Privacy in the Age of the Coronavirus: A Deontological Perspective

Sarah Mardjuki

Abstract

The COVID-19 pandemic has rigorously tested government emergency response systems, from detection to monitoring to treatment. As governments have raced to slow the speed of the pandemic, they have turned to digital surveillance technologies to help them enforce lockdowns and conduct contact tracing for infected patients. However, the collection and publication of personal health and location data can often lead to harmful consequences for individual privacy rights. This paper examines the measures the South Korean government has taken with regards to pandemic surveillance technology. Under a deontological framework, this paper also establishes clear guidelines for acceptable use of surveillance technology during pandemics, acknowledging that surveillance systems can often provide crucial data needed to lower the coronavirus case rate. These guidelines cover privacy, consent, and the potential consequences individuals may face as a result of the usage of surveillance technology. As countries scramble to collect and analyze pandemic data for key insights on the spread of the virus, clear guidelines are crucial to maintain a balance between public health and privacy.

Introduction

With over 2,407,000 confirmed cases and over 165,000 deaths (as of April 19, 2020), COVID-19 has swept across the globe, leaving countries scrambling (Worldometer, 2020). As governments attempt to slow the spread of the virus, more and more attention has turned to the use of digital technology for surveillance and containment purposes. In ten minutes, the South Korean government can generate a list of everyone an infected patient has had contact with using smartphone location data. The Israeli government has called upon Shin Bet, its counterterrorism intelligence unit, to track down those who have been potentially infected (Lin and Martin, 2020). Aggregating data points like location data, credit card records, and public transportation data can paint a vivid and extremely accurate picture of where an infected patient has been. But this vast wealth of data comes at a significant cost to the consent and privacy rights of individuals. This paper will weigh the balance of public health and the right to privacy using a deontological perspective and propose guidelines for morally acceptable use of surveillance technology during a pandemic. The South Korean government's response will be used as a case study to examine where surveillance measures have failed according to these principles and what improvements can be made to balance the effectiveness of the technology with individual privacy rights.

Deontological Framework

This paper will utilize three primary deontological principles: Kant's Formula of the Universal Law, Kant's Formula of the End in Itself, and Ross's concept of *prima facie* duties. When it comes to matters of privacy and consent, only a deontological framework can provide the appropriate structure needed to evaluate such issues and weight infringements on individual rights accordingly.

Kant's Formula of the Universal Law dictates that one should act in such a way that that action can be turned into a rule that can be consistently universalized. When applied in practice, this principle helps guide rules for the usage of digital technology in relation to privacy, autonomy, consent, and other issues. Kant's Formula of the End in Itself demands that individuals are treated as ends in themselves, not as mere means to an end. This principle ensures that the uses of technology are driven by the right intentions and are not created for selfish purposes. Finally, Ross's concept of *prima facie* duties states that we have a duty to fulfill a variety of duties, not merely the ones that Kant lists. These duties may conflict at times, and certain duties may override others. In practice, Ross's duties of nonmaleficence, harm prevention, and beneficence will help ensure that a technology will not cause unreasonable harm.

Privacy vs. Public Health: A Case Study of South Korea

As the coronavirus has spread from country to country, governments have increasingly turned to surveillance in order to enforce lockdown measures and track the spread of the virus. Governments are tapping hospital and telecommunication records to gather data points on age, gender, travel history, home address, previous locations, and more on infected patients. The key dilemma that emerges is the age-old battle between individual rights and societal benefits. While these surveillance measures may be an effective method to flatten the curve, they come at a significant cost to privacy rights. The following will examine the extent to which pandemic surveillance in South Korea has come at the price of privacy.

South Korea: Swift Coronavirus Response, But At What Cost?

South Korea experienced its first case of coronavirus on January 20, 2020, with cases peaking on February 29, 2020. In just 20 days following the peak, South Korea was able to

flatten the curve of the number of coronavirus cases diagnosed (Woodward, 2020). In its report, "Flattening the Curve on COVID-19: The Korean Experience," the South Korean government credits this achievement to the usage of information and communications technology to educate, test, and trace its citizens. From a privacy standpoint, two measures stand out as potential causes for concern: 1) the tracking apps the South Korean government utilizes to collect personal and location information, and 2) the publication of individual travel and location history records of infected patients onto the government's Ministry of Health and Welfare website.

The South Korean government's self-diagnosis app forces inbound travelers to input their personal information and report their health condition for a 14-day quarantine period. Beginning February 12, all inbound travelers from China were required to download the app; however, effective April 1, all inbound travelers have been required to download the app before being granted entry. Downloaded over 170,000 times, the app collects user information such as passport numbers, nationality, names, and addresses. It also requires travelers to report body temperature, coughs, sore throats, and difficulties breathing once a day until their quarantine has been lifted. Failure to submit a daily report for two consecutive days will result in text message warnings from the government. An additional day without a health status report will result in a phone call from the government. If after four days the user does not comply, the South Korean police force is called upon to track the user down (Government of the Republic of Korea, 2020).

The South Korean government's self-monitoring app provides similar features but for all individuals under self-quarantine. Launched on March 7, 2020, it was made voluntary for Korean citizens to download. However, as of April 1, all travelers entering Korea – including Korean nationals – are required to download the app before being granted entry to the country. With this mandate, the app reached a 91.4% download rate of those under self-quarantine. The app

connects users with a government case officer and requires users to submit a similar health report to the one described above, twice a day. The app also collects GPS location data and sounds an alarm when the user leaves their quarantine area. The alarm notifies the assigned government case worker, who establishes contact with the user to encourage them to return home (Government of the Republic of Korea, 2020).

Finally, the South Korean government has publicized a database of infected patients' past locations, dates of diagnosis, age, gender, and more. The government compiles this information using telecommunication, credit card, and CCTV data (Government of the Republic of Korea, 2020). Whenever a new patient tests positive for the coronavirus, the database is updated on the government's Ministry of Health and Welfare website and a series of mass emergency text alerts are sent out, regardless of if the patient has consented or not. While patient names are omitted from the database, the identity of patients is not completely untraceable given the wealth of information being published. Infected patients have still faced harassment and judgment, both surrounding their whereabouts and for transmitting the virus to others. Patients are repeatedly blamed for spreading the virus and harassed over social media (BBC, 2020). A survey of 1,000 South Koreans by the Seoul National University's Graduate School of Public Health revealed that people were more afraid of "criticisms and further damage they may suffer from being infected" than having the actual virus itself (BBC, 2020). While the database has certainly done much to improve access to updated, crucial information, it has also come at the cost of patient consent and privacy rights and has led to significant harassment of patients.

Determining Appropriate Surveillance Technology Usage During a Pandemic

Given how quickly South Korea was able to flatten the curve, it is clear that from a public health perspective, the government's response was effective. However, it is also evident that

there are privacy concerns with publishing so many personal data points on such a wide scale. Defining technology usage guidelines using deontological principles can help create a balance between these two opposing forces. Specifically, in order to be morally permissible under deontological theory, pandemic surveillance measures must 1) give prior notification of usage of the technology with a viable option for nonconsent, 2) be rigorously tested to ensure that the technology does not cause harm and must be accompanied by reconciliatory measures if harm is created, and 3) avoid restricting agency for those that have nothing illegal or immoral. Using these guidelines, it becomes clear that the South Korean government apps fail primarily the first principle, while the government's database fails all three.

1. Prior Notification of Technology Usage

First, governments must give prior notification of the usage of pandemic surveillance technology and must give individuals a viable option for nonconsent. Individuals have a right to know when, how, and where the technology will be used. Given the potential sensitivity of health and location data, prior notification is imperative. As a key second point, individuals must be able to choose nonconsent as a viable option, without further consequences. Under this principle, governments could not punish individuals who choose to not share their data but instead would have to respect their wishes.

Failure to give prior notification of technology usage fails all three deontological principles discussed in the framing section. It violates Kant's Formula of the Universal Law because allowing a government to deploy surveillance technology without having to inform the public would not be universally applicable. Those within the government would certainly agree to such a plan, but the individuals who are being surveilled would likely not. However, if governments were transparent surrounding their technology usage and individuals were given a

viable option for nonconsent, all parties would likely agree. Additionally, failure to give prior notification violates Kant's Formula of the End in Itself, which requires that every action treat individuals with respect. Utilizing surveillance technology without consent violates their right to privacy. Even if a justification like public health is used to defend the use of the technology, this would still assume that the will of the government matches the will of the individual. While this may be true in some instances, such an assumption would be treating the individual as a mere means to an end. Finally, the requirement for non-consent to be a viable option emphasizes the respect for the freedom of individuals, a possible addition to Ross's list of *prima facie* duties. Governments should not be able to coerce individuals into participating in surveillance.

In the context of South Korea, it is clear that the government's response violates both elements of this principle. Firstly, the government does not give prior notification of the usage of the technology before publishing the data online. Both the collection and publication of personal data are also conducted without patients' consent. Secondly, there is no viable option for nonconsent on multiple levels. Patients are unable to opt out of the database and can do nothing to stop the government from collecting data on them. Individuals are also forced to use the government's apps, with the threat of police force for noncompliance. Thus, the South Korean government's response fails this first principle.

2. Rigorous Testing to Ensure Limited Harm

Next, the technology must be carefully tested to ensure that no individuals will be unfairly targeted or harmed as a result of the system. Governments must anticipate foreseeable harms and create solutions to limit those harms. In this case, governments need to take significant measures to mask patient identities and ensure that patients do not face stigma once

their data is released to the public. This also entails ensuring that the data is properly protected and erased post-pandemic.

Failure to do so is a clear infringement on Ross's duties of beneficence, nonmaleficence, and harm prevention. The government fails its moral duties to protect its citizens when it knowingly deploys a system that causes patients significant harm. With pandemic surveillance technology, patients bear significant costs – both the publication of their personal data and the potential ensuing harassment – with little upside. Such practice could also be treating infected patients as a mere means to the health and safety of the larger group, a violation of Kant's Formula of the End in itself. Without a reasonable attempt at mitigating harms created by the surveillance system, the government risks treating a group of its citizens as expendable. With regards to Kant's Formula of the Universal Law, it is clear that individuals would never consent to the publication of their personal data when such publication could become fodder for harassment.

In this case, the South Korean government can do much more to protect the patients whose data they are exposing. From a data publication standpoint, the government can do a much better job of anonymizing the dataset to ensure that patients' identities cannot be detected. This can include removing information like gender and age, which may be less essential information for the public but which can go a long way to protect identities. The government can also choose to not make the database public and instead to individually reach out to people who may have had close contact with the patient to restrict access to the data. Additionally, as anxieties rise with the number of coronavirus cases diagnosed, it is foreseeable that those already inflicted with the virus will be unfairly harassed for unknowingly spreading the virus to others. At the very least, the government can accompany the data and emergency text message alerts

with a reminder that infected patients should not be treated as the enemy and that the alerts were simply for informative purposes. Instead of doing this, however, the South Korean government has exposed extremely sensitive data with no attempt to mitigate the backlash that patients have experienced. In one notable instance, the mayor of one city in South Korea even exposed the last name of one of the patients listed in the database (BBC, 2020).

3. Avoid Restriction of Agency

Finally, usage of technology cannot go so far as to restrict the agency from those who have done nothing wrong. This principle dovetails nicely from the previous discussion on limiting harm to patients who are included in a database. Even if the usage of pandemic surveillance technology satisfies the first two criteria, it may still be impermissible if it denies autonomy to those that are acting within the law. In this context, a surveillance system is impermissible if it creates a scenario where infected patients are frightened to freely live their lives post-recovery for fear that others may continue to harass them. This would violate the autonomy and agency of individuals who have done nothing wrong except to be unfortunate enough to contract the virus.

The restriction of agency is a violation of Kant's Formula of the End in Itself and a violation of Kant's *prima facie* duties of justice and beneficence. Quarantine and self-isolation aside, restricting the freedom of patients to go about their daily lives cannot be viewed as just. While patients may still experience some degree of harassment regardless, the government publishing exact whereabouts and information surrounding infected patients goes a long way in enabling those who want to place blame on certain people for the spread of the virus. More broadly, the system restricts agency and freedom for patients and nonpatients alike, since currently healthy individuals may someday contract the virus and have their information reported

in the database as well. Thus, this fails Kant's Formula of the Universal Law, since all parties would never agree to this version of the surveillance system.

In this case, the South Korean government has created a system which restricts the freedom of both healthy and infected individuals. Healthy individuals may feel as though they cannot live their lives normally for fear that the places they frequent may be exposed if they are diagnosed with the coronavirus. Infected patients may experience threats and harassment that may continue even after they have recovered. The fact that more people are less scared of the virus itself and more scared of the blame and judgment they would receive if they contracted the virus speaks volumes. As such, the government should mitigate these concerns with better data protections and better transparency surrounding how and what data will be published.

Conclusion

In summary, pandemic surveillance technology can only be morally permissible under a deontological framework if it satisfies the following three conditions. First, individuals must receive prior notification of the technology's usage and a viable option for nonconsent to avoid infringing on the privacy rights of individuals without their consent. Second, the technology must be rigorously tested to ensure that it does not cause harm, and proper reconciliatory measures must be taken to mitigate any harms that may arise. Third, the technology cannot restrict the agency and freedom of individuals who have not committed any wrongdoings. A system that fails on any number of these points is morally impermissible. The South Korean government's response demonstrates that while these surveillance technologies can do much to provide swift, accurate information to the public, they can also cause significant emotional and physical harm to patients whose data are contained within the government's database. However, with appropriate protective measures, the government can mitigate many of the key concerns

while still making use of its successful surveillance technology. Properly executed pandemic surveillance systems must strike a careful balance between public health and individual rights to autonomy and privacy. The key is recognizing that the relationship between these two concepts is one of a balance, not a tradeoff. As more and more countries turn to surveillance technology to monitor and slow the rate of coronavirus cases, robust data protection guidelines are imperative. Without these guidelines, lost privacy rights will be yet another side effect to the pandemic.

References

BBC News. (2020). *BBC News*. Coronavirus privacy: Are South Korea's alerts too revealing? Retrieved April 21, 2020, from https://www.bbc.com/news/world-asia-51733145.

Government of the Republic of Korea. (2020). *Flattening the curve on COVID-19: How Korea responded to a pandemic using ICT*.

Lin, L, and Martin, T. (2020). *Wall Street Journal*. How Coronavirus Is Eroding Privacy. Retrieved April 19, 2020, from https://www.wsj.com/articles/coronavirus-paves-way-for-new-age-of-digital-surveillance-11586963028.

Woodward, A. (2020). *Business Insider*. South Korea controlled its coronavirus outbreak in just 20 days. Here are the highlights from its 90-page playbook for flattening the curve. Retrieved April 20, 2020, from https://www.businessinsider.com/how-south-korea-controlled-its-coronavirus-outbreak-2020-4.

Worldometer. (2020). *Worldometer*. Covid-19 Coronavirus Pandemic. Retrieved April 19, 2020, from https://www.worldometers.info/coronavirus/?utm_campaign=homeAdUOA?Si.