Journal of Cybersecurity Education, Research and Practice

Volume 2022 | Number 1 Article 4

July 2022

Digital Contact Tracing and Privacy

Mahdi Nasereddin
The Pennsylvania State University, mxn16@psu.edu

Edward J. Glantz
Pennsylvania State University, ejg8@psu.edu

Galen A. Grimes
The Pennsylvania State University, gag5@psu.edu

Joanne Peca
Carnegie Mellon University, jpeca@cmu.edu

Michelle Gordon
The Pennsylvania State University, mgh11@psu.edu

See next page for additional authors

Digital Contact Tracing and Privacy

Abstract

Digital contact tracing tools were developed to decrease the spread of COVID-19 by supplementing traditional manual methods. Although these tools have great potential, they were developed rather quickly resulting in tools with varying levels of success. The main issues with these tools are over privacy and who might have access to the information gathered. In general, their effectiveness varied globally, where users expressed privacy concerns associated with sharing identity, illness, and location information. This paper reviews these issues in deployments across Asia, Europe, and the United States. The goal is to begin a discussion that improves the design and development of digital technologies that not only improve the control of infectious disease spread, but also achieve an appropriate standard of privacy and security.

Keywords

privacy, contact tracing, digital tracking

Authors

Mahdi Nasereddin, Edward J. Glantz, Galen A. Grimes, Joanne Peca, Michelle Gordon, and Mike Bartolacci

INTRODUCTION

This work reviews contract tracing and recent use of its digital successor for control of the spread of disease. In particular, the introduction of COVID-19 digital contact tracing and emerging implications for privacy are explored. Privacy concerns have increased along with increasing use of digital tools for contact tracing and other health-related interventions such as vaccination passports. Even in early stages, digital contact tracing development and implementation has raised public concerns relating to personal data collection, access, and storage. This paper introduces this discussion in an attempt to further research that improves development. This is important as benefits of digital tool use hinges on public trust of the data management.

The United States Centers for Disease Control and Prevention (CDC) states that the purpose of contact tracing is a means to slow or stop the spread of infectious disease through the process of informing individuals who may have been exposed to self-isolate, or "socially distance" themselves from others, thus limiting further spread. If a person is suspected of being infected, having safer interactions from a minimal distance (e.g., six feet), while using protective items such as face masks can limit the transmission of the disease (Maragakis, 2020). Contact tracing and this notion of keeping a distance from others, known as social distancing, are often combined to control the spread of disease. The identification of "exposure" (contact with an infected person within a certain distance for a certain period of time without proper precautions) is where contact tracing and its digital counterpart come into use.

COVID-19 facilitated case management and the tracking of people using digital contact tracing with smartphones and such portable wireless devices that can load the associated application. Such information and communication technologies (ICT) inherent in these devices, such as global positioning systems (GPS) which can give fairly accurate location information (GPS here is just being used for a general location, not firing missiles 1000 miles away), and Bluetooth which can allow digital contact tracing to be possible. As with implementation of such technologies, potential privacy issues arise including breaches of individual identities, government surveillance instilling fear, the threatening of civil liberties, and questions regarding data anonymizing and retention requirements (Whitelaw et al., 2020). A key factor that pervades the introduction of digital tracing during the COVID-19 pandemic is the tradeoff in the minds of the affected population between the fear of loss of privacy and the ability of the applications to protect them from getting ill. This paper takes a more descriptive approach in that it reports on what took place with the rollout of digital contact tracing in various parts of the world and does not delve specifically into the psychological aspects of new technology acceptance or this tradeoff between privacy and illness.

CONTACT TRACING HISTORY

The first step in the process of contact tracing is to identify those currently infected, and therefore capable of transmitting disease. Testing is then required to confirm infection, although the results may require one or more days. The second step of the process is to monitor possible contact with those who have tested positive for the disease being monitored. The third step attempts to control spread by safely quarantining those exposed, even if not yet showing symptoms. Testing

delays complicate an already difficult process that must monitor both one-on-one contact and contact at mass gathering events such as meetings, shopping, and other large events (CDC, 2020).

Despite these issues, contact tracing has a long history of use by the CDC in the U.S. as well as globally by the World Health Organization (WHO). Contact tracing has been used to help control sexually transmitted and other infectious diseases in the past (Bland, 2020). The general idea of controlling the spread of infectious diseases through contact tracing and quarantine is not novel to the COVID-19 pandemic, as such methods having existed for centuries. Archaeological and anthropological researchers have found evidence that 5,000 years ago a prehistoric village in northeast China burned the dead bodies of an infected group to prevent spread of a disease (Jarus, 2020).

In the United States, contemporary contact tracing dates to the early 20th-century response to syphilis, and later its use was expanded to include other sexually transmitted diseases. Contact tracing has generated debate since its inception about the right to the confidentiality of infected individuals, as well as the rights of the infected individual's contacts to be informed about their exposure. The public skepticism relating to the right to privacy grew with the emergence of the human immunodeficiency virus (HIV), especially among urban male homosexuals during the 1980s and 1990s (Burr, 1997).

Only a limited number of states had mandatory reporting of the names of those infected with HIV or other sexually transmitted diseases. In other states, reporting and testing were voluntary and resulted in a much lower volume of both. There also existed no uniformity in testing measures. For example, HIV testing was required only for immigrants entering the country, foreign-service and military personnel, and prison inmates at the federal level. Requiring HIV testing was prohibited everywhere else except at the state level under narrowly defined circumstances (Burr, 1997). Traditionally, the associated contact tracing was performed through health departments in response to HIV and other sexually transmitted disease cases using trained department-employed disease intervention specialists. Such specialists played vital roles in case investigation and contact tracing through supervisory roles, despite facing challenges like distrust and concerns about confidentiality (Bland, 2020).

Contact tracing was also adopted for the 2009 H1N1 swine flu pandemic. This disease, thought to have originated in Mexico in the spring of 2009 before spreading to the rest of the world, was a pandemic of a smaller scale than COVID-19. This pandemic killed more than 100,000 people worldwide, primarily affecting children and young adults (Jarus, 2020).

COVID CONTACT TRACING

Information and communication technologies (ICT) solutions were developed in response to the late 2019 emergence of the COVID-19 virus which is also known by the more technical name as SARS-CoV-2. Within six months of its appearance in China in 2019, the virus had spread to more than 155 countries and affected more than 8 million people to varying degrees. With no inherent immunity or clear treatment to protect against COVID-19, a digital contact tracing application emerged as one method to attempt to control the spread of the disease by reporting contact between application uninfected users and possible infection sources also using the application.

Contact tracing applications have had some success in preventing the spread of COVID-19, although these applications failed to maintain all of the public's trust due to privacy concerns. In the United States, for example, a large percentage of the population resisted contact tracing in part due to data privacy and data security concerns. China and South Korea, on the other hand, encountered less resistance with similar efforts in the use of such applications (Cohen et al., 2020). Despite the limited use of contact tracing applications and other means such as social distancing, the United States failed to contain and trace the spread of COVID-19 during early 2020. The lack of a recent pandemic precedent in the United States, the varying reports on the characteristics of the disease, the presumption that only the elderly and patients with pre-existing conditions were at risk, and the fear of economic consequences, led to multiple setbacks in the response to COVID-19. Thus, the effectiveness of digital and even manual contact tracing overall was severely limited (Nowroozpoor et al., 2020).

In contrast, to control the spread of COVID-19, China employed aggressive measures initially in Wuhan and then in other cities. In an attempt to slow down and stop the chains of transmission, the government imposed strict lockdowns along with case investigations and contact tracing, including travel restrictions by contacts. Though government authorities and health experts worldwide have adopted various approaches to mitigate and contain such spread of infectious diseases, contact tracing has remained one the most relied-upon methods of containing the spread of an infectious disease. Digital contact tracing is a product of the 21rst century technologies in order to carry it out. In the early stages of the COVID-19 outbreak, many east Asian countries took rapid, stringent, and pervasive measures including implementing digital means of tracking the population. In contrast, most European countries and the United States took more apprehensive, delayed, and reactive responses with limited rollouts and implementations of digital contact tracing. (Owusu, 2020).

For example, studies in South Korea and Singapore suggest that the use of electronic tracking of citizens' location data facilitated mitigation of the pandemic's impact without the same level of societal lockdowns used in Europe and the United States. Although additional waves of disease are possible even with the current vaccines becoming more readily available across the globe, the initial results of such ICT applications technologies to this point are promising. However, concerns have been raised about the acceptability of surrendering privacy via location data gathered from cellular phones, and similar portable electronic devices, to government and private entities. The potential for misuse of such data has raised considerable debate in public and academic spheres regarding how to balance privacy risks against public health benefits (Owusu, 2020).

Digital Contact Tracing Issues

The United States, and other countries with high COVID infection rates, used both manual and digital methods of contact tracing. The public health agencies converted the role of many non-essential agency workers and other employees to a temporary position of "contact tracer". Among many approaches attempted in trying to mitigate the spread of the virus, the most critical strategy initially was to contain the coronavirus using rapid tracing and notification of potentially infected individuals and their contacts. Several nations implemented mobile phone applications to alert individuals to potential exposure due to its expected advantages of speed, specificity, and mass reach over the traditional manual method of contact tracing (Owusu, 2020).

The United States used both digital and manual methods of contact tracing based on the guidance from the CDC. These tracings were conducted based on the number of ongoing cases that states were having at a given time and the associated infection rate. Manual tracing became more convenient and successful in states experiencing a smaller number of cases with a relatively low spread rate, whereas digital/electronic tracing gives more confidence and reliability when the outbreak was larger and spreading faster in a geographic region or state. Digital tracing platforms utilize mobile applications with location detection capabilities and a means to detect others nearby using the same application. Recording these proximity encounters by the application only becomes relevant when a person using the application tests positive for the disease.

The gathered information about other application users who came within close contact of the infected person allows for the backward tracing during the approximate incubation period. Bluetooth functionality is most often the technology of choice for detecting this close proximity due to the fact that it is built into all mobile phones. Once a user is determined to be infected, central authorities can alert other users who were in close proximity to the user who has tested positive via the application or other means. Such applications help healthcare officials and other public entities understand how rapid the spread is to assist in developing strategies or plans to interrupt its spread. It also alerts users to be wary of symptoms and to isolate themselves in order to prevent the spread if they truly are infected.

Many United States citizens were skeptical of digital contact tracing due in part to privacy concerns. Fears that government agencies outside of the public health arena might have access to the collected data prevented many from adopting the applications. Most states were able to create their own applications and with the lockdowns of 2020, such applications could cover the population of a state fairly well if utilized. Unfortunately, such widespread adoption of the applications was hindered when people postulated a privacy compromise under the guise of public health measures. A general lack of trust existed between citizens of most states and government/private entities that would collect the personal data when signing up for the application and the location/contact information stored during its operation. Concerns grew that the government might utilize such information to control the lives of people in some onerous fashion (Thompson, 2020).

PRIVACY CONCERNS

Privacy concerns associated with contact tracing came to the surface as the COVID-19 pandemic spread across the globe and 2020 moved into 2021. In South Korea, for example, the government widely used digital contact tracing and location tracking. At times it also attempted to impose strict movement control through the platform utilized. Even though anonymity was supposed to be present for many contact tracing application users across various platforms, some researchers and human-rights activists started to voice concerns that the data trails released in such efforts were so detailed that individuals could be identified. Despite such claims, the public has generally been positive of the South Korean government's measures to control the spread of the disease using a digital means (Zastrow, 2020). In fact, most of Southeastern and Far East Asia saw relative success in the acceptance of digital contact tracing by the population.

The development of digital contact tracing tools continues to emerge and evolve geopolitically, both in technical approach, as well as the privacy afforded personal data collection,

access, and storage. History and government control influence citizen expectations of personal data privacy. South Korea's previous experience managing Middle East respiratory syndrome (MERS) enabled laws that subordinate personal data "privacy" expectations to "transparent and accurate" virus information, including publishing travel histories of confirmed patients (Zastrow, 2020). The following is a sampling of tracing technologies and data privacy. A more detailed investigation of this trend is merited and included in the "future work" section of this paper.

Digital Tracing in South Korea and East Asia

The South Korean government created a centralized public database about infected individuals and their movements, which was used by application developers to identify the proximity of users to infected individuals (Ryan, 2020). Claiming a direct privacy infringement, Western media has generally been critical of some East Asian countries' use of digital contact-tracing to control COVID-19. Authorities in South Korea used GPS information and card transaction logs to identify routes and potential contacts when manual contact-tracing was unsuccessful. The government also had the authority to access the data of infected individuals from telecommunications operators in order to identify more details about the infected individuals' routes and those likely to be infected by the virus along such paths. GPS data, times, locations, and travel routes were mapped to determine the paths of infected individuals and modes of transportation used. The government also used satellite technology to quickly identify the paths of the confirmed cases and informed the residents of the areas along such paths in real-time via mobile text messages.

Digital Tracing in Europe

The spread of COVID-19 created the need for digital contact tracing in Europe. Using location data, many European countries such as Austria, Croatia, Denmark, Germany, Italy, Ireland, Latvia, and Poland launched contact tracing applications using Bluetooth technologies to monitor close encounters that could spread the disease. The applications typically displayed a 'green', or safe, status if a given user did not have close contact with a known infected individual for a given period of time. Should the user spend more than 15 minutes within two meters of another application user who then tests positive and uploads this result, the first user would get an exposure notification along with others who had a similar exposure. The design of Bluetooth-based applications had the trade-off between usefulness and privacy as it was difficult to pinpoint the exact time and place of risk events from the application alone (Reuters, 2020).

Due to its strict data privacy laws, Germany initially relied on the traditional method of contact tracing by setting up call centers to help its citizens in contact tracing and referring callers to medical personnel. Germany's attempts at manual contact tracing eventually proved unsuccessful as the cases surged. It eventually launched a national contact tracing application entitled "Corona-Warn". This application was built on the backbone of a Bluetooth-enabled contact tracing API jointly developed by Apple and Google. The platform was designed to preserve user privacy by limiting the amount of personal data processed. The application broadcasts a random identifier, while regularly scanning for and locally storing other phones' unique identifiers using the Bluetooth low energy technology. If a user tests positive for the coronavirus, they will receive a QR code along with their results from the testing facility. The user then can upload their identifier to a server over a 14-day window. Once uploaded, the process generates a warning to the devices whose identifiers

have been matched to the identifier broadcasted by the person who has been infected. Despite the German government's effort to stick to its privacy commitments, this application was not utilized by a significant percentage of the population. In fact, a poll concluded that 39% of the population stated that they would not use the application (Leprince-Ringuet, 2020).

Digital Tracing in the United States

Studies have shown that exposure notification applications, in other words digital contact tracing, could reduce COVID-19 infections if used by a large percentage of a given population. In the U.S., Alabama, South Carolina, and North Dakota were among the first to express interest in Apple and Google's Exposure Notifications API for assisting COVID-19 contact tracing (Leswing, 2020). The states of New York (NY), Pennsylvania (PA), and New Jersey (NJ) soon followed, releasing, respectively, COVID-Alert NY, PA, and NJ; all are Bluetooth-based contact tracing apps. Similarly, California's CA COVID Notify had the goal of allowing officials to help track exposure to COVID-19 and determine the spread of the virus (Schuster et al., 2020).

Though many countries had initially and successfully mitigated the COVID-19 pandemic via stringent measures to limit an individual's movements and abate public interactions, these approaches were unlikely to be accepted in the United States. The initial lack of national coordination and inadequate testing hindered manual contact tracing efforts. Due to the lack of coordinated public health leadership, the United States still struggled to achieve adequate and consistent testing despite being the largest economy in the world (Clark et al., 2021). Thus, the need for digital contract tracing to assist in stemming the tide of COVID's spread across the country.

A Pew Research poll conducted in July of 2019 found that many Americans saw declining levels of trust in the country's governmental agencies; thus, equating to a declining level of trust in actions taken by the federal government or even state governments. The research also found that personal trust ranges across a wide spectrum with differences in trust levels tied to race and age, ethnicity, education, and household income. Individuals who are not white, are younger, are less educated, and who are in a lower socioeconomic group have lower levels of personal trust than other Americans. Most people of these groups believe the federal government and the major news media withhold important and useful information from the public (Rainie & Perrin, 2019). In light of this environment, attempts at implementing digital contact tracing were undertaken in 2020.

Another research effort on general attitudes toward the process of contact tracing conducted during the COVID-19 pandemic shows that most adults would be open to participating in some parts of the process of identifying and isolating people who have fallen ill with COVID-19. Unfortunately, it was also found that they would be reluctant to engage fully with public health authorities as a result of such participation. The research also noted that about four in ten adults stated that they would not be likely to speak with public health officials by phone or text message or at their home as part of this process. A significant portion of adults also stated they would be uncomfortable sharing names of contacts or places they have recently visited with a public health official (McClain & Rainie, 2020).

The perceived conflict between privacy associated with contact tracing (or lack thereof) and public trust and fears of misinformation associated with the federal government resulted in inconsistency in the approaches and measures used to deploy uniform contact tracing methodologies

in the United States. The inconsistency brought confusion to many people as state, local, and the federal governments failed to convince skeptical citizens that their privacy would not be compromised. In the U.S., health officials and government workers struggled to get the public to cooperate with coronavirus contact tracing. Tracers struggled to communicate with the infectious, or those who came in close contact for more than fifteen minutes with an infected person.

The main reason behind this ineffectiveness was again the issues of privacy and how the collected information might be used. People did not want to let others know where they were at a given time or who they were meeting with (Feuer, 2020). As an example, manual contact tracers in North Carolina's Mecklenburg County, home to Charlotte, investigated over five-thousand confirmed COVID-19 infections. Among them, 48% reported not coming into close contact with anyone. Of the contacts provided, 25% did not return tracers' phone calls, thus impeding the contact tracing process. Due to personal privacy concerns, individuals in this county were not comfortable discussing contacts and movements with governmental and health officials (Feuer, 2020).

PRIVACY MATTERS TO PEOPLE

The general contact tracing process created confusion among individuals which lead to further concern over privacy. University students, for example, were unsure whether they needed to quarantine when a roommate was contact traced and called in for testing (Heights, 2020). Privacy concerns extend beyond just contact tracing to also include location identification. In response to this concern, states attempted to achieve contact tracing without disclosing location information. For example, Pennsylvania's free application used Bluetooth wireless technology to only detect proximity defined as when two users were within six feet of each other for 15 minutes or more, but not direct location information. Health officials hoped this would allow more citizens to participate in the contact tracing process (Rushing & Goodin-Smith, 2020).

The application itself provided users with testing-related information, thus reducing time needed for health departments to communicate with a possible contact. Citizens appeared more comfortable cooperating with this initiative's emphasis on proximity, rather than location identifiers. Users were able to use encryption to protect identity, as well as anonymous identifier beacons that changed frequently. When a user received a proximity alert to an individual that later tested positive, the health department asked the user if he/she was willing to use the application to notify other users who have been in close contact with them in the past fourteen days. Officials believe this decreased confusion with digital contact tracing while building overall trust in the process. An added benefit was that people were more comfortable receiving an alert message from a known entity, rather than from government officials or health workers (Rushing & Goodin-Smith, 2020).

Privacy advocates argue that governments should use methods to trace the virus without compromising citizens' privacy or creating the perception of compromise. As a result, some colleges and universities researched other methods and techniques to collect data to control the virus. Yale University researchers found that "sewer sludge" analysis flowing out of student dorms detected coronavirus outbreaks faster than individual contact tracing. A further benefit of this approach is that individuals would not need to compromise privacy while health officials achieved faster results, expediting efforts to contain the spread (Sykes, 2020). Another approach for contact tracing in Singapore used Bluetooth-based lanyards for elderly populations, rather than cell phones due to the

nature of the elderly to not carry cell phones everywhere with them or even own one. The lanyard token was viewed as less intrusive than mobile devices for those concerned with privacy, as well as an improvement for those less likely to own a cell phone.

Several European Union countries including the Czech Republic, Denmark, Germany, Ireland, Italy, and Latvia continued testing a system that enables their COVID-19 contact tracing applications to work across borders (Holt, 2020). Mandatory reporting of pandemic statistics has added complexity to the digital contact tracing process. Despite privacy being universally valued, only 66% of the countries worldwide have privacy legislation with varying degrees of protection for information that may be collected in the digital contract tracing process. In Africa, only half of the countries have privacy protection legislation; while for Asia-Pacific countries, only 57% have privacy protection laws (*Data Protection and Privacy Legislation Worldwide | UNCTAD*, n.d.).

Currently, the EU's General Data Protection Regulation (GDPR) is considered the privacy standard in terms of privacy protection. GDPR gives the EU citizen greater control of their data than the EU's 1995 Data Protection Directive. The United States, unlike Europe, does not have an all-encompassing regulation, but it does have sector-specific privacy protection regulations. For example, HIPPA is used to secure protected health information and GLBA is used to protect personal financial information. In general, the US legislation focuses on the integrity of data as a commercial asset as opposed to placing individual rights before the interest of businesses as in the EU GDPR legislation. Additionally, some states have their own privacy protection legislation (California's being the most protective) (*EU vs US: How Do Their Data Privacy Regulations Square Off? | Endpoint Protector*, n.d.).

FUTURE WORK

There are several opportunities to apply digital technologies as a tool to respond and control pandemics. These areas include, for example, contact tracing, as well as monitoring quarantine and self-isolation efforts, screening for infection, self-treatment recommendations, clinical management, and planning and distribution of medical supplies. The success of these tools could be enhanced by development of privacy and security standards that protect individual information while preventing compromise and abuse. We seek to examine the issues surrounding such standards and the probability of their coming into existence in the near future. In addition, analysis of the continued global development of digital tracking and disease management tools would be beneficial, especially from the perspective of public trust and personal data collection, access, and storage.

CONCLUSIONS AND RECOMMENDATIONS

Privacy and confidentiality have always existed as primary issues in healthcare, especially when healthcare professionals are required to notify government agencies attempting to control the spread of disease. To preserve trust in the healthcare system, individuals must be comfortable with the ethical and legal aspects of their private information and its usage. Contact tracing, whether manual or digital, is part of this discussion. Both approaches to contact tracing, digital and manual, must assure individual privacy to achieve the necessary percentage of use and compliance in order to be useful in preventing the spread of disease. When properly accepted by the general public

during a health emergency such as the COVID-19 pandemic, digital contact tracing has great potential to supplement traditional manual contact tracing and achieve greater public protection from infection. The COVID-19 pandemic accelerated deployment of such digital solutions in healthcare. Much remains to be done in order to gain more widespread acceptance of digital contact tracing across the globe.

To this end that more widespread use and acceptance are necessary for effective use of digital contact tracing to truly prevent the spread of disease, we offer several suggestions for future introductions of these applications:

1. Although there is certainly a time consideration in introducing digital contact tracing applications to the affected population, such introductions should be phased and spaced out over time in order to combat the natural resistance to change by people and to show that the current set of users are not having their privacy compromised or having ill effects from its usage,
2. Third party "watchdog" organizations that are not affiliated with the government or the application's developers should be employed to monitor how the applications are being implemented and to address complaints or issues of concern from users and the general population, and
3. The offer of low cost or no cost mobile devices and cellular service to vulnerable (more suspectable to the disease due to their location, their socioeconomic status, or to their underlying medical condition) members of the general population in exchange for their pledge to not disable the application and to heed any alerts it gives them.

REFERENCES

Bland, S. (2020). Reflections on the History of Contact Tracing | O'Neill Institute. Retrieved July 10, 2021, from https://oneill.law.georgetown.edu/reflections-on-the-history-of-contact- tracing/

Burr, C. (1997). The AIDS exception: Privacy vs. public health. Atlantic Monthly (Boston, Mass.: 1993). https://www.theatlantic.com/magazine/archive/1997/06/the-aids- exception-privacy-vs-public-health/308779/

CDC. (2020). Case investigation and contact tracing: Part of a multipronged approach to fight the COVID-19 pandemic. Centers for Disease Control and Prevention. https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html

CDC. (2021). FAQ: Contact tracing: What is contact tracing? Centers for Disease Control and Prevention. https://www.cdc.gov/coronavirus/2019- ncov/faq.html#Contact-Tracing

Clark, E., Chiao, E. Y., & Amirian, E. S. (2021). Why contact tracing efforts have failed to curb coronavirus disease 2019 (COVID-19) Transmission in Much of the United States. Clinical Infectious Diseases, 72(9), e415– e419. https://doi.org/10.1093/CID/CIAA1155

Cohen, I.G., Gostin, L.O., & Weitzner, D.J. (2020). Digital smartphone tracking for COVID-19: Public health and civil liberties in tension. JAMA, 323(23): 2371–2372. doi:10.1001/jama.2020.8570.

Data Protection and Privacy Legislation Worldwide | UNCTAD. (n.d.). Retrieved September 10, 2021, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

EU vs US: How Do Their Data Privacy Regulations Square Off? | Endpoint Protector. (n.d.). Retrieved September 10, 2021, from https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/

Feuer, W. (2020). U.S. health officials struggle with coronavirus contact tracing, CDC study says. CNBC. Retrieved July 10, 2021, from https://www.cnbc.com/2020/09/22/us-health-officials-struggle-with- coronavirus-contact-tracing-cdc-study-says.html

Heights (2020). To combat confusion, release details on contact tracing procedures. Retrieved July 10, 2021, from https://www.bcheights.com/2020/09/21/to-combat-confusion-release- details-on-contact-tracing-procedures/

Holt, K. (2020, September 14). The EU is testing cross-border COVID-19 contact tracing. Engadget. https://www.engadget.com/covid-19-contact-tracing- test-european-union-cross-border-162652272.html

Jarus, O. (2020). 20 of the worst epidemics and pandemics in history. Live Science. https://www.livescience.com/worst-epidemics-and-pandemics-in- history.html

Leprince-Ringuet, D. (2020). Germany's contact-tracing app gets downloaded

6.5 million times in a day. ZDNet. Retrieved July 10, 2021, from https://www.zdnet.com/article/germanys-contact-tracing-app-gets- downloaded-6-5-million-times-in-a-day/

Lesswing, K. (2020). Three states will use Apple-Google contact tracing technology for virus tracking apps. CNBC. https://www.cnbc.com/2020/05/20/three-states-commit-to-apple-google- technology-for-virus-tracking-apps.html

Maragakis, L.L. (2020). Coronavirus, social and physical distancing, and self- quarantine. Infectious Diseases: Hopkins Medicine. https://www.hopkinsmedicine.org/health/conditions-and- diseases/coronavirus/coronavirus-social-distancing-and-self-quarantine

Mcclain, C., & Rainie, L. (2020, October 30). The challenges of contact tracing as U.S. battles COVID-19. Pew Research. https://www.pewresearch.org/internet/2020/10/30/the-challenges-of- contact-tracing-as-u-s-battles-covid-19/

Nowroozpoor, A., Choo, E. K., & Faust, J. S. (2020). Why the United States failed to contain COVID-19. Journal of the American College of Emergency Physicians Open, 1(4), 686–688. https://doi.org/10.1002/EMP2.12155

Owusu, P. N. (2020). Digital technology applications for contact tracing: The new promise for COVID-19 and beyond? Global Health Research and Policy, 5(1). https://doi.org/10.1186/S41256-020-00164-1

Rainie, L., & Perrin, A. (2019). Americans' declining trust in government, each other: Eight key findings. Pew Research Center. Retrieved July 10, 2021, from https://www.pewresearch.org/fact-tank/2019/07/22/key-findings-about-americans-declining-trust-in-government-and-each-other/

Reuters. (2020). Explainer: Europe's coronavirus smartphone contact tracing apps. Reuters. Retrieved July 10, 2021, from https://www.reuters.com/article/us-health-coronavirus-europe-tech- explai/explainer-europes-coronavirus-smartphone-contact-tracing-apps- idUSKCN2510MX

Rushing, E., & Goodin-Smith, O. (2020, September 23). Contact tracing app tells Pennsylvanians if they've been exposed to coronavirus. The Philadelphia Inquirer. https://www.inquirer.com/health/coronavirus/contact-tracing-app-pennsylvania-coronavirus-cases-20200923.html

Ryan, M. (2020). In defence of digital contact-tracing: Human rights, South Korea and COVID-19. International Journal of Pervasive Computing and Communications, 16(4): pp. 383-407. DOI: 10.1108/IJPCC-07-2020-0081

Schuster, H., Blitz, M., & Barthel, M. (2020). Community spread Is making contact tracing harder in the D.C. region – WAMU. Retrieved July 10, 2021, from https://wamu.org/story/20/11/25/covid19-contact-tracing-dc- md-va-what-we-know/

Sykes, S. (2020, September 24). 'Sewer sludge' detects coronavirus outbreaks days faster than contact tracing, study finds. NBC News. https://www.nbcnews.com/news/us-news/sewer-sludge-detects- coronavirus-outbreaks-days-faster-contact-tracing-study-n1240740

Thompson, S. (2020). Contact tracing: States make it hard to know if efforts are successful. The Washington Post. Retrieved July 10, 2021, from https://www.washingtonpost.com/local/contact-tracing-metrics/2020/07/04/da7d2812-bae4-11ea-bdaf-a129f921026f_story.html

Whitelaw, S., Mamas, M.A., Topol, E., & Van Spall, G.C. (2020). Applications of digital technology in COVID-19 pandemic planning and response. The Lancet. 2(8). e435-e440. https://doi.org/10.1016/S2589-7500(20)30142-4

Zastrow, M. (2020). South Korea is reporting intimate details of COVID-19 cases: Has it helped? Nature. https://doi.org/10.1038/D41586-020-00740-Y