*The Dartmouth Undergraduate Journal of Politics, Economics, and World Affairs*
*Volume. I, Issue. III, 23-52, June 2021*

# Tracking the Tracing:
# A Global Investigation of Privacy Issues in the Age of COVID-19

JESSIE MILLER

Claremont McKenna College

ABSTRACT: As the COVID-19 pandemic tore through the globe, policymakers grappled with two key questions. First, to what extent could new tools to collect and analyze data on a massive scale help limit the virus's spread and, second, how would the collection of that data impact the privacy rights of individuals? This paper examines both questions and reveals how nation-specific traditions, values, and leaders shaped the delicate balance between the right to privacy and the protection of the population from COVID-19. An exploration of the surveillance techniques developed in response to the SARS and HIV pandemics reveals the growing consensus around the importance of accurate data collection and analysis. Next, this paper examines the COVID-19 response in 6 areas (China, South Korea, Singapore, Israel, the United States, and the European Union) to demonstrate the diverse array of responses to the pandemic. Different attitudes toward privacy and government control in each country led to dramatically different outcomes. Finally, this paper examines the role of regime type, leadership, experience with pandemics, and privacy norms in a comparison between China and the United Kingdom. This paper concludes by arguing that the balance between privacy and health can be successfully maintained by ensuring government transparency, reasonable scope and duration of implemented measures, and optimized use of technology to reduce excess data collection.

## Section I: Introduction

As COVID-19 spread throughout the world, causing shutdowns and disruptions to modern society on an unprecedented scale, the threat of pandemics became painfully clear. The failure of governments and international organizations to prevent and mitigate the dangers of a global pandemic such as COVID-19 has left many desperate for the creation of new policies, norms, and infrastructure. The scientific community, alongside policy experts, demands the utilization of data that are mass collected in the 21st century to respond to pandemics. While this may be effective, if not vital, in the fight against COVID-19, one would be remiss to ignore the privacy implications of tracking the disease and its human carriers.

This paper will examine the privacy implications and efficacy of a data-driven tracking approach, with its scope limited to the first six months (March through August 2020) of the pandemic. Focusing on the early months of the pandemic provides insight into governments' immediate responses, and allows investigation into policymakers' first instincts when they are faced with crises. This paper also contains two sections of cross-country comparison; the first

details the strategy, efficacy, and privacy implications of pandemic response from a diverse subset of nations, while the second explores how regime type and leadership impacted nations' pandemic response in China and the United Kingdom.

**Section II: A Fundamental Review of Relevant International Pandemic Response Policy**

Recent history lends an important perspective on the pandemic response. With our technological capabilities increasing at breakneck speed, pandemics such as Severe Acute Respiratory Syndrome (SARS) and Human Immunodeficiency Virus (HIV)/Acquired Immunodeficiency Syndrome (AIDS) provide the most applicable insight into technologically-assisted responses to pandemics, as governments' utilized digitally-assisted tracking systems and developed surveillance databases. SARS is relevant to study because it, like COVID-19, is caused by a coronavirus. Reflecting on the response to HIV/AIDS is also of interest because, as will be further discussed below, it had the most significant privacy implications of any recent pandemic or epidemic.

SARS is often referred to as the first pandemic of the 21st century. The disease is thought to have first emerged in the Chinese province of Guangdong and quickly spread throughout many countries, killing hundreds. Knowledge of the disease spread internationally when the World Health Organization (WHO) sent out a worldwide alert on March 12, 2003, describing a "severe respiratory illness of undetermined cause that was rapidly spreading among hospital staff in Hong Kong."[1] Within months, many nations implemented new policies and responses to combat the spread.

One common approach included setting up measures to track persons who were suspected to be infected. For example, the United States implemented a tracking system in an attempt to contain the spread. Soon after the WHO announcement on March 12th, 2002, the United States developed a case form to track and collect demographic data about the spread. Healthcare providers were requested (though not required) to report all suspected cases of SARS to the CDC and data on possible carriers was collected and added to a national "line list." It is unclear whether patient permission was expressly requested before personal information was added to the list. This method of tracing was technologically limited in the sense that the collection of information was paper-based, though the CDC did keep epidemiologic data in an electronic database.[2] To evaluate the effectiveness of such a response, it is helpful to analyze the surveillance system sensitivity, which is the measurement of the proportion SARS found through the surveillance system implemented in the United States. Since there were eight confirmed SARS cases, and all had been identified as "probable cases," the sensitivity was an impressive 100%.[3]

Canada took a similar approach to combating SARS. The nation created a SARS hotline which was tasked with identifying potential SARS cases and contacts of infected individuals. People voluntarily called the line to report symptoms and exposure to SARS, and to ask questions about the disease. Additionally, a case reporting telephone system was developed to help hospitals report cases with ease. Furthermore, a Case Management team was established to investigate reports of potential SARS cases and determine if they met the criterion to be classified as a suspect case. Through these methods, Canada conducted 2,000 case investigations, identified 23,300 possible contacts, and placed 13,374 individuals in quarantine.[4] This method was relatively effective, since the outbreak was able to be contained within populations such as hospital staff, patients and their visitors, and household members of known cases.[5]

Other countries opted to go beyond reporting and tracing to screening individuals in public places and at points of travel in ways that had little cause for privacy concerns. For example, in Singapore, many public buildings, offices, and residential spaces required a temperature check upon entry.[6] At Singapore's Changi Airport, travelers were met with infrared scanners that screened body temperature; Hong Kong, China, the Philippines, Thailand, and Taiwan also followed suit in screening passengers' temperatures.[7] The screenings do not appear to have been recorded, added to any database, or shared among any nations. Accordingly, such airport screenings did not result in any accusations of privacy invasion. The screenings appear to be moderately effective. Before the implementation of screening policies, transmission of the disease occurred on five flights that infected individuals onboard. After its implementation, which was recommended by WHO in March 2003, no additional flight transmissions were identified.[8]

The myriad of international SARS policies raised many questions about the legality and rights implications of health surveillance. Tracking an individual's contacts, movements, and health data in the name of public health posed threats to privacy. Individuals' health data is widely considered sensitive information, and is treated with an expectation of confidentiality. Furthermore, in the haste to respond swiftly to the threat of SARS, legal professionals and courts had little say in the health policies and mitigation efforts of their respective nations. A legal review undertaken by Leslie Jacobs of York University examined legal consciousness during SARS in Hong Kong, Shanghai, and Toronto. Jacobs found that legal actors such as judges and lawyers were uninvolved in the public health efforts to reduce the spread of SARS.[9] The exclusion of legal actors was problematic because the very parties that are tasked with the protection of and advocacy for rights were cut off from forming responses that had rights implications.

The response policies' disconnect with legal considerations disregarded the priorities and concerns of many citizens. A survey conducted by Shanghai Academy of the Social Sciences as part of the Asia Pacific Dispute Resolution Project shows that individuals in Singapore and Toronto did not approve of their governments disregarding rights during times of health crisis.[10] Of the approximately 200 Toronto residents who were surveyed, only 19% of respondents gave the highest importance to the government having the right to do whatever it judged necessary to prevent the spread of the disease. This shows that individuals are not willing or comfortable with sacrificing their privacy and freedom of movement in the name of public health.

Furthermore, a survey taken by 634 residents of Singapore reflects concerns about their government's response to the pandemic in terms of privacy violations. Almost two-thirds of respondents protested against the broadcast of names to the public of those who were under quarantine orders, and 33.1% of the total respondents were against the hypothetical installation of web cameras and tag surveillance of those under home quarantine orders. In the case of public health responses aimed at preventing the spread of SARS, there is clear evidence of privacy concerns.

Similar concerns about the right to privacy concerns emerged during the HIV/AIDS epidemic. Many of the first recognized cases of AIDS emerged in 1981 in the United States, though the virus soon spread globally. Transmitted through sexual contact, blood contamination, needles, and from mothers to infants, tracking carriers of the disease quickly was a common policy. However, challenged by privacy concerns and the stigma surrounding HIV/AIDS infections, nations faced a struggle between protecting the confidentiality of infected individuals while also effectively preventing the spread of the disease. Some nations prioritized prevention

over confidentiality, using name-based tracking of infected individuals. Other countries were more conscientious of privacy concerns, and developed alternative tracking measures that protected infected individuals' identities to varying degrees. It is imperative to recognize that homophobia and a lack of information about HIV/AIDS shaped both policy design and outcome.

One of the nations that is well known for robust HIV/AIDS surveillance is Cuba. Favoring prevention over confidentiality, Cuba developed strong testing and tracking measures. For example, by February 1988, Cuba had the capacity to test 25% of its sexually-active population; this was accomplished through mandatory testing of blood donors, pregnant women, those with other sexually transmitted infections, all hospital admissions, and sexual contacts of infected individuals.[11] Tracing and notifying the sexual contacts of individuals who have tested positive was a controversial aspect of Cuba's HIV/AIDS policy. Many concerns about protecting infected individual's identities to protect them from social stigmatization arose. Although Cuba has faced criticism for its response, as it violated the privacy of infected persons and endangered their safety, the country has touted the effectiveness of its HIV/AIDS policy. As of 2008, Cuba claimed the highest level of AIDS treatment and the lowest rate of HIV infection out of the entire Caribbean region.[12]

Other countries worked to find alternative, less invasive, methods of tracking the disease and its carriers. Two such countries were Canada and (within certain states) the United States. Canada implemented a compulsory case reporting system in which medical providers entered information on their patient's birth dates, gender, and risk behaviors into a database that was maintained by the Massachusetts General Hospital Utility Multi-Programming System (MUMPS). This was done in an effort to provide some measure of protection for infected patients' identities, while also enabling public health officials to identify trends such as higher HIV rates among injection drug users and native British Columbians.[13]

Both Maryland and Texas took initiative and separately attempted to develop their own state surveillance systems that utilized non-name unique identifiers (UI) in the early 1990s. The UI codes were comprised of the last four digits of the patient's Social Security number, six-digit date of birth, one-digit code for race/ethnicity, and one-digit code for sex.[14] These codes were then entered into a surveillance database, which the CDC planned to later evaluate. Although there was cooperation between state and federal authorities, the UI systems in Maryland and Texas were developed as a result of the states' own prerogatives. Unfortunately, these systems faced problems such as attaining the data elements to construct a UI (e.g. failing to collect Social Security Numbers) and the issue of duplicate tests interfering with the accuracy of collected data.[15] The UI system also made it difficult to follow-up with those who had tested positive; only 60% of reports could later be matched to client records.[16] As a result, Maryland and Texas deemed the system to be "unworkable" and abandoned it in favor of name-based reporting.[17]

In light of the failed attempts made by Maryland and Texas to adopt a UI system, many states overlooked confidentiality concerns and adopted name-based tracking systems. In fact, 31 states were conducting name-based HIV surveillance as of January 1998.[18] This was bolstered by a 1999 policy by the Center for Disease Control (CDC) that required states to adopt a system of HIV case reporting that encouraged (though did not require) the use of names. The shift towards name-reporting reflects many Americans' beliefs that previous AIDS responses had been inadequate and unaggressive.[19] Most AIDS-service organizations continued to support UI and oppose name reporting, though the CDC found that "such an approach would simply impede the adoption of an effective system of surveillance." [20] The divergence of opinions on UI by AIDS-service organizations and the CDC highlights underlying biases that inform government policy.

Service organizations worked first-hand with infected individuals, and thus were more sympathetic towards the privacy concerns of persons living with HIV/AIDS.

Internationally, a common method of global surveillance included the use of unlinked anonymous testing (UAT). UAT involves screening blood specimens that were taken for purposes besides HIV testing and stripping them of personal identifiers without informed consent of the patient. This was done in an attempt to gather data for public health officials to analyze that would not be tainted by selection or participation bias.[21] This response policy faced backlash from ethicists, policymakers, and academics for a multitude of reasons; the failure to obtain consent from the patients raised ethical questions and also prevented medical practitioners from notifying those who had tested positive. The tides turned most dramatically against UAT when the United States developed guidance for AIDS surveillance as a part of the President's Emergency Plan for AIDS Relief (PEPFAR). This plan dictated that the default position was non-UAT-based surveillance and that "a waiver should be submitted to conduct UAT surveillance."[22] As a result of these shortcomings and public opposition, most countries have since abandoned this method.

Privacy considerations are of particular import when it comes to examining HIV/AIDS response policies. In 1987 as many as 90% of AIDS cases in North America were in people who are homosexual, bisexual, hemophiliac, and/or those exposed through intravenous drug abuse or contaminated blood products.[23] This is significant because a large proportion of infected individuals come from groups that are marginalized, and as a result stigma around HIV/AIDS itself has developed. The need for confidentiality in the handling of identifying and tracking those infected individuals is therefore of the utmost importance.

Problematically, there are often breaches of confidentiality when it comes to handling sensitive health information. There have been many instances of disclosure of such information, leading to a sense of distrust and fear from those who are affected by HIV/AIDS.[24] For example, in 1991 a doctor at Pacific Oaks Medical Group (a clinic specializing in AIDS treatment) disclosed the information of infected patients to a fellow doctor looking to solicit supporters for homosexual candidate who was running for office.[25] This is merely one example of an unquantifiable number of unwarranted disclosures that led affected populations to believe disclosures were common.[26]

Disclosures are damaging to HIV/AIDS public health responses because "in the context of the intense concerns of gay men about government intentions and the severe consequences of disclosure of HIV status, the guarantee of confidentiality was a prerequisite to encouraging affected populations to access the health care system."[27] Inadequate privacy protections can deter high-risk populations from seeking essential care and can hinder effective tracking that can mitigate the spread of HIV/AIDS. As a result, confidentiality should be prioritized when designing and implementing any public health strategies.

If the difficult experience responding to SARS and HIV/AIDS has taught us anything, it is that there is a delicate balance between designing effective (and often intrusive) public health strategies and preserving the rights of those who are affected by pandemics. These issues existed before and throughout the development of the technology that exists today; as a result the effectiveness and intrusiveness of health surveillance has exponentially increased. Although nations such as Cuba have claimed great success in preventing the spread of a disease such as AIDS, they have not done so without threatening the ability to maintain necessary confidentiality. On the other hand, states such as Maryland and Texas learned the hard way that protecting the privacy of infected individuals can impede the effectiveness of a public health

strategy. Strategies developed in response to COVID-19 should keep in mind the lessons of past pandemics and work to find a balance between privacy and efficacy.

## Section III: Background on COVID-19 and its Privacy Implications

COVID-19, commonly referred to as coronavirus, originated in Wuhan, China in 2019. Though the origins of the disease are disputed, it is thought that it likely emerged in the Hunan seafood market in Wuhan and quickly spread to more than 50 individuals.[28] The disease is spread from human to the human and is highly transmissible and deadly. As a result, it has spread to nearly every country and has claimed millions of lives. Nations across the globe have rushed to find different solutions to combat this growing crisis. Yet in their haste to develop effective public health strategies, concerns about rights and privacy have been oft left unconsidered.

Rights protection plays an important role in determining the efficacy of any response. In order for any contact tracing to be effective, public trust and enthusiasm is a must.[29] This is especially important for any voluntary solutions; if concerns over privacy exist, there is little to no chance of adoption being widespread. A study conducted in April 2020 by the University of Washington surveyed the opinions and preferences of 100 individuals.[30] The study found that while 72% of those surveyed were open to downloading a contact tracing app that "protected their data perfectly," that number decreased as they were asked about an app with less protections. For example, when respondents were asked about an app that knew their location but claimed not to share it, only 19% of respondents said they would be extremely likely to download it. In addition, only 49% of respondents felt that it was somewhat likely that they would download an app that shared their location with their government. Public trust and privacy protections are important to consider in designing any public health measure. If public trust is undermined, people will be less likely to follow other public health advice (such as wearing masks or social distancing) that could help prevent the spread of the virus.[31]

Concerns about the diminution of privacy rights are not limited to the short-term implications of COVID-19 public health strategies. In fact, there are many long-term concerns about the permanence of emergency measures. If countries spend lots of money and effort developing strong surveillance measures, they may be unwilling to dismantle them after the crisis has passed. This was seen in the United States after the terror attacks on 9/11. In response to these attacks, the United States government developed the Patriot Act and other anti-terror measures that continued to be used for purposes outside of their initial design.[32] In the aforementioned survey conducted by researchers at the University of Washington, respondents were unsupportive of governments collecting and utilizing location data.[33] Specifically, respondents felt that they did not trust their governments to use collected data solely for COVID-19 mitigation efforts and 72% of respondents reported that they felt it was "extremely unlikely" that collected data would be deleted after the threat of COVID-19 subsided. In addition, more than half of respondents were concerned that sharing their data would "bring harm to themselves or their community."[34] When designing measures to combat the spread of COVID-19, caution surrounding their permanence and scope must be employed.

Another emerging issue involves the growing power and influence of the tech industry during the pandemic. As these companies work to promote a better public image during the crisis, they also hope to increase their influence on politics. During COVID-19, tech companies have increased their lobbying efforts in order to precipitate favorable policies and weak regulation of their behavior. This has led to concerns that privacy protections will be dismantled to support the interests of technology companies as a result of their 'good behavior' during the

pandemic.[35] As nations turn to technology to enable and promote societal recovery from COVID-19, resources and power will be handed over to a limited number of private players in the technology sector.[36] These companies face countless accusations of privacy infringement as they amass large amounts of personal data from their consumers. As a result, their empowerment during the COVID-19 crisis raises concerns about their ability to dismantle privacy protections in the future.

The global privacy issues that have arisen during COVID-19 will not fade even if a cure or vaccine is produced. As experts predict increasing incidents of serious pandemics, the rights issues that they pose become greater threats.[37] The increase in pandemic frequency, coupled with rapid technological advancements, makes it imperative to consider and design adequate policy measures that balance public safety and individual privacy.

**Section V: A Review of International COVID Policies, Their Effectiveness, And Their Privacy Implications**

This section explores the diverse COVID-19 response policies implemented in China, South Korea, Singapore, Israel, the United States, and the European Union. For each country, the policies are identified, and their efficacy and privacy implications are explored. These countries were selected because they each utilized unique approaches that provide insight into the diverse array of possible public health measures.

**China:**

Following the devastating 2003 SARS outbreak in China, the government drafted the "Regulations on Preparedness for the Response to Emergent Public Health Hazards" in order to create an emergency response plan for future epidemics.[38] As a result, at the outset of the outbreak, China enacted measures such as closing transportation in Wuhan, canceling New Year celebrations and other large gatherings, enacting self-quarantine orders, and closing public spaces like schools and restaurants.[39]

Additionally, the implementation of contact tracing apps has become widespread, often in the form of digital applications such as software on smartphones.[40] China integrated one such software, dubbed "Health Code," into the popular wallet app Alipay that has over 900 million users.[41] Reports indicate that usage of the app is, in essence, mandatory for all kinds of movement within China; to use services such as public transportation or to enter a supermarket, one must display their status on the app.[42] Those who use the app are given color-coded QR codes depending on their COVID-19 risk. Those who have not been exposed to an infected individual should display a green QR code, while those who may have come in contact with the virus or a carrier display yellow or red codes. China has also developed Artificial Intelligence applications such as chatbots or automated callers that review individuals' travel histories in an attempt to identify and combat disease hotspots.[43] Many companies require employees to submit a "travel verification report" upon return to work. Telecom providers formulate these reports which contain all the locations that an individual has traveled to for the past 14 days, as well as provide a recommended quarantine period based on the travel history.

Although skepticism surrounds the COVID-19 infection and death statistics that China has reported, independent reports suggest that many of their measures are effective. An investigation published in *Science* explores China's transmission control measures during the early stages of the outbreak in China suggests that the nation's policies at least somewhat delayed the growth of the epidemic and reduced the number of cases.[44] The investigation quantifies that without the national response and Wuhan travel ban, there would have been

744,000 confirmed cases in China by the February 19th, 2020; in the presence of these measures, there were only 29,839 confirmed cases reported as of February 2020, which is 96% fewer than there would have been without interventions.[45]

China's technology-assisted system of contact tracing has also had success in limiting the spread. A retrospective cohort study conducted by Qifang Bi of John Hopkins University, Yongsheng Wu of the Shenzhen Department of Public Health Information, Shujiang Mei of the Shenzhen Department of Communicable Diseases Control and Prevention, and Chenfei Ye of Harbin Institute of Technology at Shenzhen sampled 391 Chinese COVID-19 patients and their 1,286 close contacts to investigate the efficacy of contact tracing control measures.[46] The study found that, of the 379 confirmed cases who had a known mode of detection, 77% were detected via "symptom-based surveillance."[47] The study also found that contact tracing enabled quicker detection of COVID-19 cases. While COVID-19 takes on average 4.9 days to detect with symptom-based surveillance, contact tracing reduced the time to 2.7 days.[48] Overall, the authors of the study said that they believe their research provides evidence that contact tracing is an effective measure.

Despite the claimed successes of China's COVID-19 response, many concerns about the government's policies have emerged. For example, Alipay's Health Code does not have a transparent system for deciding who is allowed in public spaces and who is designated to quarantine.[49] Individuals have expressed frustrations about the lack of provided rationale for their rating; the app, which updates your contagion risk status in real-time, can change your status from green to red and any point and stay that way for an unspecified amount of time.[50] In addition, breaches of confidentiality have occurred in regard to the identity of infected persons. For example, a Chinese telecom company, Chinese Mobile, recently sent texts to media outlets with infected individuals' detailed travel history.[51] This is clearly a violation of the individuals' privacy rights, and merits apprehension.

Furthermore, the Alipay's Health Code appears to share information with the police, which has raised concerns about it being a "new form of automated social control."[52] A *New York Times* analysis of the software code found that "as soon as a user grants the software access to personal data, a piece of the program labeled 'reportInfoAndLocationToPolice' sends the person's location, city name and an identifying code number to a server."[53] Additionally the analysis discovered that every time a person scans their code (an occurrence that happens numerous times as one travels about their city), their location is uploaded to the system's servers, enabling authorities to in essence track individuals locations. The analysis concludes that "The sharing of personal data with the authorities further erodes the thin line separating China's tech titans from the Communist Party government."[54] An additional fear is that these measures are not temporary or limited to the time of COVID-19, but rather that they are a calculated and permanent addition to China's already advanced state surveillance system.

**South Korea:**

During the worst of the COVID-19 outbreak, South Korea relied heavily on a combination of high-tech solutions and widespread testing. Working in tandem with private sector partners, the South Korean government built numerous high-capacity screening clinics. At the height of the outbreak, there were around 600 testing sites that completed up to 20,000 tests per day.[55] This non-technological aspect of their response has garnered praise from the international community for its facilitation of timely testing.

South Korea also utilized GPS tracking and IT solutions to trace the spread of the disease. One GPS location-based tracking app, Corona 100m, is downloaded on a volunteer basis. The app has been reported to be wildly popular and was downloaded one million times within just 17 days of its launch in February 2020.[56] The app uses data provided by telecommunication companies and notifies users who are near (within 100 meters) to any location that an infected person has frequented.[57] There are a variety of websites that are publicly available that track and show infection hotspots.[58] One such website is Coronamap, which illustrates the travel histories of individuals who have been confirmed as COVID-19 carriers.[59]

Additionally, South Korea has developed a mandatory app that uses GPS to track infected patients in quarantine and set off an alarm if they venture outside.[60] Anyone who may have come into contact with these confirmed carriers is also put under mandatory quarantine; to enforce this the South Korean government has developed a "geo-fencing" system that relies on calls, home visits, and the voluntary use of a government quarantine app.[61] Mobile testing teams from agencies such as the Ministry of Health and Welfare (MOHW) and Korea Centers for Disease Control and Prevention (KCDC) use location data, immigration records, CCTV footage, credit and debit card transactions, transit pass records, personal identification information, and prescription/medical records to track infected and potentially infected individuals.[62] This collection is extensive, and has the potential to deeply infringe upon citizens' privacy rights.

South Korea promptly mitigated the spread of COVID-19 without taking severe measures such as closing many businesses or issuing widespread stay-at-home orders.[63] In April, mere months after original concerns about the epidemic in South Korea emerged, there had only been 10,708 cases with 240 deaths.[64] Since mid-March, there have only been "a handful of new cases per day."[65] An article written by Sangchul Park of the University of Chicago, Gina Jeehyun Choi of the Korea Law Center, and Haksoo Ko of Seoul National University claims that South Koreans' use of advanced information technology systems deserves credit for flattening the curve of new COVID-19 cases and deaths.[66]

Nevertheless, South Korea's use of technology has major privacy implications for its citizens. Though the availability of data may be useful for tracing efforts, it also enables problematic trends such as identifying COVID-19 carriers publicly.[67] The collected and shared data includes information such as infection paths, hospitals of infected persons, the health of individuals who have had contact with infected persons, sex, nationality, and age (though names are not revealed).[68] This level of detailed data makes it easy to identify and publicize the identity of infected individuals. This identification has led to profiling, unveiling of embarrassing personal details, public disdain, and loss of business for infected owners of restaurants, shops, and other businesses.[69] Despite these negative impacts, the South Korean citizens do not necessarily disapprove of their government's actions. In an unpublished survey of South Koreans conducted by Youngkee Ju of Hollym University and Myoungsoon You of Seoul National University between the months of February and April 2020, the majority of respondents (68.2% ) said that they would be willing to sacrifice their individual privacy rights in order to continue information-sharing practices with their government.[70] This willingness likely stems from cultural factors; South Koreans are accustomed to sharing personal data with their government because it was a common practice in their nation even before the spread of COVID-19.[71]

Importantly, in the aforementioned article written by Park, Choi, and Ko, the authors claim that the level of public data sharing in South Korea is unnecessary for effective COVID-19 tracking and containment efforts.[72] While acknowledging the importance of tracing the location and movement of infected individuals for epidemiologic purposes, these authors contend that

rather than revealing personal information to the public, it could be used to inform officials where to focus public health measures. The authors also suggest that the sharing of less precise location data could help to preserve the privacy of infected individuals.

**Singapore:**

Singapore has also relied heavily on technology during the spread of COVID-19, and has found moderate success. One critical aspect of their approach is the government-developed TraceTogether app. This app utilizes Bluetooth technology in order to track the proximity of users' phones to each other. If any individual is later diagnosed with COVID-19, the owners of phones that have been in proximity to the infected user's phone can be notified to quarantine. While the Singaporean government claims that health officials "ask" to view and release the data from their phones, failing to assist the Ministry of Health to track movement is actually a crime in Singapore. The data taken from the phones are only stored for 21 days. Singapore has also enacted surveillance measures for infected patients. These measures consist of daily phone check-ins, randomized SMS messages including links to check location, and the requirement that infected patients send images of their surroundings to verify that they are in quarantine.[73] Those who do not comply can face detainment, isolation, and be forced to be tracked with RFID technology.[74]

The TraceTogether app is unique in that it is voluntarily downloaded by users. This aspect of the app originally hindered its efficacy; as of April, only 16% of the population downloaded TraceTogether.[75] Nevertheless, as the severity of the virus and knowledge of its spread increases, so did citizens' willingness to utilize the app. Currently, the app has 2.3 million users[76]; for context, the country had a population of 5.7 million as of June 2019.[77] The app's efficacy aside, Singapore has generally done well during COVID-19 despite its close proximity to and involvement with China. The COVID-19 infection spread in Singapore is one of the slowest in the world, and the COVID-19 death rate is also very low.[78] Overall, Singapore has successfully managed the virus.

Many privacy concerns have emerged regarding the TraceTogether app. While it succeeds in protecting the identity of users from each other, it does not afford the same protections from the government. Any diagnosed individual must give the list of locations they have visited (compiled in the TraceTogether app) to the Ministry of Health. The Ministry in turn collects the cell phone numbers that the infected individuals' phone has come into contact with.[79] While there is no indication that this information is being abused, its collection is nonetheless concerning because the identity of infected individuals and those they have physically come into contact with is not protected from the government in any way. Furthermore, the government's creation of a database that contains location information connected to individuals numbers presents the possibility of the government tracking the locations of its individuals.[80] Though there is no evidence that the Singapore government is doing so, its capability to do so remains alarming.

**European Union:**

Although countries in the EU by no means acted uniformly in their responses to COVID-19, there are certainly observable trends. For example, a report published by the Hague Center for Strategic Studies identifies two prominent trends of technologically-assisted responses that were implemented throughout the European Union.[81] The first trend consisted of enacting anonymized phone location tracking. Utilizing connections to cellular businesses, the

governments of Belgium, Austria, Estonia, France, Germany, Latvia, Greece, Portugal, Italy, and Spain utilized data provided from companies such as Orange S.A., Tele2, A1, Deutsche Telekom, Vodafone, and LMT to track individuals' movements and the spread of the virus.[82] In total, at least 13 countries in the EU have confirmed access to their citizens' anonymized location data.[83] The uses of this data varies, and includes aiding with insight on movement trends and checking compliance with lockdown orders. The second observed trend was the widespread government implementation of contact tracing apps. Germany, the Netherlands, Austria, Spain, Ireland, and Croatia all have contact tracing apps and projects in use or development.[84]

Notably, countries within the European Union are cooperating to find solutions. For example, Germany is spearheading collaborations with the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project.[85] A concerned group of scientists and technologists from more than eight European nations have taken on this project in the hopes of proposing solutions that are both effective and conscious of privacy issues. The EU has supported such efforts and recommends the implementation of a coordinated approach towards mobile tracing applications.[86] This aligns with the EU's stance that requires member states to share the information that they collect regarding contact-tracing with other nations in the EU via the electronic Early Warning and Response System.[87] This information includes personal and health data such as health status and travel history of infected individuals.[88]

Countries utilizing anonymized phone location data have seen moderate successes. These successes include insight into population movement and trends during the pandemic. For example, the telecom company Orange (in partnership with the French Government), had sufficient information to find that 17% of Parisians moved away from the French capital.[89] Additionally, countries have used collected information to shape their policy decisions. In Italy, the government used telecom reports to inform their decision to bolster lockdown measures after finding that their citizens were still moving about.[90] Furthermore in Latvia, the telecom company LMT has asserted that the data they share could be used to inform law enforcement of large, illegal gatherings.[91] It is clear that countries in the EU are not merely collecting anonymized phone location data, but instead analyzing it to make informed decisions for effective public health measures.

Contract tracing in the EU has faced some setbacks that limit efficacy. First, there is the universal problem with the contact tracing: it relies on high-risk groups such as children and senior citizens to have sufficient technology and knowledge of its use.[92] In addition, academics have warned that apps can lead to a false sense of security which can cause individuals to forgo compliance with other measures.[93] This problem is compounded by issues with the actual reliability and accuracy of contact tracing apps. While widespread contact tracing certainly has its merits, it seems unwise to solely rely on it to curb the spread of the virus.

Concern for privacy rights in the EU is certainly present in the time of COVID-19. While a survey of individuals in the EU residents found that 83% of respondents approved of fining those who violate quarantine, banning of public gatherings, and closing borders, 23% of respondents disapproved of using mobile phone data for tracking purposes.[94] In fact, the survey found that the issue that was most polarizing among respondents was governments' use of cellphone data for COVID-19 tracking.[95] The EU has some of the world's strongest digital privacy protections, which were bolstered in 2018 by the implementation of the General Data Protection Regulation. As a result, governments and telecom companies have taken steps to put privacy-related fears to rest. For example, telecom providers work to anonymize and aggregate data before it is shared. Specifically, when aggregating data the companies use groups of at least

30 users to prevent identification of individuals from their data.[96] This anonymization is legally necessary for countries hoping to share their data with other nations in the EU without the consent of users.[97] Sharing data across the EU has faced vocal criticism; Hannah van Kolfschooten and Anniek de Ruijter of Amsterdam Law School argue that in mandating data sharing, the "European Commission has implicitly decided that the protection of public health outweighs the importance of the right to privacy in case of serious cross border threats to health."[98] The plethora of concerns and criticisms by citizens and academics in the EU give evidence that further privacy considerations for COVID-19 measures are necessary.

**United States:**

The United States' approach to combating COVID-19 consists of a very decentralized system of response. The federal government took actions such as suspending travel from China in February and from 26 European countries in March. Furthermore, institutions such as the CDC and many US embassies made statements discouraging non-essential travel. While travel certainly decreased within the United States, it remains unclear whether this was a result of these warnings or other factors. The individual states within the nation largely made their own unique policies and responses during the pandemic. As of August 2020, there is no centralized or widespread method of contact tracing in the United States. The development of contact tracing measures has largely been left up to states rather than the federal government. This has led to a lag in tracing, leaving the US far behind its international peers. While states such as California, Washington, and Massachusetts have invested significant resources in hopes of developing large-scale contact tracing measures, many other states have implemented little in the way of contact tracing.[99]

The United States' infection and mortality rates reflect the efficacy of the nations' response to COVID-19. In August 2020, at least 5,140,300 Americans were infected and at least 164,000 had died.[100] In addition, the United States leads the world in both cases and deaths. Some experts, such as Adriane Casalotti, chief of government and public affairs at the National Association of County and City Health, blame the concerning rates of infection and spread on insufficient contact tracing measures.[101] It is clear that the United States' public health measures during COVID-19 are largely insufficient and ineffective.

The failure to enact comprehensive public health measures coincides with the prioritization and protection of privacy in the United States. Culturally, this can be contextualized with the general emphasis on individual freedoms and rights within the nation. Victor Cha of the Center for Strategic and International Studies explains that, "For countries in the West still suffering from the virus, political leaders struggle over the tradeoff between privacy rights and the use of smartphone app-tracking technology for contact tracing."[102] Interestingly, while the American people tend to be adamantly opposed to government infringement upon their privacy, they allow big tech to access and collect enormous amounts of their data. This raises fundamental questions about how privacy is conceptualized by the American people.

Furthermore, recent issues with data privacy in America have led policymakers to be cautious about technological strategies. Although the White House did meet with the leaders of big tech during COVID-19, conversations surrounding mobile tracing and location technologies were reportedly avoided.[103] Another factor that may influence American's aversion to more intrusive public health measures is the nation's experience (or lack thereof) with SARS, MERS, and Ebola. The United States faces a mere 27 cases of SARS, 2 cases of MERS, and 11 cases of

Ebola. While nations that were more affected by these diseases put in place precautionary public health measures, the United States remained unprepared for a pandemic such as COVID-19.[104]

**Israel:**

The Israeli government has taken one of the most extreme approaches to curtailing the spread of COVID-19. At first, the government worked to stop flights into the country, create social distancing guidelines, close schools, and impose curfews.[105] To add to these measures, the Israeli Health Ministry has created a voluntary app, entitled "HaMagen," which uses cellular location data over 14 days to check for contact with infected individuals.[106] Additionally, the Israeli government has relied on Shin Bet, Israel's internal security service, to help with tracing and identifying COVID-19 carriers using cell phone location data.[107] In order to do this, the Health Ministry is required to share the names, ID numbers, and cell phone numbers of infected individuals. Shin Bet then uses a classified database dubbed "the Tool" to retrieve cell phone data from cellular providers which enables them to identify anyone who has been within two feet of an infected individual for more than 15 minutes.[108] Once the information is collected, Shin Bet notifies the Health Ministry, which in turn attempts to reach potentially infected contacts and instruct them to quarantine. There have also been reports that Shin Bet has used the collected information to inform police on defiance of quarantine orders.[109]

The data collected by Shin Bet is incredibly detailed, and includes information on location, voice calls and text messages (their occurrence but not their content), and website visitation.[110] The intrusive nature of these measures has caused concern about the privacy and rights of Israeli citizens. As a result, the measures have faced challenges in the courts. In late April, the Supreme Court of Israel ruled that "explicit statutory authority" rather than executive authorization was necessary to continue the program in the case Ben Meir v. Prime Minister.[111] Despite this challenge, the program will seemingly prevail as recent legislation has passed that authorizes Shin Bet to extend the practice of its measures for at least another six months.[112]

Although Israel initially had success in preventing the spread of COVID-19, rising infection and mortality rates in July and August have set back the nations' progress. In the early days of the pandemic, Israel's public health measures caused the rates of infection to plummet to 10-20 new cases per day.[113] To the world, it appeared that Israel was making all the right moves.[114] Unfortunately, in late June and early July, the number of cases began to rise again. Citizens are blaming the increase in infections on the government's reopening of schools and permitting large gatherings such as weddings.[115] On July 15th, Israel reported 42,813 cases and 375 deaths.[116] Furthermore, on July 21st, Israel faced over 1,500 new coronavirus cases daily.[117] This infection rate is more than twice as high as it was during March and April.[118] The initial successes of Israel have given way to a concerning second wave as restrictions were hastily and prematurely loosened.

Taking one of the most intrusive approaches to disease control, Israel has significantly infringed on its citizens' privacy rights. In utilizing its domestic security service for implementation of COVID-19 measures, Israel has made clear that this problem, as well as most others the nation faces, is one of national security.[119] As such, Israel has created an opportunity for its national surveillance to extend to areas besides public health.[120] The Israeli government justifies these measures with a host of explanations: contact-tracing is ineffective as individuals' memories are fallible, the large Orthodox community does not own cell phones, and the impossibility of otherwise tracing the contact of individuals in crowded places.[121] Despite these rationales, it still appears that unnecessarily invasive and stringent measures are being put into

place. For example, there is no form of appeal for those who may be incorrectly classified as a potential contact.[122] Furthermore, Israel's aforementioned use of "the Tool" operates with no judicial oversight. Its use is generally classified and the contents, storage length, and protection of collected data are largely unknown.[123] Israel's approach to COVID-19 - shrouded in secrecy and heavily reliant on intrusive surveillance - certainly poses threats to the long-term privacy rights of its citizens.

**Taiwan:**

Taiwan, known for its technological prowess, has predictably relied heavily on data collection and technology for its COVID-19 mitigations efforts. One of the main control measures being employed is the border quarantine: those who return to Taiwan must either quarantine in a hotel or return to their own residences and undergo intense digital surveillance for a 14-day period.[124] The surveillance measures include digital fencing, which consists of using an electronic fence or perimeter, enabled by cell tower triangulation from telecom providers, that sets a boundary that a quarantined individual must stay within.[125] In order to ensure that individuals do not simply leave their phones at home and travel as they wish, officials video call multiple times a day to check in and failure to answer one of these check ins results in heavy fines. Furthermore if a quarantined individual's cellular device runs out of battery or is turned off, the police will report to their house.[126] During the 14-day mandatory quarantine, each individual received a $33 per day stipend. If at any time an individual breaks the quarantine, they are forced to pay back one thousand times the stipend received.[127]

Taiwan also employed a variety of datasets to supplement its surveillance efforts. For example, the National Health Insurance database has been merged with the immigrations and customs dataset in order to ensure individuals had undergone health screenings and disclosed their travel history.[128] In addition, Taiwan has implemented forms of contact tracing. The first 100 confirmed COVID-19 cases were all extensively tracked.[129] An outbreak investigation team, led by the Taiwan CDC, thoroughly investigates cases and possible contacts.[130] It is important to note that since Taiwan has seen relatively few cases (numbering less than 1,000), contact tracing may be a less important measure than in other nations where the spread is far more prevalent.

Taiwan's response has generally been very effective and has helped curtail both the spread of COVID-19 and the resulting deaths in the nation. As of August 17, 2020, the nation had only 500 cases and a mere seven deaths.[131] Taiwan's successes come even in the face of significant challenges such as proximity to mainland China and frequent travel between the two neighbors.[132] The technological aspects of Taiwan's response have been credited for these strikingly low statistics.[133] Technology plays an important role in shaping Taiwan's culture and identity. As a result, citizens have enthusiastically engaged in both the use and production of virus-mitigation technologies. Jaron Lanier and E. Glen Weyl of Microsoft explain that "bottom-up information sharing, public-private partnerships, 'hacktivism' (activism through the building of quick-and-dirty but effective proofs of concept for online public services), and participatory collective action have been central to the country's success in coordinating a consensual and transparent set of responses to the coronavirus."[134]

Though some of Taiwan's measures such as digital fencing may seem invasive, the general widespread trust in the government and transparency of officials' actions have helped to ease fears of privacy intrusion. Examples of government officials' transparency include daily briefings from political leaders and scientific experts as well as the broadcasting of all of Digital Minister Tang's meetings.[135] This communication has helped maintain citizens' confidence

despite the curtailment of privacy rights.[136] The Taiwan Public Opinion Foundation conducted a survey of 1079 Taiwanese citizens in order to assess their opinions of their government's actions. 80% of those surveyed approved of the Minister of Health and Welfare's handling of COVID-19 and 70% approved of the president and the premier's work.[137] The government's empowerment of previously mentioned "hacktivists" likely has to do with these high approval ratings. By allowing citizens to shape and produce the very measures they are subject to, the Taiwanese government has created a form of '"participatory self-surveillance."[138] One example of this is Taiwanese citizens who, in collaboration with their government, created an online tool that aggregated data on the availability and location of face masks. As Andreas Kluth of Bloomberg explains, "by involving people in the solutions, rather than just dictating policies to them, the process is transparent and inspires trust, even civic pride."[139] It seems as though Taiwan has managed to create measures that approach the nearly elusive balance between privacy and public health.

**Country Comparison:**

The diverse array of public health measures implemented by different nations enable meaningful and informative comparisons. The failures of both the intensely invasive approaches of countries like Israel and China, and the astonishingly weak effort by the U.S. reveal the dangers of living on either extreme of the privacy spectrum. The experiences of the countries in between these extremes provide guidance for future policymakers.

China's extreme secrecy enabled the virus to spread far beyond its borders; although this failure may not have had domestic health implications, it should certainly be considered when measuring the success of the nations' measures. Israel's measures have also proven to be somewhat unsuccessful; the nation's burgeoning second wave undermines the government's claims that stringent surveillance is the best response to COVID-19.

On the other side of the spectrum, the United States' approach has been an arguably worse catastrophe. The United States, ever concerned with the protection of individual liberties, has struggled to create effective measures that can coexist with the utmost protection of rights. The unwillingness of Americans to sacrifice even limited rights for the larger societal good has led to unthinkable rates of infection and mortality. In addition, the Trump administration's sluggish and insufficient attempts to address the disease played a large role in the nation's ultimate failure. Lacking an efficient federal strategy, the United States has failed to use any widespread data collection or contact tracing measures to curtail the spread. Though Americans are averse to rights infringements, the absence of any meaningful attempts to track the spread with contact tracing measures makes it hard to discern whether the problem lies with American cultural norms or with the Trump administration itself. What is clear, however, is that both overreaction and inaction are problematic as governments grapple with COVID-19.

Although South Korea has low infection and mortality rates, the nation has by no means found a tenable balance between privacy and public health. Its health successes are tainted by the unnecessary disclosure of personal information that has enabled reidentification and ostracization. While South Korea has developed solid tracing and prevention infrastructure, it needs to do far better in the protection of privacy to be considered a true success story.

Nations in the EU are struggling to find a unified approach, which is reflected in the infection and mortality rates. As of August, a second wave of COVID-19 threatens most of Europe.[140] This has led to the shuttering of borders and increase in testing throughout the EU. Still, the EU deserves recognition for mitigating the first wave after a devastating March and

April in Italy. Furthermore, there are valiant attempts at considering privacy throughout the EU. The coalition entitled Pan-European Privacy Preserving Proximity Tracing has worked to provide suggestions for "privacy-friendly contact tracing apps."[141] While the EU has not been ultimately successful in battling COVID-19, it is at least attempting a balance between privacy and public health.

Singapore and Taiwan have found the most success in the balancing of priorities. Singapore's TraceTogether app, while initially facing challenges with voluntary adoption, has now grown into a global success story. TraceTogether is effective in tracking the movement of the virus while also protecting privacy with limited 21-day data storage and protection of users' identities from fellow users. The Hague Centre for Strategic Studies labeled TraceTogether's use of Bluetooth technology as the "least intrusive" option among mobile tracing applications.[142] Singapore's approach appears to be moderately effective as well, with the country boasting very low mortality rates. In addition, Taiwan's measures have had wild success rates. With only 7 reported deaths in a population of nearly 24 million citizens, it is clear that the Taiwanese government is utilizing the country's technology savvy to its benefit. Furthermore, Taiwan's transparency and inclusion of its citizens in developing public health measures has helped mitigate fears of privacy infringement. Taiwan's triumph proves that governments can indeed use technology to fight COVID-19 without foregoing the protection of privacy rights.

**Section V: Factors that Influence Response Type - A Case Study of China and the United Kingdom**

While it is important to consider how nations differ in their responses, it is also vital to consider why they have chosen distinct approaches. Factors such as regime type, leadership, national pandemic history, and privacy norms play an important role in shaping a nation's response. The importance of these factors emerges clearly when comparing the starkly divergent responses of two very different countries: China and the United Kingdom. China's regime type, which has become increasingly totalitarian, empowers it to forcefully enact strict shutdowns and contact tracing measures while simultaneously stymying the necessary flow of information via state censorship. China's leader, Xi Jinping has played an important role in charting China's response, as he has utilized his strongman rule to create and enforce effective public health measures. The United Kingdom, on the other hand, has struggled to control the virus for almost its entire duration, and is currently in the midst of a devastating second wave. This can partly be attributed to the United Kingdom's regime type, parliamentary democracy, which constrains the country from enacting intense surveillance methods as in China, and requires the government to respond to the demands of the general population. Furthermore, Boris Johnson's populist leadership and disconnect with science has led the nation to greatly suffer.

China's powerful centralized government allows it to implement highly invasive policies that would not be permitted in democracies because of their intrusiveness. For example, the aforementioned Chinese app "Health Code" tracks the movements of users and controls their quarantine status to an extreme degree by dictating if a person can access public spaces. While Democratic countries such as Taiwan and South Korea have also implemented COVID-19 tracing efforts, those governments' responses have been far more transparent and much less intrusive than China's efforts.[143] As discussed in the previous section, in Taiwan location-based tracking is generally confined to those who have recently entered the country. In South Korea, the download of the most popular contact tracing app, Corona 100m, is done on an entirely volunteer basis.[144] In contrast to these responses, China's app is, in essence, mandatory for all

individuals wishing to function in society, and its implementation has been overwhelmingly non-transparent. The government's opacity is evident in its decision to secretly embed the Health Code application feature that sends the collected location information directly to the police.[145] While democratic countries can certainly implement tracing efforts, the scope of their invasiveness is generally limited by citizen pushback and partisan politicking. Totalitarian regimes, on the other hand, may infringe upon citizens' privacy with greater ease as they blur the line between state and society.

Although the increasingly totalitarian regime in China allows for invasive but effective public health measures to be implemented, their style of centralized government has also faced difficulties in mitigating the harms of the pandemic. The government aims to have a high degree of control over the flow of information, frequently engaging in state censorship. This can backfire, however, as critical intelligence can be muffled in the effort to constrain communications. The failure of information to flow both up to policymakers in the Politburo and down to citizens on the street could be a possible explanation for China's delayed response. If the Chinese government was unaware of the extent of the virus due to censorship, it may have been unable to adequately and promptly address the situation and quickly develop public health measures. While one cannot know for certain the extent and timeline of the government's knowledge of COVID-19, another issue that almost certainly impacted the Chinese response was the population's lack of information about the virus early on. When doctor Li Wenliang spoke out about the virus, he was interrogated and silenced by the government, and eventually perished from COVID-19.[146] Because the government attempted to control COVID-19 information during the early days of the pandemic, citizens were unable to take necessary precautionary measures or adequately protect themselves from the disease. China's inability to quickly address the pandemic due to issues with information flow had serious implications; A simulation done by researchers at the University of Southampton concluded that had China implemented its control measures a mere week earlier, it could have prevented 67% of its cases.[147]

China's leadership is another critical factor in the country's response. President Xi Jinping has centralized power under himself and become a personalistic strongman. President Xi's willingness to employ "draconian" and "repressive" means, such as swiftly quarantining the 11 million people of Wuhan, are a result of his strongman rule.[148] Insulated from particularist pressures and firmly in control of internal security, the military, the police, the National Security Commission, and the People's Liberation Army (PLA), President Xi has been able to implement policies that a less secure political figure likely could not. President Xi has been active in purging political rivals and those who speak out against him.[149] This massive consolidation of power allowed President Xi to not only have the capability to impose China's extensive response, but also the political capital to do so. President Xi's COVID-19 approach would be risky for a politician that is highly prone to the whims of the people or vulnerable to criticisms from rivals. The shutdowns so necessary for combating the spread of COVID-19 can certainly cause harm to the economy, which in the short term can be very unpopular with the masses. Yet President Xi was able to pursue such a policy without fear of immediate backlash. While President Xi's strongman rule may not permanently overpower dissent, in the short term it has enabled him to enact necessary but potentially unpopular COVID-19 measures. The success of those measures has now bolstered the popularity of President Xi and further cemented his strongman rule.

Another factor to consider when analyzing China's response is the country's history with confronting pandemics. The Chinese experience with SARS and the resulting "Regulations on

Preparedness for the Response to Emergent Public Health Hazards" afforded China some preparation for the pandemic. While other countries struggled to consult experts and rapidly develop a plan during the first wave of COVID-19, China was able to utilize its existing policy infrastructure to address the crisis. Furthermore, Chinese citizens, scarred by the toll of SARS, were willing to make sacrifices in the name of public health. Citizens in nations that were less affected by SARS, such as the United Kingdom, have demonstrated less willingness to make sacrifices such as quarantining and wearing masks for the broader good of public health. China's SARS experience has thus worked to increase compliance of the citizenry with public health measures and overall improved COVID-19 outcomes in China.

The United Kingdom has been far less successful in managing the spread of COVID-19, and has the second-highest coronavirus death toll of the world's wealthiest nations.[150] The United Kingdom, like China, had a slow start to its pandemic response. Early on, Prime Minister Boris Johnson chose to promote the idea of "herd immunity," which entailed letting the virus naturally spread so that a large portion of the population eventually becomes immune.[151] However, in late March, the Prime Minister reversed course and implemented a three-month lockdown. Despite this lockdown effort in the Spring, the United Kingdom has suffered from a second spike. Although the United Kingdom has been credited with increasing the country's testing capacity, the failure of the government to use the collected data or adequately implement robust contact tracing has limited the testing's efficacy. Though the United Kingdom has made steps to combat the spread of the virus, they have thus far been much less effective than the Chinese measures.

The parliamentary democracy within the United Kingdom certainly impacted how the government chose to respond. In a democracy where political officials are held accountable to the people, the government is inherently responsive to the demands of its citizens. As a result, citizens' discontent about the prolonged lockdown and economic harms of COVID-19 public health measures may have stymied the government's ability to create a more robust response that would require greater citizen sacrifice. The government in the United Kingdom faced severe political pressure to ease the COVID-19 restrictions because they were thought to suppress the economy and limit citizen's freedoms.[152] While politicians being held accountable to the citizenry is one of the marked strengths of democracy, in times of crisis where unpopular sacrifice is necessary, some democratic regimes may flounder.

The leader of the United Kingdom, Prime Minister Boris Johnson, played a large role in shaping the country's COVID-19 response. The Prime Minister has faced great criticism for his promotion of "herd immunity," and was mocked after he became infected with COVID-19 himself. Many have blamed the Prime Minister's failed response on his populist leadership style. Populist leaders across the globe, such as President Donald Trump in America and President Jair Bolsonaro in Brazil, preside over the countries that have been some of the worst affected by COVID-19.[153] One reason that populist leaders may falter in the face of the pandemic is that populism, by nature, often leads to the disparagement of expert knowledge and the propagation of anti-elite and anti-scientific attitudes.[154] The anti-establishment element of populism presents a threat during COVID-19, where reliance and collaboration with established health experts and organizations is imperative.

In Britain, the disconnect between the scientific community and the populist Prime Minister has become painfully clear. Sir Patrick Vallance, chosen by Prime Minister Boris Johnson to be his chief scientific adviser, has rejected the scientific community's known aversion to "herd immunity" and chose to promote it. Sir Patrick Vallance publicly announced that "herd immunity" would require 40 million Britons to catch the disease, but failed to mention that an

estimated 250,000 would perish.[155] Furthermore, a group of senior British scientific advisers, who are members of the Scientific Advisory Group on Emergencies (SAGE), have found their advice blatantly ignored by Prime Minister Boris Johnson. Although SAGE recommended that the Prime Minister impose a myriad of restrictions, including banning contact within the home and closing all bars, restaurants, and indoor gyms in early September, the Prime Minister opted only to advise individuals to work from home if possible.[156] The divide between the scientific community and populist Prime Minister Johnson may account for the country's dismal COVID-19 response.

In addition, norms surrounding the protection of an individual's rights may have led to bureaucratic delays as a product of privacy concerns. One reason that England's contact tracing program, Test and Trace, has had limited success is because it is highly bureaucratic in its efforts to protect patient confidentiality.[157] For example, if a known contact resides in the same house as an infected individual, their personal information cannot be collected by contact tracers who conduct home visits. Instead, the contacts must wait days until the tracers reach out to them. This slows the process of contact tracing and hampers the government's efforts to alert potentially infected individuals. A study conducted by Reuter's found that in England, the Test and Trace program has only been able to trace one non-household contact for every two confirmed cases of COVID-19.[158] To put that in perspective, the Singaporean government can trace, on average, twenty contacts for every confirmed case of COVID-19.

In China, citizens have become accustomed to government surveillance and privacy intrusions. As a result, the government could successfully implement its Health Code tracing app, which instantly notifies an individual if one of their contacts has tested positive. Such an app would likely never be allowed in the United Kingdom, where the Information Commissioner's Office is tasked with protecting data privacy for all individuals.[159] The stark difference in China's successful Health Code and the United Kingdom's lackluster Test and Trace can be largely attributed to the privacy norms. While the Chinese government has little transparency in how the Health Code application functions, what data is being collected by the app, and who has access to the data, the United Kingdom is forced to enact heavily bureaucratic and inefficient systems in order to ensure that the identity of persons infected with COVID-19 are protected. The privacy norms that exist in different countries therefore greatly affect the nature and efficacy of response measures.

China, currently boasting staggeringly low rates of daily cases, has emerged as a winner of the COVID-19 pandemic.[160] It's response has been lauded for its efficacy, even as the nation suffered setbacks at the beginning of the crisis. While the officially reported numbers may seem suspect to some, as the Chinese government is known for its use of propaganda and information manipulation, China's response has been generally thought of as a success.[161] The United Kingdom, on the other hand, has struggled for almost the entire duration of the pandemic. The country has failed to get a strong grasp on the spread of the virus, despite the delayed yet lengthy shutdowns in the spring. The disparities in the countries' responses can be attributed to innumerable factors, yet some emerge more clearly than others. First, regime type is of the utmost importance; while in China, the increasingly totalitarian regime has been able implement necessarily stringent public health measures, the democratic British government has struggled to enact efficacious but unpopular policies. Individual leaders have also influenced the path of the pandemic. President Xi has used his strongman rule to implement drastic yet effective measures, while populist Prime Minister Boris Johnson has distanced himself from science with devastating consequences. Other factors such as national pandemic history and privacy norms have impacted

countries' response efforts as well. Juxtaposing the vastly different responses of China and the United Kingdom may allow other countries and leaders to see where their peers have succeeded and failed, and to shape their own responses accordingly.

## Section VI: Policy Suggestions

The use of technology is unavoidable when devising the most effective approach to COVID-19. As a result, privacy rights will inevitably be affected by the new and extensive public health measures. In order to minimize the privacy implications of responses while also maintaining their efficacy, a Bluetooth-based contact tracing app is advisable. Such an app would function similarly to Singapore's TraceTogether; individual's cellular devices can emit signals or "tokens" which are then used to record proximity to other nearby devices and individuals. If any individual is later diagnosed as a confirmed COVID-19 case, their contacts can be traced and notified. This approach protects the privacy of individuals' movements since it uses data on a person's proximity to other users rather than the location of the user themselves. Put simply, such an app could detect the *who* but not the *where* of an individual's contacts. This kind of tracking is actually preferable to GPS/location tracking in terms of its efficacy because it is generally more accurate and works in a multitude of otherwise difficult situations such as in indoor and underground settings or in crowded areas.[162] It is also more effective than contact tracing that relies solely on the memory that users have of their locations and contacts.

Another necessary aspect of such an app would be the veiling of individuals' identities. When users' devices come into contact and exchange "tokens", they should be immediately anonymized to protect all individual's identities from each other. Later, if a user is a confirmed carrier of COVID-19, anyone who received one of their "tokens" can be notified to quarantine. They will not, however, be notified of the identity of the individual that is the confirmed case. An app that utilizes Bluetooth is well-equipped to anonymize identities and protect the privacy of users because "the only information involved is contact tokens, which can be cryptographically secured in a way that is less vulnerable to de-anonymization than location histories."[163]

Beyond the design of a contact tracing app, more general guidelines can help shape privacy preserving practices. Marcello Ienca and Effy Vayena of the Swiss Federal Institute of Technology recommend three insightful data-management practices that help guide an interest-balancing approach.[164] First, the authors explain that the response should be proportional to the threat; a common cold would not merit the same data-collection efforts as COVID-19. Their second guideline relates to necessity. The least possible amount of data-collection should be utilized to achieve necessary efficacy. This guideline would likely address the approaches of both Israel and China, whose data collection has been far more extensive than what is likely absolutely necessary. The final guideline proposed by the authors addresses the need for scientific justification of proposed measures. This guideline could relate to South Korea's public disclosure of the identities of infected individuals in South Korea. The Organisation for Economic Co-operation and Development (OECD) has also provided valuable suggestions.[165] The OECD advises that the public remains knowledgeable of their government's COVID-19 policies and that the utmost transparency is employed when implementing new approaches. In addition, the OECD suggests that the duration of invasive COVID-19 technology use and data gathering be limited to what is absolutely necessary to avoid any measures becoming unnecessarily permanent. These guidelines can and should extend far beyond the development of tracing apps to all public health measures developed during COVID-19.

**Section VII: Conclusion**

Past pandemics and the recent experience with COVID-19 have revealed the importance of rapid and effective responses in order to mitigate the spread of dangerous illnesses. As seen in the case of China, a speedy response can spare tens of thousands of lives. One needs only to look at America's experience to see the unthinkable danger of a slow and ineffective approach to COVID-19. The virus is a stark reminder of the need to develop detailed, researched, and robust response plans in advance of, rather than in response to, future pandemics.

Nonetheless serious privacy implications can arise that can have pernicious effects on citizens. In the case of HIV/AIDS, privacy violations had grave consequences for infected individuals, and ultimately discouraged many from seeking vital care. Though COVID-19 may not carry the same stigma as HIV/AIDS, the protection of privacy is still fundamental, especially in countries that are implementing voluntary tracing and surveillance efforts. Unless people feel that their sensitive health and location data will be protected, they will be unlikely to participate in such voluntary programs, thus undermining the success of government efforts. The anonymization of data through Bluetooth-based tracing apps are a promising example of policy measures that ensure both privacy and efficacy.

Analyzing the disparate responses of countries with different governance systems, leadership styles, and attitudes toward privacy reveal possible causes of the varying successes and failures of nations faced with COVID-19. Centralized governments with strongman rulers are able to quickly enact stringent policy measures, though challenges are likely to arise due to the hindered flow of information. On the other hand, democratic governments may struggle to enact efficacious yet unpopular policies, but are more likely to respect the privacy of citizens. The cases of China and the United Kingdom provide important insight into what factors facilitate or impede the ability of nations to respond to pandemics in the future.

Though the balance between privacy and effective public health measures may be precarious, nations can and should strive to find equilibrium. History teaches that pandemics will never be a thing of the past; creating norms around the protection of privacy even in the midst of health crises is therefore imperative. By employing universal guidelines such as establishing transparency of government actions and ensuring reasonable scope and duration of implemented measures, nations and their citizens can limit the long-term disruptions that pandemics produce. In addition, optimizing the use of technology to both prevent the spread of a disease and protect the privacy of users enables rights protections to persist even in the modern world. Singapore's TraceTogether app is a perfect example of how technology can spur both effective public health measures and privacy protections. Nonetheless, more should be done to ensure the proportionality, necessity, and scientific justification of all implemented policies. As technology inevitably develops, so too should the privacy protections that surround it.

---

**Endnotes**

[1] Beaglehole, R., Irwin, A., & Prentice, T. (2003). *The World Health Report 2003*. The World Health Organization. https://www.who.int/whr/2003/en/whr03_en.pdf

[2] Schrag, S. J., Brooks, J. T., Van Beneden, C., Parashar, U. D., Griffin, P. M., Anderson, L. J., Bellini, W. J., Benson, R. F., Erdman, D. D., Klimov, A., Ksiazek, T. G., Peret, T. C. T., Talkington, D. F., Thacker, W. L., Tondella, M. L., Sampson, J. S., Hightower, A. W.,

Nordenberg, D. F., Plikaytis, B. D., … Chamberland, M. E. (2004). SARS Surveillance during Emergency Public Health Response, United States, March–July 2003. *Emerging Infectious Diseases*, *10*(2), 185–194. https://doi.org/10.3201/eid1002.030752

[3] Ibid

[4] Basrur, S. V., Yaffe, B., & Henry, B. (2004). SARS: A Local Public Health Perspective. *Canadian Journal of Public Health = Revue Canadienne de Santé Publique*, *95*(1), 22–24. https://doi.org/10.1007/BF03403628

[5] Ibid.

[6] Teo, P., Yeoh, B. S. A., & Ong, S. N. (2005). SARS in Singapore: Surveillance strategies in a globalising city. *Health Policy (Amsterdam, Netherlands)*, *72*(3), 279–291. https://doi.org/10.1016/j.healthpol.2004.11.004

[7] Bowen, J. T., & Laroe, C. (2006). Airline networks and the international diffusion of severe acute respiratory syndrome (SARS). *The Geographical Journal*, *172*(2), 130–144. https://doi.org/10.1111/j.1475-4959.2006.00196.x

[8] Chan, E., & Schloenhardt, A. (2004). The 2003 Sars Outbreak In Hong Kong: A Review Of Legislative And Border Control Measures. *Singapore Journal of Legal Studies*, 484–510. JSTOR. https://www.jstor.org/stable/24869491

[9] Jacobs, L. A. (2007). Rights and Quarantine during the SARS Global Health Crisis: Differentiated Legal Consciousness in Hong Kong, Shanghai, and Toronto. *Law & Society Review*, *41*(3), 511–551. JSTOR. https://www.jstor.org/stable/4623394

[10] Ibid.

[11]Anderson, T. (2013). HIV/AIDS in Cuba: A rights-based analysis. *Health and Human Rights Journal*. https://www.hhrjournal.org/2013/09/hivaids-in-cuba-a-rights-based-analysis/

[12] Ibid.

[13] Patrick, D. M., Rekart, M. L., Cook, D., Strathdee, S. A., Spencer, D., & Rees, A. D. (1999). Non-Nominal HIV Surveillance: Preserving Privacy While Tracking an Epidemic. *Canadian Journal of Public Health*, *90*(3), 164–167. https://doi.org/10.1007/BF03404499

[14] *Evaluation of HIV Case Surveillance Through the Use of Non-Name Unique Identifiers—Maryland and Texas*. (1994). Centers for Disease Control. https://www.cdc.gov/mmwr/preview/mmwrhtml/00050807.htm

[15] Patrick, D. M., Rekart, M. L., Cook, D., Strathdee, S. A., Spencer, D., & Rees, A. D. (1999). Non-Nominal HIV Surveillance: Preserving Privacy While Tracking an Epidemic. *Canadian Journal of Public Health*, *90*(3), 164–167. https://doi.org/10.1007/BF03404499

[16] *Evaluation of HIV Case Surveillance Through the Use of Non-Name Unique Identifiers—Maryland and Texas*. (1994). Centers for Disease Control. https://www.cdc.gov/mmwr/preview/mmwrhtml/00050807.htm

[17] Bayer, R., & Fairchild, A. (2002). The Limits of Privacy: Surveillance and the Control of Disease. *Health Care Analysis : HCA : Journal of Health Philosophy and Policy*, *10*, 19–35. https://doi.org/10.1023/A:1015698411824

[18] *Evaluation of HIV Case Surveillance Through the Use of Non-Name Unique Identifiers—Maryland and Texas*. (1994). Centers for Disease Control. https://www.cdc.gov/mmwr/preview/mmwrhtml/00050807.htm

[19] Bayer, R., & Fairchild, A. (2002). The Limits of Privacy: Surveillance and the Control of Disease. *Health Care Analysis : HCA : Journal of Health Philosophy and Policy*, *10*, 19–35. https://doi.org/10.1023/A:1015698411824

[20] Ibid.

[21] Fairchild, A. L., & Bayer, R. (2012). Unlinked Anonymous Testing for HIV in Developing Countries: A New Ethical Consensus. *Public Health Reports*, *127*(1), 115–118. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3234388/
[22] Ibid.
[23] Chen, L. C. (1987). The AIDS Pandemic: An Internationalist Approach to Disease Control. *Daedalus*, *116*(2), 181–195. JSTOR. https://www.jstor.org/stable/20025102
[24] Doughty, R. (1994). The Confidentiality of HIV-Related Information: Responding to the Resurgence of Aggressive Public Health Interventions in the AIDS Epidemic. *California Law Review*, *82*(1), 111–184. JSTOR. https://doi.org/10.2307/3480851
[25] Mydans, S. (1991, July 30). Names List Leads to Ethics Debate. *The New York Times*. https://www.nytimes.com/1991/07/30/us/names-list-leads-to-ethics-debate.html
[26] Doughty, R. (1994). The Confidentiality of HIV-Related Information: Responding to the Resurgence of Aggressive Public Health Interventions in the AIDS Epidemic. *California Law Review*, *82*(1), 111–184. JSTOR. https://doi.org/10.2307/3480851
[27] Ibid.
[28] Shereen, M. A., Khan, S., Kazmi, A., Bashir, N., & Siddique, R. (2020). COVID-19 infection: Origin, transmission, and characteristics of human coronaviruses. *Journal of Advanced Research*, *24*, 91–98. https://doi.org/10.1016/j.jare.2020.03.005
[29] Cho, H., Ippolito, D., & Yu, Y. W. (2020). *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs*. http://arxiv.org/abs/2003.11511
[30] Simko, L., Calo, R., Roesner, F., & Kohno, T. (2020). *COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences*. University of Washington. http://arxiv.org/abs/2005.06056
[31] Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine*, *26*(4), 463–464. https://doi.org/10.1038/s41591-020-0832-5
[32] Duri, J., Zúñiga, N., Granjo, A., Jenkins, M., Khaghaghordyan, A., Kukutschka, R., . . . Rougier, J. (2018). Getting Ahead Of The Curve: Exploring Post-Covid-19 Trends And Their Impact On Anti-Corruption, Governance And Development (pp. 9-11, Rep.) (Vrushi J. & Chêne M., Eds.). *Transparency International*. http://www.jstor.org/stable/resrep24924.5
[33] Simko et al., "COVID-19 Contact Tracing and Privacy."
[34] Ibid.
[35] Duri, J., Zúñiga, N., Granjo, A., Jenkins, M., Khaghaghordyan, A., Kukutschka, R., . . . Rougier, J. (2018). Getting Ahead Of The Curve: Exploring Post-Covid-19 Trends And Their Impact On Anti-Corruption, Governance And Development (pp. 9-11, Rep.) (Vrushi J. & Chêne M., Eds.). *Transparency International*. http://www.jstor.org/stable/resrep24924.5
[36] Van de Pas, R. (2020). *Globalization Paradox and the Coronavirus pandemic* (Clingendael Report). Netherlands Institute of International Relations. https://www.clingendael.org/publication/globalization-paradox-and-coronavirus-pandemic
[37] Swaine, M. D. (2012). *America's Challenge: Engaging a Rising China in the Twenty-First Century*. Brookings Institution Press. https://muse.jhu.edu/book/30595
[38] Liu, W., Yue, X.-G., & Tchounwou, P. B. (2020). Response to the COVID-19 Epidemic: The Chinese Experience and Implications for Other Countries. *International Journal of Environmental Research and Public Health*, *17*(7). https://doi.org/10.3390/ijerph17072304
[39] Tian, H., Liu, Y., Li, Y., Wu, C.-H., Chen, B., Kraemer, M. U. G., Li, B., Cai, J., Xu, B., Yang, Q., Wang, B., Yang, P., Cui, Y., Song, Y., Zheng, P., Wang, Q., Bjornstad, O. N., Yang, R., Grenfell, B. T., … Dye, C. (2020). An investigation of transmission control measures during

the first 50 days of the COVID-19 epidemic in China. *Science*, *368*(6491), 638–642. https://doi.org/10.1126/science.abb6105
[40] Van de Pas, R. (2020). *Globalization Paradox and the Coronavirus pandemic* (Clingendael Report). Netherlands Institute of International Relations. https://www.clingendael.org/publication/globalization-paradox-and-coronavirus-pandemic
[41] Mozur, P., Zhong, R., & Krolik, A. (2020, March 1). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *New York Times*. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[42] Klimburg, D. A., Faesen, L., Verhagen, P., & Mirtl, P. (2020). *Pandemic Mitigation in the Digital Age*. The Hague Centre for Strategic Studies & The Austrian Institute for European and Security Policy. https://hcss.nl/report/pandemic-mitigation-digital-age
[43] Ibid.
[44] Tian, H., Liu, Y., Li, Y., Wu, C.-H., Chen, B., Kraemer, M. U. G., Li, B., Cai, J., Xu, B., Yang, Q., Wang, B., Yang, P., Cui, Y., Song, Y., Zheng, P., Wang, Q., Bjornstad, O. N., Yang, R., Grenfell, B. T., … Dye, C. (2020). An investigation of transmission control measures during the first 50 days of the COVID-19 epidemic in China. *Science*, *368*(6491), 638–642. https://doi.org/10.1126/science.abb6105
[45] Ibid.
[46] Bi, Q., Wu, Y., Mei, S., Ye, C., Zou, X., Zhang, Z., Liu, X., Wei, L., Truelove, S. A., Zhang, T., Gao, W., Cheng, C., Tang, X., Wu, X., Wu, Y., Sun, B., Huang, S., Sun, Y., Zhang, J., … Feng, T. (2020). 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*(8), 911–919. https://doi.org/10.1016/S1473-3099(20)30287-5
[47] Ibid.
[48] Ibid.
[49] Van de Pas, R. (2020). *Globalization Paradox and the Coronavirus pandemic* (Clingendael Report). Netherlands Institute of International Relations. https://www.clingendael.org/publication/globalization-paradox-and-coronavirus-pandemic
[50] Mozur, P., Zhong, R., & Krolik, A. (2020, March 1). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *New York Times*. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[51] Yuan, S. (2020, March 1). How China is using AI and big data to fight the coronavirus. *Al Jazeera*. https://www.aljazeera.com/news/2020/03/china-ai-big-data-combat-coronavirus-outbreak-200301063901951.html
[52] Van de Pas, R. (2020). *Globalization Paradox and the Coronavirus pandemic* (Clingendael Report). Netherlands Institute of International Relations. https://www.clingendael.org/publication/globalization-paradox-and-coronavirus-pandemic
[53] Mozur, P., Zhong, R., & Krolik, A. (2020, March 1). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *New York Times*. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[54] Ibid.
[55] *Emerging COVID-19 success story: South Korea learned the lessons of MERS*. (2020, June 30). Our World In Data. https://ourworldindata.org/covid-exemplar-south-korea"
[56] Watson, I., & Jeong, S. (2020, February 28). *Coronavirus mobile apps are surging in popularity in South Korea*. CNN. https://www.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html

[57] Klimburg, D. A., Faesen, L., Verhagen, P., & Mirtl, P. (2020). *Pandemic Mitigation in the Digital Age*. The Hague Centre for Strategic Studies & The Austrian Institute for European and Security Policy. https://hcss.nl/report/pandemic-mitigation-digital-age
[58] Ibid.
[59] https://coronamap.site/
[60] Klimburg, D. A., Faesen, L., Verhagen, P., & Mirtl, P. (2020). *Pandemic Mitigation in the Digital Age*. The Hague Centre for Strategic Studies & The Austrian Institute for European and Security Policy. https://hcss.nl/report/pandemic-mitigation-digital-age
[61] Ibid.
[62] Park, S., Choi, G. J., & Ko, H. (2020). Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea-Privacy Controversies. *JAMA*. https://doi.org/10.1001/jama.2020.6602
[63] *Emerging COVID-19 success story: South Korea learned the lessons of MERS*. (2020, June 30). Our World In Data. https://ourworldindata.org/covid-exemplar-south-korea"
[64] Lu, N., Cheng, K.-W., Qamar, N., Huang, K.-C., & Johnson, J. A. (2020). Weathering COVID-19 storm: Successful control measures of five Asian countries. *American Journal of Infection Control*, *48*(7), 851–852. https://doi.org/10.1016/j.ajic.2020.04.021
[65] Ibid.
[66] Park, S., Choi, G. J., & Ko, H. (2020). Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea-Privacy Controversies. *JAMA*. https://doi.org/10.1001/jama.2020.6602
[67] Klimburg, D. A., Faesen, L., Verhagen, P., & Mirtl, P. (2020). *Pandemic Mitigation in the Digital Age*. The Hague Centre for Strategic Studies & The Austrian Institute for European and Security Policy. https://hcss.nl/report/pandemic-mitigation-digital-age
[68] Park, S., Choi, G. J., & Ko, H. (2020). Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea-Privacy Controversies. *JAMA*. https://doi.org/10.1001/jama.2020.6602
[69] Ibid.
[70] Cox, D. (2020). Alarm bells ring for patient data and privacy in the covid-19 goldrush. *BMJ*. https://doi.org/10.1136/bmj.m1925
[71] *Emerging COVID-19 success story: South Korea learned the lessons of MERS*. (2020, June 30). Our World In Data. https://ourworldindata.org/covid-exemplar-south-korea"
[72] Park, S., Choi, G. J., & Ko, H. (2020). Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea-Privacy Controversies. *JAMA*. https://doi.org/10.1001/jama.2020.6602
[73] Klimburg, D. A., Faesen, L., Verhagen, P., & Mirtl, P. (2020). *Pandemic Mitigation in the Digital Age*. The Hague Centre for Strategic Studies & The Austrian Institute for European and Security Policy. https://hcss.nl/report/pandemic-mitigation-digital-age
[74] Ibid.
[75] Van de Pas, R. (2020). *Globalization Paradox and the Coronavirus pandemic* (Clingendael Report). Netherlands Institute of International Relations. https://www.clingendael.org/publication/globalization-paradox-and-coronavirus-pandemic
[76] https://www.tracetogether.gov.sg/
[77] *Statistics Singapore—Population and Households*. (n.d.). Department of Statistics Singapore. Retrieved August 23, 2020, from https://www.singstat.gov.sg/publications/reference/singapore-in-figures/population-and-households

[78] Kuguyo, O., Kengne, A. P., & Dandara, C. (2020). Singapore COVID-19 Pandemic Response as a Successful Model Framework for Low-Resource Health Care Settings in Africa? *OMICS: A Journal of Integrative Biology*, *24*(8), 470–478. https://doi.org/10.1089/omi.2020.0077
[79] Cho, H., Ippolito, D., & Yu, Y. W. (2020). *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs*. http://arxiv.org/abs/2003.11511
[80] Ibid.
[81] Klonowska, K., & Bindt, P. (2020). *The COVID-19 pandemic: Two waves of technological responses in the European Union*. Hague Centre for Strategic Studies; JSTOR. https://doi.org/10.2307/resrep24004
[82] Ibid.
[83] Ibid.
[84] Ibid.
[85] Sabat, I., Neuman-Böhme, S., Varghese, N. E., Barros, P. P., Brouwer, W., van Exel, J., Schreyögg, J., & Stargardt, T. (2020). United but divided: Policy responses and people's perceptions in the EU during the COVID-19 outbreak. *Health Policy*. https://doi.org/10.1016/j.healthpol.2020.06.009
[86] Van Kolfschooten, H., & de Ruijter, A. (2020). COVID-19 and privacy in the European Union: A legal perspective on contact tracing. *Contemporary Security Policy*, *41*(3), 478–491. https://doi.org/10.1080/13523260.2020.1771509
[87] Ibid.
[88] Ibid.
[89] Klonowska, K., & Bindt, P. (2020). *The COVID-19 pandemic: Two waves of technological responses in the European Union*. Hague Centre for Strategic Studies; JSTOR. https://doi.org/10.2307/resrep24004
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Ibid.
[94] Sabat, I., Neuman-Böhme, S., Varghese, N. E., Barros, P. P., Brouwer, W., van Exel, J., Schreyögg, J., & Stargardt, T. (2020). United but divided: Policy responses and people's perceptions in the EU during the COVID-19 outbreak. *Health Policy*. https://doi.org/10.1016/j.healthpol.2020.06.009
[95] Ibid.
[96] Klonowska, K., & Bindt, P. (2020). *The COVID-19 pandemic: Two waves of technological responses in the European Union*. Hague Centre for Strategic Studies; JSTOR. https://doi.org/10.2307/resrep24004
[97] Ibid.
[98] Van Kolfschooten, H., & de Ruijter, A. (2020). COVID-19 and privacy in the European Union: A legal perspective on contact tracing. *Contempora*
[99] Landman, K. (2020, June 28). *Hey America, What Happened to Contact Tracing?* https://elemental.medium.com/hey-america-what-happened-to-contact-tracing-47a2dbccc020
[100] https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html
[101] Aschwanden, C. (2020). Contact Tracing, a Key Way to Slow COVID-19, Is Badly Underused by the U.S. *Scientific American*. https://www.scientificamerican.com/article/contact-tracing-a-key-way-to-slow-covid-19-is-badly-underused-by-the-u-s/

[102] Cha, V. (2020). Asia's COVID-19 Lessons for the West: Public Goods, Privacy, and Social Tagging. *The Washington Quarterly*, *43*(2), 1–18. https://doi.org/10.1080/0163660X.2020.1770959
[103] Pentland, A. (2020). *Restarting the Economy and Avoiding Big Brother:* MIT Initiative on the Digital Economy. http://ide.mit.edu/publications/restarting-economy-and-avoiding-big-brother.
[104] Cha, V. (2020). Asia's COVID-19 Lessons for the West: Public Goods, Privacy, and Social Tagging. *The Washington Quarterly*, *43*(2), 1–18. https://doi.org/10.1080/0163660X.2020.1770959
[105] Maor, M., Sulitzeanu-Kenan, R., & Chinitz, D. (2020). When COVID-19, constitutional crisis, and political deadlock meet: The Israeli case from a disproportionate policy perspective. *Policy and Society*, *39*(3), 442–457. https://doi.org/10.1080/14494035.2020.1783792
[106] Klimburg, D. A., Faesen, L., Verhagen, P., & Mirtl, P. (2020). *Pandemic Mitigation in the Digital Age*. The Hague Centre for Strategic Studies & The Austrian Institute for European and Security Policy. https://hcss.nl/report/pandemic-mitigation-digital-age
[107] Ibid
[108] Hershkowitz, T. S. A. and R. A. (2020, July 6). How Israel's COVID-19 mass surveillance operation works. *Brookings*. https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/
[109] Klimburg, D. A., Faesen, L., Verhagen, P., & Mirtl, P. (2020). *Pandemic Mitigation in the Digital Age*. The Hague Centre for Strategic Studies & The Austrian Institute for European and Security Policy. https://hcss.nl/report/pandemic-mitigation-digital-age
[110] Hershkowitz, T. S. A. and R. A. (2020, July 6). How Israel's COVID-19 mass surveillance operation works. *Brookings*. https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/
[111] Chachko, Elena. (2020, May 5). *The Israeli Supreme Court Checks COVID-19 Electronic Surveillance*. Lawfare. https://www.lawfareblog.com/israeli-supreme-court-checks-covid-19-electronic-surveillance
[112] Hershkowitz, T. S. A. and R. A. (2020, July 6). How Israel's COVID-19 mass surveillance operation works. *Brookings*. https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/
[113] Schulman, M. (2020, July 21). Sudden implosion of Israel's COVID response might prove Netanyahu's undoing. *Newsweek.* https://www.newsweek.com/netanyahu-covid-response-israel-chaos-1519456
[114] Murray, C. (2020, July 15). Israel's second coronavirus wave is threatening Netanyahu's hold on power. *Vox.* https://www.vox.com/2020/7/15/21326028/israel-netanyahu-coronavirus-covid-19
[115] Ibid.
[116] Ibid.
[117] Schulman, M. (2020, July 21). Sudden implosion of Israel's COVID response might prove Netanyahu's undoing. *Newsweek.* https://www.newsweek.com/netanyahu-covid-response-israel-chaos-1519456
[118] Murray, C. (2020, July 15). Israel's second coronavirus wave is threatening Netanyahu's hold on power. *Vox.* https://www.vox.com/2020/7/15/21326028/israel-netanyahu-coronavirus-covid-19

[119] Hershkowitz, T. S. A. and R. A. (2020, July 6). How Israel's COVID-19 mass surveillance operation works. *Brookings*. https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/
[120] Ibid.
[121] Ibid.
[122] *Israel's coronavirus surveillance is an example for others—Of what not to do.* (2020, May 1). *Privacy International*. https://privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do
[123] Hershkowitz, T. S. A. and R. A. (2020, July 6). How Israel's COVID-19 mass surveillance operation works. *Brookings*. https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/
[124] Yarmosky, J. (2020, August 17). How Taiwan is battling coronavirus with tech, crowdsourced data and trust. *The World*. https://www.pri.org/stories/2020-08-17/how-taiwan-battling-coronavirus-tech-crowdsourced-data-and-trust
[125] Klimburg, D. A., Faesen, L., Verhagen, P., & Mirtl, P. (2020). *Pandemic Mitigation in the Digital Age*. The Hague Centre for Strategic Studies & The Austrian Institute for European and Security Policy. https://hcss.nl/report/pandemic-mitigation-digital-age
[126] Ibid.
[127] Ibid.
[128] Wang, C. J., Ng, C. Y., & Brook, R. H. (2020). Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing. *JAMA*, *323*(14), 1341–1342. https://doi.org/10.1001/jama.2020.3151
[129] Steinbrook, R. (2020). Contact Tracing, Testing, and Control of COVID-19—Learning From Taiwan. *JAMA Internal Medicine*. https://doi.org/10.1001/jamainternmed.2020.2072
[130] Cheng, H.-Y., Jian, S.-W., Liu, D.-P., Ng, T.-C., Huang, W.-T., & Lin, H.-H. (2020). Contact Tracing Assessment of COVID-19 Transmission Dynamics in Taiwan and Risk at Different Exposure Periods Before and After Symptom Onset. *JAMA Internal Medicine*. https://doi.org/10.1001/jamainternmed.2020.2020
[131] Yarmosky, J. (2020, August 17). How Taiwan is battling coronavirus with tech, crowdsourced data and trust. *The World*. https://www.pri.org/stories/2020-08-17/how-taiwan-battling-coronavirus-tech-crowdsourced-data-and-trust
[132] Duff-Brown, B. (2020, March 3). *How Taiwan Used Big Data, Transparency and a Central Command to Protect Its People from Coronavirus*. Stanford Health Policy. https://healthpolicy.fsi.stanford.edu/news/how-taiwan-used-big-data-transparency-central-command-protect-its-people-coronavirus
[133] Yarmosky, J. (2020, August 17). How Taiwan is battling coronavirus with tech, crowdsourced data and trust. *The World*. https://www.pri.org/stories/2020-08-17/how-taiwan-battling-coronavirus-tech-crowdsourced-data-and-trust
[134] Lanier, J., & Weyl, E. G. (2020, April 10). How Civic Technology Can Help Stop a Pandemic. *Foreign Affairs.* https://www.foreignaffairs.com/articles/asia/2020-03-20/how-civic-technology-can-help-stop-pandemic
[135] Ibid.
[136] Yarmosky, J. (2020, August 17). How Taiwan is battling coronavirus with tech, crowdsourced data and trust. *The World*. https://www.pri.org/stories/2020-08-17/how-taiwan-battling-coronavirus-tech-crowdsourced-data-and-trust

[137] Wang, C. J., Ng, C. Y., & Brook, R. H. (2020). Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing. *JAMA*, *323*(14), 1341–1342. https://doi.org/10.1001/jama.2020.3151
[138] Kluth, A. (2020, April 22). If We Must Build a Surveillance State, Let's Do It Properly. *Bloomberg.com*. https://www.bloomberg.com/opinion/articles/2020-04-22/taiwan-offers-the-best-model-for-coronavirus-data-tracking
[139] Ibid.
[140] Stancati, M. (2020, August 13). Rising Coronavirus Infections Trigger Renewed Travel Restrictions Across Europe. *Wall Street Journal*. https://www.wsj.com/articles/rising-coronavirus-infections-restrict-european-holidaymakers-11597326586
[141] Klonowska, K., & Bindt, P. (2020). *The COVID-19 pandemic: Two waves of technological responses in the European Union*. Hague Centre for Strategic Studies; JSTOR. https://doi.org/10.2307/resrep24004
[142] Ibid.
[143] Lanier, J., & Weyl, E. G. (2020, April 10). How Civic Technology Can Help Stop a Pandemic. *Foreign Affairs.* https://www.foreignaffairs.com/articles/asia/2020-03-20/how-civic-technology-can-help-stop-pandemic
[144] Watson, I., & Jeong, S. (2020, February 28). *Coronavirus mobile apps are surging in popularity in South Korea*. CNN. https://www.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html
[145] Mozur, P., Zhong, R., & Krolik, A. (2020, March 1). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *New York Times*. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[146] Pei, M. (2020, July 17). China's Coming Upheaval. *Foreign Affairs*. https://www.foreignaffairs.com/articles/united-states/2020-04-03/chinas-coming-upheaval
[147] Cyranoski, D. (2020). What China's coronavirus response can teach the rest of the world. *Nature*, *579*(7800), 479–480. https://doi.org/10.1038/d41586-020-00741-x
[148] Reilly, T. (2020, March 19). COVID-19 and Xi Jinping: How the Strongman Got Stronger. *The Diplomat*. https://thediplomat.com/2020/03/covid-19-and-xi-jinping-how-the-strongman-got-stronger/
[149] Ibid.
[150] Macaskill, Andrew. (2020, November 24). 50,000 COVID-19 deaths and rising. How the UK keeps failing. *Reuters*. https://www.reuters.com/investigates/special-report/health-coronavirus-britain-newwave/
[151] Giugliano, Ferdinando. (2020, March 25). Boris Johnson's Coronavirus Response Is a Fiasco. *Bloomberg*. https://www.bloomberg.com/opinion/articles/2020-03-25/coronavirus-boris-johnson-s-response-has-been-a-fiasco
[152] Ibid
[153] Gugushvili, A., Koltai, J., Stuckler, D., & McKee, M. (2020). Votes, populism, and pandemics. *International Journal of Public Health*, *65*(6), 721–722. https://doi.org/10.1007/s00038-020-01450-y
[154] Ibid
[155] English, O. (2020, March 18). Coronavirus' next victim: Populism. *Politico*. https://www.politico.eu/article/coronavirus-next-victim-populism-uk-boris-johnson-us-donald-trump/

[156] McGee, L. (2020, October 13). *Analysis: Boris Johnson has split from his top scientists on coronavirus*. CNN. https://www.cnn.com/2020/10/13/uk/boris-johnson-versus-scientific-advice-intl-gbr/index.html
[157] Macaskill, Andrew. (2020, November 24). 50,000 COVID-19 deaths and rising. How the UK keeps failing. *Reuters*. https://www.reuters.com/investigates/special-report/health-coronavirus-britain-newwave/
[158] Ibid.
[159] *Data protection and coronavirus—What you need to know*. (2020, July 20). ICO. https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/
[160] https://coronavirus.jhu.edu/map.html
[161] Is China winning? (2020, April 16). *The Economist*. https://www.economist.com/leaders/2020/04/16/is-china-winning
[162] Hart, V., Siddarth, D., Cantrell, B., & Tretikov, L. (n.d.). *Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks*. Retrieved August 23, 2020, from https://ethics.harvard.edu/outpacing-virus
[163] Ibid
[164] Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine*, *26*(4), 463–464. https://doi.org/10.1038/s41591-020-0832-5
[165] *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics*. (2020). Organisation for Economic Co-operation and Development. https://read.oecd-ilibrary.org/view/?ref=129_129655-7db0lu7dto&title=Tracking-and-Tracing-COVID-Protecting-privacy-and-data-while-using