GPS. While it is illegal to track someone unknowingly in the United States, it would not technically be against the law if downloaders of the software signed a contract granting use of the location services of their mobile devices. This would prohibit the US government from implementing such tracing measures on a federal level, but it would not exclude private companies from developing similar software.

## Discussion

While, unsurprisingly, the South Korean contact tracing app broke United States privacy laws, the conclusion about the Chinese digital contact tracing software was unexpected. Granted, there is a profound caveat wherein American citizens would need to sign a contract if they were to participate in a contact tracing software similar to China’s. Given the United State’s individualist nature and aversion to data sharing, if such a software were to exist in the US, there would most likely not be enough Americans willing to take part in it to make the software successful. As the pandemic rages, Americans need to determine whether their allegiance lies with personal privacy or with public safety because, in light of the coronavirus, the two may be mutually exclusive. In such an individualist society, the public must be willing to put public health and “the greater good” above themselves. For this to happen, a substantial cultural barrier must be surpassed. The only question is whether such a barrier can be overstepped in a polarized political climate, a broken economy, and a deadly public health emergency.

## Conclusion

After a qualitative analysis was performed comparing “Corona 100m” and the “QR Traffic Light” system against the fourth and fifth amendments of the United States Constitution, it was determined that “Corona 100m” would not be permissible by US law but the “QR Traffic Light” system would be operable if participants willingly signed a contract releasing their location data to a private company. Since the United States Constitution is interpretable in various contexts, a drawback of this study is that the United States Supreme Court could potentially rule differently if given the opportunity. This is why the study was conducted using excerpts from past supreme court cases, but the court still reserves the right to walk back a previous statement. Until the court explicitly states otherwise, software companies and app developers should continue to curate potential digital contact tracing operating systems for use in the United States as a combatant against the spread of the novel coronavirus.

## References

[CDC. (2020, February 11). Coronavirus Disease 2019 (COVID-19). Retrieved July 17, 2020, from Centers for Disease Control and Prevention website: https://www.cdc.gov/coronavirus/2019-ncov/global-covid-19/index.html](https://www.zotero.org/google-docs/?bIJ1zo)

[Daily confirmed COVID-19 cases and deaths. (n.d.). Retrieved July 29, 2020, from Our World in Data website: https://ourworldindata.org/grapher/daily-covid-cases-deaths](https://www.zotero.org/google-docs/?bIJ1zo)

[Ebola virus disease. (n.d.). Retrieved August 2, 2020, from https://www.who.int/westernpacific/health-topics/ebola](https://www.zotero.org/google-docs/?bIJ1zo)

[Freitas, A. R. R., Napimoga, M., & Donalisio, M. R. (2020). Análise da gravidade da pandemia de Covid-19. *Epidemiologia e Serviços de Saúde*, *29*, e2020119. https://doi.org/10.5123/s1679-49742020000200008](https://www.zotero.org/google-docs/?bIJ1zo)

[Reed, C., Biggerstaff, M., Finelli, L., Koonin, L. M., Beauvais, D., Uzicanin, A., … Jernigan, D. B. (2013). Novel Framework for Assessing Epidemiologic Effects of Influenza Epidemics and Pandemics. *Emerging Infectious Diseases*, *19*(1), 85–91. https://doi.org/10.3201/eid1901.120124](https://www.zotero.org/google-docs/?bIJ1zo)

[Stanger, A., Tabarrok, A., & Tretikov, L. A. (n.d.). *ANNE-MARIE SLAUGHTER*. 56.](https://www.zotero.org/google-docs/?bIJ1zo)

[Zika virus disease. (n.d.). Retrieved August 2, 2020, from https://www.who.int/health-topics/zika-virus-disease](https://www.zotero.org/google-docs/?bIJ1zo)