The Global Business Law Review

Volume 10 | Issue 2 Note

8-1-2022

Flattening the Curve While Protecting Our Right to Privacy: How the United States Can Implement the Digital Contract Tracing Efforts Used in East Asia

Evan Morris
Cleveland-Marshall College of Law

Flattening the Curve While Protecting Our Right to Privacy: How the United States Can Implement the Digital Contact Tracing Efforts Used in East Asia

Evan Morris*

Table of Contents

* I would like to thank Professor Brian Ray for his guidance and mentorship.

Introduction

On December 31, 2019, the World Health Organization (WHO) learned of a "viral pneumonia" in Wuhan, People's Republic of China.[1] This disease, named "SARS-CoV-2" or "COVID-19"[2] has since infected over thirty-six million people, killing over one million.[3] One way to impede the spread of this new disease is by contact tracing.[4] Contact tracing is the process of identifying everyone who may have come into contact with an infected individual.[5] Contact tracing can be performed manually or digitally.[6] Manual contact tracing can take weeks to carry out,[7] whereas digital contact tracing has the potential to be faster and more efficient.[8] Countries in East Asia have used digital contact tracing, among other technologies, to effectively "flatten the curve" of their COVID-19 infection rate,[9] while the Americas accounted for the majority of

---

[1] World Health Organization, Timeline: WHO's COVID-19 response, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/interactive-timeline (last visited Oct 10, 2020).

[2] *Naming the coronavirus disease (COVID-19) and the virus that causes it*, WORLD HEALTH ORGANIZATION [WHO], https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it (last visited Oct 10, 2020).

[3] *WHO Coronavirus Disease (COVID-19) Dashboard*, World Health Organization [WHO], https://covid19.who.int (last visited Oct 10, 2020).

[4] Harvard Health Publishing, *Preventing the spread of the coronavirus*, HARVARD HEALTH , https://www.health.harvard.edu/diseases-and-conditions/preventing-the-spread-of-the-coronavirus (last visited Oct 10, 2020).

[5] *See Id.*

[6] *See* Ramesh Raskar et al., *Comparing manual contact tracing and digital contact advice*, ARXIV:2008.07325 [CS] (2020), http://arxiv.org/abs/2008.07325 (last visited Nov 28, 2020).

[7] Association of State and Territorial Health Officials [astho], *COVID-19 Case Investigation and Contact Tracing: Considerations for Using Digital Technologies*, 4. (2020)

[8] *See* Centers for Disease Control and Prevention (CDC), *Contact Tracing: Using Digital Tools*, 1., https://www.cdc.gov/coronavirus/2019-ncov/downloads/digital-contact-tracing.pdf (last visited Dec. 13, 2020)

[9] *See* How Digital Contact Tracing Slowed Covid-19 in East Asia, HARVARD BUSINESS REVIEW, 2020, https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia (last visited Nov 28, 2020); *see*

reported COVID-19 deaths globally in October 2020.[10] A reason for this vast difference in outcomes could be attributed to the steps taken to control the spread COVID-19. Although 81% of Americans own smartphones,[11] the United States does not have a national exposure notification app,[12] and individual states vary in their contact tracing methods.[13] Although the digital contact tracing initiatives taken overseas intrude into the freedom of citizens far more than would be allowed under U.S. law, this paper argues that there is a lawful path through the COVID-19 pandemic that utilizes digital contact tracing.

This paper will look at the digital contact tracing efforts implemented by other nations and assess how similar measures could operate under enacted and proposed United States laws. Part I will overview the history of contact tracing and its effectiveness in prior disease outbreaks. Part II will delve into the digital contact tracing efforts implemented by South Korea and Singapore. These summaries will include: the digital contact tracing efforts taken, the laws that authorize these efforts, the public's reception, and the overall effectiveness of the efforts. Part III will overview the digital contact tracing efforts in the United States, including proposed legislation aimed at user privacy. This part will focus on two proposed legislations: the Exposure

---

also Coronavirus Disease 2019 (COVID-19) WHO Thailand Situation Report (2020), WORLD HEALTH ORGANIZATION [WHO], HTTPS://WWW.WHO.INT/DOCS/DEFAULT-SOURCE/SEARO/THAILAND/2020-03-19-THA-SITREP-26-COVID19.PDF?SFVRSN=6F433D5E_2 (last visited Dec. 13, 2020) (explaining the meaning of "flattening the curve").

[10] Global Epidemic Situation, WORLD HEALTH ORGANIZATION [WHO], https://www.who.int/docs/default-source/coronaviruse/situation-reports/20201012-weekly-epi-update-9.pdf (last visited Nov 28, 2020); *See id.* (reporting a cumulative death toll of 212,229 in the United States, but only 432 and 27 in South Korea and Singapore, respectively.)

[11] *Demographics of Mobile Device Ownership and Adoption in the United States*, PEW RESEARCH CENTER: INTERNET, SCIENCE & TECH, https://www.pewresearch.org/internet/fact-sheet/mobile/ (last visited Nov 28, 2020).

[12] Mitch Leslie, *COVID-19 Fight Enlists Digital Technology: Contact Tracing Apps*, ENGINEERING (BEIJING) (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7492143/ (last visited Nov 28, 2020).

[13] *See* State Approaches to Contact Tracing during the COVID-19 Pandemic – The National Academy for State Health Policy, , https://www.nashp.org/state-approaches-to-contact-tracing-covid-19/, (last visited Nov 28, 2020).

Notification Privacy Act and the Public Health Emergency Privacy Act. Part IV will analyze which provisions of the ENPA and the PHEPA would best restrain the digital contact tracing efforts used in South Korea and Singapore if they were to be implemented in United States. Part V will conclude this note with a final recommendation and recap of the following analysis.

Part I – The History of Contract Tracing

Manual Contact Tracing

Contact tracing is the process of identifying and monitoring people who may have been exposed to someone with an infectious disease, in order to locate other potentially infected individuals.[14] "For a highly contagious respiratory disease such as COVID-19, a contact could be anyone who has been nearby."[15] Traditional contact tracing involves specially trained public health staff helping an infected individual recall everyone they have had close contact with during the time they may have been infectious.[16] Traditional contact tracing is well established[17]. Surveillance and containment programs, such as the Leicester Method, were successful in

[14] 1 1 (July 09, 2020) *COVID-19: Digital Contact Tracing and Privacy Law* 1.

[15] Timothy M. Persons, *Science & Tech Spotlight: Contact Tracing Apps*, U.S. GOV'T ACCOUNTABILITY OFF., https://www.gao.gov/assets/710/708405.pdf (last visited Oct 3, 2020); *see also* Contact Tracing for COVID-19, The Centers for Disease Control and Prevention [CDC]*, supra* note 3, (defining "a close contact for COVID-19 as any individual who was within 6 feet of an infected person for at least 15 minutes starting from 2 days before illness onset (or, for asymptomatic patients, 2 days prior to positive specimen collection) until the time the patient is isolated").

[16] *Coronavirus Disease 2019 (COVID-19)*, CENTERS FOR DISEASE CONTROL AND PREVENTION [CDC] (2020), https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html (last visited Oct 9, 2020).

[17] Persons, *supra* note 15.

identifying cases of Smallpox and quarantining contacts.[18] Contact tracing was not only used[19], but "crucially important" during the SARS outbreak in 2003.[20]

Digital Contact Tracing

Similar tracing efforts, combined with physical distancing and self-isolation, would be likely to achieve control of COVID-19.[21] However, as of June, 2020, only seven states and the District of Columbia have a sufficient contact tracing workforce, and 37 states do not meet the estimated need of contact tracers.[22] This lack of contact tracers can be attributed, in part, to a 28% cut in federal funding and a reduction of 50,000 jobs due to the 2008 recession.[23] Also as of June 2020, many states are relying on the National Guard or volunteers to fill the gap.[24] Digital contact tracing (DCT) is the use of technology, such as smart phones, to aid in the manual contact tracing workflow. Digital contact tracing has the potential to address this shortage of

[18] F. Fenner, D. A. Henderson, I. Arita, Z. Jezek, I. D. Ladnyo, *Smallpox and its Eradication* , 275, 493 - 515 (World Health Organization, 1988). (describing the essentials [of the Leicester Method] as being the prompt notification of cases, the isolation of those cases in a hospital, and quarantine of all immediate contacts).

[19] Christl A. Donnelly et al., *Epidemiological determinants of spread of causal agent of severe acute respiratory syndrome in Hong Kong*, 361 THE LANCET 1761–1766 (2003).

[20] Kin On Kwok et al., *Epidemic Models of Contact Tracing: Systematic Review of Transmission Studies of Severe Acute Respiratory Syndrome and Middle East Respiratory Syndrome*, 17 COMPUT STRUCT BIOTECHNOL J 186–194 (2019).

[21] Adam J. Kucharski et al., *Effectiveness of isolation, testing, contact tracing, and physical distancing on reducing transmission of SARS-CoV-2 in different settings: a mathematical modelling study*, 20 THE LANCET INFECTIOUS DISEASES 1151–1160 (2020).

[22] Selena Simmons-Duffin, As States Reopen, Do They Have The Workforce They Need To Stop Coronavirus Outbreaks?, NPR.ORG, (June 18, 2020), https://www.npr.org/sections/health-shots/2020/06/18/879787448/as-states-reopen-do-they-have-the-workforce-they-need-to-stop-coronavirus-outbre (last visited Oct 10, 2020); *see also* Fitzhugh Mullan Institute for Health Workforce Equity, *GWU Contact Tracing Workforce Estimator*, https://www.gwhwi.org/estimator-613404.html (last visited Oct. 12, 2020).

[23] Crystal Watson et al., *A National Plan to Enable Comprehensive COVID-19 Case Finding and Contact Tracing in the US*, Association of State and Territorial Health Officials [astho], 8.

[24] Simmons-Duffin, *supra* note 22.

manual contact tracing by creating a system that would automatically notify individuals who are potentially exposed to an infected person [25]

Digital contact tracing enables more efficient tracing of those infected and notification to those at-risk.[26] DCT can be implemented through a variety of technologies.[27] The major system adopted in the U.S. and Europe is called "exposure notification," a term created by Google and Apple to distinguish their system from direct contact tracing. Exposure notification has gained significant traction in some countries throughout the current COVID-19 pandemic. Google and Apple have even collaborated on an exposure notification system so users of their phones may be quickly notified of a possible exposure.[28] The advantages of exposure notification is that it works even if the user does not know they were exposed or by whom they were exposed.[29] Exposure notification utilizes Bluetooth, Global Positioning System (GPS), or both.[30] However, the Google/Apple system uses only Bluetooth.[31]

---

[25] CDC, *supra* note 16.

[26] CQ Roll Call Staff, *Digital contact tracing needs strong privacy laws Lowenstein attorney says*, ROLL CALL WASHINGTON DATA PRIVACY BRIEFING (2020)

[27] *See* astho, *supra* note 7. (describing multiple technologies for enhancing manual contact tracing).

[28] *Exposure Notifications: Helping fight COVID-19*, EXPOSURE NOTIFICATIONS: HELPING FIGHT COVID-19 - GOOGLE, https://www.google.com/intl/en_us/covid19/exposurenotifications/ (last visited Nov 15, 2020). (describing Google Apple Exposure Notifications as "a joint effort between… [the companies]… to enable Bluetooth technology to help governments reduce the spread of Covid-19); *See also Exposure Notifications Frequently Asked Questions*, APPLE | GOOGLE, https://www.blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf (last visited Sep 29, 2020).

[29] astho, *supra* note 7.

[30] *Id.* at page 6.

[31] Exposure_Notification_-_FAQ_v1.1.pdf, *supra* note 28.

Early in the COVID-19 pandemic, a range of DCT tools were being developed.[32] Several of these proposed to use either GPS alone or in combination with Bluetooth technology.[33]

Bluetooth allows electronic devices, such as cell phones, to connect to one another using short-range radio waves.[34] For contact tracing purposes, these radio waves would measure the distance between Bluetooth enabled devices and notify the users if two signals come close enough together.[35] Most phones sold today, including some non-smartphones,[36] have Bluetooth capabilities.[37] The breadth of this technology makes Bluetooth-based exposure notification an obvious contact tracing supplement.[38] However, Bluetooth technologyis not a perfect solution. Bluetooth signals can be unreliable in measuring distance[39] and requires users to have their

[32] Demonstrating 15 contact tracing and other tools built to mitigate the impact of COVID-19, , TECHCRUNCH , https://social.techcrunch.com/2020/06/05/demonstrating-15-contact-tracing-and-other-tools-built-to-mitigate-the-impact-of-covid-19/ (last visited Nov 19, 2021). *See also* Digital tools for COVID-19 contact tracing, WORLD HEALTH ORGANIZATION, https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1 (last visited Nov 19, 2021). Table 1 details how proximity tracing / tracking tools can use GPS or Bluetooth, as well as the consideration for implementation. *Id.*

[33] *Id*. *See also* Muhammad Shahroz et al., *COVID-19 digital contact tracing applications and techniques: A review post initial deployments*, 5 TRANSPORTATION ENGINEERING 100072 (2021).

[34] Jeanette Ferrara, *How do Bluetooth devices work?*, SCIENCELINE (2016), https://scienceline.org/2016/04/how-do-bluetooth-devices-work/ (last visited Feb 15, 2021).

[35] Patrick Howell O'Neill, *Bluetooth contact tracing needs bigger, better data*, MIT TECHNOLOGY REVIEW, https://www.technologyreview.com/2020/04/22/1000353/bluetooth-contact-tracing-needs-bigger-better-data/ (last visited Feb 15, 2021).

[36] Jon Stone, *The Best Non-Smartphones for 2020: Which Should You Buy?*, THE INFORMR (2011), https://theinformr.com/cell-phones/p/best-basic-phone-10094/ (last visited Feb 15, 2021).

[37] Mike Chaussee, *Does My Cell Phone Have Bluetooth?*, ND ASSISTIVE (2014), https://ndassistive.org/blog/does-my-cell-phone-have-bluetooth/ (last visited Feb 15, 2021).

[38]*See generally* S. O'Dea, *Smartphone users 2020*, STATISTA , https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (last visited Feb 15, 2021) (noting that smartphone users surpass three billion, with some countries over 100 million).

[39] O'Neill, *supra* note 31.

phone turned on (and on their person) at all times.[40] Bluetooth also requires the user to install third-party applications onto their device to utilize this method.[41] The third-party application is required to provide the key location and time information that Bluetooth does not collect.

GPS information collection is another contact tracing technique. GPS is a system of satellites, owned by the U.S. government, that send signals to receivers on Earth to determine the receiver's location.[42] For contact tracing purposes, GPS offers several advantages over Bluetooth. First, a third-party application would not be required to collect the time and location data mentioned above.[43] Also, GPS location information can be used to track the movements of infected users and ensure user compliance with quarantine measures.[44] Further, GPS is globally available and is present on modern smartphones.[45]

Combining the advantages of both Bluetooth and GPS technologies could provide much of the information needed to aid manual contact tracers. Utilizing Bluetooth would alert a user if they were in close proximity of an infected individual. Consensually given user GPS data can show where an infected user has been and at what times. This would allow contact tracers to alert

[40] CDC, *Health Departments*, CENTERS FOR DISEASE CONTROL AND PREVENTION (2020), https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/contact-tracing.html (last visited Dec 13, 2020).

[41] *Id.*

[42] GPS.gov: GPS Overview, https://www.gps.gov/systems/gps/ (last visited Feb 15, 2021). *See also* How Does GPS Work? | NASA Space Place – NASA Science for Kids, https://spaceplace.nasa.gov/gps/en/ (last visited Feb 15, 2021).

[43] Using contact tracing and GPS to fight spread of COVID-19, , GPS WORLD (2020), https://www.gpsworld.com/using-contact-tracing-and-gps-to-fight-spread-of-covid-19/ (last visited Nov 19, 2021).

[44] Mobile Location Data and Covid-19: Q&A, HUMAN RIGHTS WATCH (2020), https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa (last visited Feb 15, 2021).

[45] Shahroz et al., *supra* note 33.

businesses or other public gathering places of the infected user's presence.[46] This information could also be uploaded to contact tracing applications to alert other users who may have been at that the same location at the same time, but who may not have come into close proximity of the infected individual.

Countries that use Bluetooth notification or GPS information in their contact tracing efforts have to choose how the data collected will be stored. This data can be stored on servers usually controlled by the government (centralized), or on the individual users device (decentralized). "The primary difference between centralized and decentralized communication networks has to do with the question of who has control over the network itself."[47] In a centralized method, for Bluetooth and GPS, user information is stored on the server owned by the government[48] or some other authority.[49] Although this data is anonymized, there is potential for misuse.[50] Countries that have used centralized methods of storage have come under fire because of its privacy invasive nature.[51] A decentralized system, however, provides enhanced

---

[46] *See* Vesedia proposes COVID-19 contact tracing platform, , GPS WORLD (2020), https://www.gpsworld.com/vesedia-proposes-covid-19-contact-tracing-platform/ (last visited Nov 19, 2021). Tracing

[47] Alan Seal, *Centralized vs Decentralized Network: Which One Do You Need?*, https://www.vxchnge.com/blog/centralized-decentralized-network (last visited Dec 12, 2020).

[48] Cristina Criddle & Leo Kelion, *Coronavirus contact-tracing: World split between two types of app*, BBC NEWS, May 7, 2020, https://www.bbc.com/news/technology-52355028 (last visited Feb 15, 2021).

[49] Dong Wang & Fang Liu, *Privacy Risk and Preservation For COVID-19 Contact Tracing Apps* 10. China's Alipay Health Code assigns users a status based on their GPS location. *Id.* Users who have been to a COVID-19 hotspot are assigned a red code, indicating a 2 week quarantine. *Id.*

[50] Joseph Duball, *Centralized vs. decentralized: EU's contact tracing privacy conundrum*, https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/ (last visited Feb 15, 2021). (theorizing a "social graph" that could be created through the information collected).

[51] Bahrain, Kuwait and Norway contact tracing apps a danger for privacy, https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/ (last visited Oct 22, 2020). *see also* Hermesauto, *Norway halts coronavirus tracking app over privacy*

privacy[52] because all the data collected is stored on the user's device, not on a central database accessible by the government.[53] In a Bluetooth notification system, the individual devices periodically download the anonymous identifiers of COVID-19 positive users. If the device has come within range of one of these COVID-19 positive identifiers, the user will be alerted of the potential exposure.[54] In a decentralized GPS model, users track their own location, and will only upload an anonymized report upon a positive COVID-19 diagnosis.[55] In this model, the user must also consent before any information is reported.[56]

Models suggest that sixty percent population use of a digital contact tracing app can "substantially reduce" the spread of COVID-19.[57] Most nations have yet to reach that amount of participation.[58] However, Professor Fraser at Oxford University says that all levels of exposure

concerns, THE STRAITS TIMES (2020), https://www.straitstimes.com/world/europe/norway-halts-coronavirus-tracking-app-over-privacy-concerns (last visited Oct 2, 2020) (stating that the Norwegian government halts its contact tracing app amid privacy concerns).

[52] astho, *supra* note 7.

[53] Diana Plutis and Jaime-Heather Schwartz, *When it comes to COVID tracing apps a decentralized model is preferred*, AVIRA BLOG (2020), https://www.avira.com/en/blog/when-it-comes-to-covid-tracing-apps-the-decentralized-model-is-preferred (last visited Feb 15, 2021).

[54] Cristina Criddle & Leo Kelion, *supra* note 39. *See also* EXPOSURE NOTIFICATIONS: HELPING FIGHT COVID-19 - GOOGLE, *supra* note 28.

[55] Wang and Liu, *supra* note 49.

[56] *Id.*

[57] Univ. of Oxford, *Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown* (2020), https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown (last visited Oct 9, 2020) (modeling that approximately 60% of the whole population using the application and adhering to the application's recommendations can stop the epidemic. Lower numbers of app users will also have a positive effect; we estimate that one infection will be averted for every one to two users").????some of this is quoted, but where does the quote start?

[58] Craig Timberg et al., *Cellphone apps designed to track covid-19 spread struggle worldwide amid privacy concerns*, WASHINGTON POST, https://www.washingtonpost.com/technology/2020/08/17/covid-tracking-apps-cellphones/

notification use can reduce the number of cases.[59] Fraser's estimates show that even 15% participation, combined with a well-staffed manual contact tracing workforce, could reduce infections by 15% and deaths by 11%.[60]

Part II – Digital Contact Tracing in East Asia

A. South Korea

i. Tools Used

South Korea has implemented their Epidemic Investigation Support System (EISS) for faster processing of patient data to better track infected Koreans.[61] The EISS, for COVID-19 contact tracing purposes, now compiles cell phone location and credit card data to more accurately determine if an infected individual's travels resulted in social activity.[62] For example, the EISS was able to track an individual moving between a number of nightclubs and bars while infected.[63]

(last visited Sep 29, 2020) (reporting that Ireland had 26 percent participation, Switzerland had 23 percent participation, and France had only 68 people use their app to report a positive COVID-19 test in the first 3 weeks).

[59] Univ. of Oxford, *New research shows tracing apps can save lives at all levels of uptake*, NEWS & EVENTS, https://www.ox.ac.uk/news/2020-09-03-new-research-shows-tracing-apps-can-save-lives-all-levels-uptake (last visited Oct 9, 2020).

[60] *Id.*

[61] Young Joon Park et al., *Development and Utilization of a Rapid and Accurate Epidemic Investigation Support System for COVID-19*, 11 OSONG PUBLIC HEALTH RES PERSPECT 118–127 (2020).

[62] *Id.* at 121 – 22. "After the entry of the confirmed COVID-19 case information, an epidemic investigator requests the case information required for tracking via the system. As for information from the mobile network companies, a corresponding request goes through the approval procedure via the Police Department. For card usage information, the Credit Finance Association identifies the cards that the confirmed case in question possesses, followed by a request to the corresponding credit card companies for information." *Id*.

[63] Hyonhee Shin, Hyunjoo Jin, Josh Smith, *How South Korea turned an urban planning system into a virus tracking database*, REUTERS, May 22, 2020, https://www.reuters.com/article/us-health-coronavirus-southkorea-tracing-idUSKBN22Y03I (last visited Nov 15, 2020).

South Korea is also using apps to keep in touch with infected individuals.[64] The Corona 100m (Co100) application can allow infected individuals to stay in touch with case workers and can alert them if they come within 100 meters of a location visited by an infected person.[65] Websites such as *coronamap.site* map positive COVID-19 diagnoses to help users avoid areas that have been visited by other infectious users .[66] A second application also uses GPS to ensure the user does not break quarantine.[67] The rate of smartphone use among Korean adults is 95%, almost 20% more than the global median.[68] South Korea's comparatively low infection rate is likely the result, in part, because of this high rate of smart phone usage combined with the EISS and other technological combatants.[69]

---

[64] Sarah Wray, *South Korea to step-up online coronavirus tracking*, SMART CITIES WORLD, https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109 (last visited Nov 22, 2020).

[65] *Id.*

[66] Mark Zastrow, *South Korea is reporting intimate details of COVID-19 cases: has it helped?*, NATURE (2020), https://www.nature.com/articles/d41586-020-00740-y (last visited Oct 9, 2020).

[67] Wray, *supra* note 39. *See also* South Korea is watching quarantined citizens with a smartphone app, , MIT TECHNOLOGY REVIEW , https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/ (last visited Dec 10, 2020). The "self-quarantine safety protection" app was created by the Ministry of Interior and Safety. *Id.*

[68] Laura Silver, *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*, PEW RESEARCH CENTER'S GLOBAL ATTITUDES PROJECT (2019), https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/ (last visited Nov 15, 2020). (reporting that nearly 100% of Korean adults have a mobile phone when non-smartphones are included).

[69] Ministry of Health and Welfare, *Coronavirus Disease-19, Republic of Korea*, CORONAVIRUS DISEASE 19(COVID-19) , http://ncov.mohw.go.kr/en/ (last visited Nov 15, 2020).

ii. Legal Authority

South Korea's Location Information Act protects from misuse of location information.[70] Article 15 subsection 1 of the Act states, "No one shall collect, use, or provide the location information regarding an individual or mobile object without the consent of the individual or the owner of the mobile object… unless otherwise provided in other Acts."[71] The Infectious Disease Control and Prevention Act overrides the Location Information Act through articles outlining the epidemiological investigation conducted during an infectious disease outbreak.[72]

iii. Reception and Effectiveness

The intrusive surveillance implemented by the South Korean government has drawn criticism and has been seen as violating basic human rights.[73] The personal data revealed by the South Korean government, although vague, has led to users identities being discovered.[74] This surveillance is especially concerning to South Korea's LGBTQ community.[75] A COVID-19

---

[70] Act on the Protection, Use, Etc. of Location Information, art. 1 (S. Kor.), *translated in* Korean Law Translation Center, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=43349&lang=ENG (last visited Nov 15, 2020).

[71] *Id.* art. 29 (noting that emergency rescue agencies or police agencies may receive this information).

[72] Sayuri Umeda, *Regulating Electronic Means to Fight the Spread of COVID-19* (2020), https://www.loc.gov/law/help/coronavirus-apps/korea.php#_ftnref23 (last visited Nov 15, 2020) (outlining the details, timing, methods, and composition of epidemiological investigations and investigation teams).

[73] Press Releases | National Human Rights Commission of Korea, https://www.humanrights.go.kr/site/program/board/basicboard/view?boardtypeid=7003&boardid=7605315&menuid=002002001 (last visited Feb 13, 2021).

[74] Nemo Kim in Seoul, *"More scary than coronavirus": South Korea's health alerts expose private lives*, THE GUARDIAN (2020), http://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives (last visited Nov 22, 2020).

[75] *See* Jason Strother, *South Korea's coronavirus contact tracing puts LGBTQ community under surveillance, critics say*, THE WORLD FROM PRX , https://www.pri.org/stories/2020-05-22/south-korea-s-coronavirus-contact-tracing-puts-lgbtq-community-under-surveillance (last visited Nov 22, 2020).

outbreak in May 2020 had been linked to the Itaewon district, a LGBTQ friendly area.[76] The community is now facing heightened discrimination following the source of the outbreak being described as a "gay club."[77] Despite these concerns, over 63% of South Koreans are satisfied with their governments COVID-19 response.[78] Despite the privacy intrusions, South Korea has been successful in managing COVID-19. South Korea has had 300 times fewer cases than the United States[79] and has only had 1,553 deaths due to the virus as of February 20, 2021.[80]

B. Singapore

i. Tools Used

Singapore was the first government to release a DCT app[81] when it debuted it's "TraceTogether" program on March 20, 2020.[82] The program uses Bluetooth signals to record

[76] *Id.*

[77] Ryan Thoreson, *Covid-19 Backlash Targets LGBT People in South Korea*, HUMAN RIGHTS WATCH (2020), https://www.hrw.org/news/2020/05/13/covid-19-backlash-targets-lgbt-people-south-korea (last visited Nov 22, 2020).

[78] Timothy S. Rich, Madelynn Einhorn, Andi Dahmer, and Isabel Eliassen, *What Do South Koreans Think of Their Government's COVID-19 Response?*, https://thediplomat.com/2020/10/what-do-south-koreans-think-of-their-governments-covid-19-response/ (last visited Nov 22, 2020).

[79] Wudan Yan and Ann Babe, *What Should the U.S. Learn from South Korea's Covid-19 Success?*, UNDARK MAGAZINE (2020), https://undark.org/2020/10/05/south-korea-covid-19-success/ (last visited Nov 22, 2020).

[80] South Korea Coronavirus: 30,733 Cases and 505 Deaths, WORLDOMETER, https://www.worldometers.info/coronavirus/country/south-korea/ (last visited Nov 22, 2020).

[81] *Singapore distributes Covid contact-tracing tokens*, BBC NEWS (September 14, 2020), https://www.bbc.com/news/business-54143015 (last visited Oct 23, 2020).

[82] *What is the TraceTogether Programme? How is it different from the TraceTogether App?*, TRACETOGETHER FAQS , https://support.tracetogether.gov.sg/hc/en-sg/articles/360053530773 (last visited Oct 23, 2020).

encounters between devices.[83] TraceTogether uses the BlueTrace Protocol.[84] This protocol helps blend decentralized and centralized methods of contact tracing by protecting the users information from third-parties, but also allowing a centralized authority to access the information to identify close-contacts.[85] Alongside the smartphone application, this program introduced what is called a "TraceTogether Token".[86] The TraceTogether Token is a piece of hardware that works just like the smartphone application, minus the smartphone.[87] Both the application and Token capture proximity data through Bluetooth, not GPS.[88] This proximity data is encrypted,[89] stored on the user's device [smartphone or Token], "and only shared with the Ministry of Health (MOH) if a user tests positive for COVID-19".[90] This information is deleted off of the user's phone after 21 days.[91] Although the proximity data is stored on the user's phone, limited identifiable information is stored on government servers.[92] This identifiable information includes

---

[83] *What is the difference between the TraceTogether App and TraceTogether Token? Why can't we have a one-stop portable device or application for contact tracing?*, TRACETOGETHER FAQS , https://support.tracetogether.gov.sg/hc/en-sg/articles/360053530813 (last visited Oct 23, 2020).

[84] *What is BlueTrace?*, TRACETOGETHER FAQS, https://support.tracetogether.gov.sg/hc/en-sg/articles/360044883814 (last visited Nov 8, 2020).

[85] Jason Bay et al., *BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders,* 9.

[86] *What is a TraceTogether Token?*, TRACETOGETHER FAQS, https://support.tracetogether.gov.sg/hc/en-sg/articles/360052534334 (last visited Oct 23, 2020).

[87] BBC NEWS, *supra* note 48.

[88] *How does the TraceTogether Token work and what are its features?*, TRACETOGETHER FAQS, https://support.tracetogether.gov.sg/hc/en-sg/articles/360052536514 (last visited Oct 23, 2020).

[89] *Id.*

[90] *How does the TraceTogether App work?*, TRACETOGETHER FAQS , https://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473 (last visited Oct 23, 2020).

[91] *Id.*

[92] *TraceTogether Privacy Safeguards*, https://www.tracetogether.gov.sg/ common/privacystatement (last visited Oct 23, 2020).

the user's contact number, identification details, and a random, anonymized User ID.[93] Use of the TraceTogether Program [smartphone appplication or Token] was to be mandatory for entrance into public venues by the end of 2020.[94] However, this mandatory check-in program has been pushed back to a date in early 2021 that has yet to be announced.[95]

ii. Legal Authority

As explained above, the BlueTrace Protocol stores encounter history locally, on the user's device.[96] Also, the BlueTrace Protocol white paper explains, "The health authority only has access to this history when an infected person chooses to share it.".[97] However, these descriptions may give a false sense of privacy to the program's users because of the Singaporean government's legal authority to collect health data. If a user is contacted by the MOH, that person is required by law to divulge the information recorded by the TraceTogether Program.[98] The Infectious Disease Act 7(2)(a) states that for the purpose of a public health surveillance program, the Director may require any person to furnish any information known to the person at

---

[93] *Id.*

[94] Lester Wong, *What to expect with mandatory TraceTogether use*, THE STRAITS TIMES (2020), https://www.straitstimes.com/singapore/what-to-expect-with-mandatory-tracetogether-use (last visited Oct 23, 2020). See also *The Multi-Ministry Taskforce on Wuhan Coronavirus*, MINISTRY OF HEALTH SING., https://www.moh.gov.sg/docs/librariesprovider5/default-document-library/multi-ministry-taskforce-on-wuhan-coronavirus-and-tor---final.pdf

[95] Hermesauto, *TraceTogether check-ins not compulsory yet, retailers told after some outlets turn on function too early*, THE STRAITS TIMES (2021), https://www.straitstimes.com/tech/tech-news/tracetogether-check-ins-not-compulsory-yet-retailers-told-after-some-outlets-turn-on (last visited Feb 20, 2021).

[96] How does the TraceTogether App work?, *supra* note 90.

[97] Bay et al., *supra* note 85.

[98] *Can I say no to uploading my TraceTogether data when contacted by the Ministry of Health?*, TRACETOGETHER FAQS, https://support.tracetogether.gov.sg/hc/en-sg/articles/360044860414 (last visited Nov 8, 2020).

those times.[99] If you put together the facts that TraceTogether use will be mandatory in 2021 and the user is required by law to give TraceTogether-collected information to the government when requested, the privacy safeguards touted by the Singaporean government seem a little less authentic.[100] As described above, limited identifiable is kept on "secure," yet centralized government servers, and Bluetooth proximity data is stored on the user's phone until the user receives a positive COVID-19 diagnosis.[101]Although the MOH claims to only access the above data for contact tracing purposes,[102] the Ministry could, in reality, access the data whenever they desire. In fact, the Minister of State for Home Affairs Desmond Tan revealed that this contact tracing information "can also be used for 'the purpose of criminal investigation.'"[103]

It should also be noted that by using TraceTogether, the user agrees to indemnify the Government Technology Agency (GovTech) against any harms suffered either directly or indirectly out of the user's access to or use of TraceTogether.[104] This means that if the user's TraceTogether-collected information is stolen by a third-party, the user has no recourse from the government if they suffer harm from the third-party's use of that data. Although Bluetooth

[99] Infectious Diseases Act, 1976 (Act. No. 137/1076)(Sing.), https://sso.agc.gov.sg/Act/IDA1976 (last visited Nov 8, 2020).

[100] *TraceTogether Privacy Safeguards, supra* note 59

[101] What data is collected? Are you able to see my personal data?, TRACETOGETHER FAQS , https://support.tracetogether.gov.sg/hc/en-sg/articles/360043735693-What-data-is-collected-Are-you-able-to-see-my-personal-data- (last visited Feb 20, 2021).

[102] *Id.*

[103] Singapore reveals Covid privacy data available to police, BBC NEWS, January 5, 2021, https://www.bbc.com/news/world-asia-55541001 (last visited Feb 21, 2021).

[104] *TraceTogether Terms*, https://www.tracetogether.gov.sg/common/terms-of-use/ (last visited Nov 8, 2020).

proximity data itself is harmless, Singapore does have a history of cyber-attacks resulting in the loss of personal data.[105]

iii. Reception and Effectiveness

Although much of the personal information involved is stored on the user's phone and is encrypted, there are still privacy concerns surrounding it. The Singaporean Prime Minister has even acknowledged this when saying, "There will be some privacy concerns, but we will have to weigh these against the benefits of being able to exit from the circuit breaker [Singapore's lockdown measures] and stay open safely."[106] Most of these concerns stem from the fact that some information is kept on a centralized server controlled by the Ministry of Health.[107] Whenever an infected user consents to having his data log decrypted by the MOH, this data log includes the identities of users with whom the infected individual has come into contact.[108] This means that when a user consents to having their data log decrypted, the identities of their contacts are being divulged to the MOH without those contacts' consent and those users are no

[105] Nurfilzah Rohaidi, *Singapore's healthcare system hacked*, GovInsider (2018), https://govinsider.asia/innovation/singapore-healthcare-system-hack-singhealth-csa-moh/ (last visited Feb 20, 2021). A 2018 hack resulted in the access 1.5 million patients personal data. *Id.*

[106] *Contact tracing apps: A new world for data privacy*, Norton Rose Fulbright , https://www.nortonrosefulbright.com/en-sg/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy (last visited Nov 8, 2020).

[107] *Contact tracing apps in Singapore*, Norton Rose Fulbright, https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/singapore-contact-tracing.pdf?la=en-za&revision= (last visited Nov 8, 2020).

[108] Hassan Asghar & Dali Kaafar, *On the Privacy of TraceTogether, the Singaporean COVID-19 Contact Tracing Mobile App and Recommendations for Australia,* 4.

longer in control of their privacy.[109] There is also pushback against the TraceTogether Token.[110] A petition on Change.org has amassed over 54,000 signatures opposing the development of a wearable contact tracing device.[111] The petition claims that a mandatory contact tracing device is an infringement upon their privacy rights and has the potential to turn Singapore into a surveillance state.[112] This claim is based on the belief that a wearable contact tracing device, such as the Token, "would allow contact tracers to locate a person's whereabouts based on their proximity to other persons' phones, cell towers, or potentially their wearable devices themselves."[113]

The claims of this petition are unfounded. In reality, the wearable device being pushed by the Singaporean government does not collect geolocation data, nor does it have internet or cellular connectivity.[114] GovTech even invited members of the community to inspect the TraceTogether Token.[115] An inspection of the Token's hardware revealed a small battery that cannot be charged.[116] Such a battery would last only a few hours if it were using GPS or Wi-Fi

[109] *Id.*

[110] Sign the Petition, CHANGE.ORG, https://www.change.org/p/singapore-government-singapore-says-no-to-wearable-devices-for-covid-19-contact-tracing (last visited Nov 8, 2020).

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] How does the TraceTogether Token work and what are its features?, *supra* note 88.

[115] *Trace Together Token: Teardown and Design Overview*, XOBS' BLOG (2020), https://xobs.io/trace-together-token-teardown/ (last visited Nov 8, 2020).

[116] *Id.*

communication.[117] Given the Token is supposed to run for several months on a single battery, it is unlikely a GPS tracker, Wi-Fi radio, or cellular modem could be hidden in the device.[118]

TraceTogether had over one million users in April 2020. [119] Although an impressive number, this means that in a random encounter between two people, there is only a 4% chance that both people will have the application.[120] Usage had doubled by September 2020, with over 2.4 million downloads, or 40% of Singapore's population.[121] By January 2021, usage had again almost doubled to 78% participation, or more than 4.2 million people.[122]

Part III – Digital Contact Tracing in the United States

Through the first six months of the COVID-19 pandemic, most states did not utilize a contact tracing application.[123] Although usage had increased by the end of 2020, only twenty-seven jurisdictions had implemented some form of a contact tracing application.[124] In these

[117] *Id.*

[118] *Id.*

[119] *COVID-19 digital apps need due diligence*, 580 Intl. J. Sci. NATURE 563–563 (2020).

[120] *Id.*

[121] Hariz Baharudin, *Distribution of TraceTogether tokens starts; aim is for 70% participation in contact tracing scheme*, THE STRAITS TIMES (2020), https://www.straitstimes.com/singapore/government-aiming-for-70-participation-in-tracetogether-programme-says-vivian-on-first-day (last visited Nov 8, 2020).

[122] Tham Yuen-C , *Over 4.2 million, or 78% of residents, using TraceTogether*, THE STRAITS TIMES (2021), https://www.straitstimes.com/singapore/politics/over-42-million-or-78-of-residents-using-tracetogether (last visited Feb 21, 2021).

[123] Ben Lovejoy, *US contact tracing apps still a mess, despite Apple's efforts*, 9TO5MAC (2020), https://9to5mac.com/2020/10/22/us-contact-tracing-apps/ (last visited Dec 4, 2020) (stating that, as of October 27th, 2020, 27 states had yet to adopt a contact tracing app).

[124] Dmitry Parshin, *Contact tracing apps now cover nearly half of America. It's not too late to use one*., MIT TECHNOLOGY REVIEW , https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/ (last visited Feb 27, 2021). *see also* Mishaal Rahman, *List of countries using Google and Apple's*

jurisdictions, the Exposure Notification System by Google and Apple, Inc. (GAEN), is most prevalent.[125] A national server, which stores exposure notification information from all states using GAEN, has also been established so individual state applications can work together.[126] Although the GAEN framework makes privacy a priority,[127] many people are "unable" to utilize the technology because they do not have a smartphone, or are "unwilling to use the technology."[128] A poll by the University of Maryland suggests that of the 82% of smartphone users, only half would use an anonymous Google/Apple smartphone application.[129] This lack of participation could also be attributed to the lack of trust the American people have in the government and big technology companies ("Big Tech").[130]

Notwithstanding many Americans' concerns, studies show that there are enough Americans willing to use contact tracing applications to have a meaningful effect on the spread of COVID-19.[131] However, because of the states slow roll out of digital contact tracing programs,

---

COVID-19 Contact Tracing API, XDA-DEVELOPERS (2020), https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/ (last visited Dec 6, 2020).

[125] Parshin, *supra* note 118.

[126] Sara Morrison, *Americans are one step closer to a national contact tracing app for Covid-19*, VOX (2020), https://www.vox.com/recode/2020/10/2/21497729/covid-coronavirus-contact-tracing-app-apple-google-exposure-notification (last visited Feb 27, 2021).

[127] Gregory Barber and Will Knight, *Why Contact-Tracing Apps Haven't Slowed Covid-19 in the US*, WIRED, https://www.wired.com/story/why-contact-tracing-apps-not-slowed-covid-us/ (last visited Dec 6, 2020).

[128] Sara Gavin, *Disinclined to Download*, THE UNIV. OF MARYLAND TODAY , https://today.umd.edu/articles/disinclined-download-1fdd9ef1-cf1d-42ac-8f23-971fbeb6aa91 (last visited Dec 6, 2020).

[129] Center for Democracy and Civic Engagement Contact Tracing App Poll, THE WASHINGTON POST (2020).

[130] Alejandro De La Garza, *Why Aren't Contact Tracing Apps Working?*, TIME , https://time.com/5905772/covid-19-contact-tracing-apps/ (last visited Feb 27, 2021). See also *Survey says majority of Americans won't use COVID-19 contact-tracing apps*, HEALTHCARE IT NEWS (2020), https://www.healthcareitnews.com/news/survey-says-majority-americans-wont-use-covid-19-contact-tracing-apps (last visited Oct 2, 2020).

[131] Univ. of Oxford, *supra* note 53.

and the above-mentioned distrust of the government and Big Tech, a federal effort restrained by legislation should be implemented to control the pandemic in the United States.

Section 2 of this Note shows that the comprehensive government strategies in South Korea and Singapore have been effective in controlling COVID-19. However, such invasive efforts would infringe on the rights of United States citizens. Therefore, regulatory restrictions would be necessary to implement such efforts. Two potential bills could provide the regulation necessary: the Exposure Notification Privacy Act (ENPA) and the Public Health Emergency Privacy Act (PHEPA).

A. Proposed Legislation

i. Exposure Notification Privacy Act (ENPA)

The "Exposure Notification Privacy Act" (ENPA) was introduced on June 1, 2020, by Senator Maria Cantwell of Washington State and Senator Bill Cassidy of Louisiana.[132] Enforceable by the Federal Trade Commission, this Act focuses on regulating entities that operate an "automated exposure notification service" and establishing privacy requirements for those operators.[133] An "automated exposure notification service" (AENS) is described in this Act as "a website, online service, online application, mobile application, or mobile operating system … that is designed, in part or in full, … for, the purpose of digitally notifying, in an automated

[132] Exposure Notification Privacy Act [ENPA], S. Res. S.3861, 116th Cong. (2020).

[133] *See Id*. at § 1,10 (2020).

manner, an individual who may have become exposed to an infectious disease ….[134] This means the ENPA would govern contact tracing applications, such as the Google/Apple framework.[135]

Section 3 of the ENPA focuses on gaining the public's trust in automated exposure notification services. This section provides that an operator of an AENS shall "collaborate" with public health authorities.[136] Although "collaborate" is not defined in the Act, Section 5(b)(2) allows operators of an AENS (an operator) to transfer covered data to a public health authority (PHA) "for public health purposes related to an infectious disease".[137] Section 3 next prevents AENS from processing any user's actual, potential, or presumptive diagnosis of an infectious disease unless that diagnosis is "authorized."[138] Section 2 defines an "authorized diagnosis" as a diagnosis that is confirmed by a PHA or a licensed health care provider.[139] Section 3 then requires an operator to publish guidance on their service functions, how to interpret notifications, and any limitations on the service's accuracy or reliability of exposure risk.[140] Lastly, Section 3 deems it unlawful for an operator to engage is any deceptive act concerning an AENS and

[134] ENPA. at § 2.

[135] List of countries using Google and Apple's COVID-19 Contact Tracing API, *supra* note 124 (stating twenty-one states, the District of Columbia, and the territories of Guam and Puerto Rico are currently using contact tracing apps based off of the GAEN framework).

[136] ENPA, *supra* note 128. at § 3.

[137] *Id.* at § 2, 5.

[138] *Id.* at § 3.

[139] *Id.* at § 2.

[140] *Id.* at § 3.

requires service providers to notify an operator or a PHA when it has knowledge of a potential violation.[141]

Section 4 of the ENPA focuses on ensuring voluntary user participation and transparency in how an operator uses a user's data.[142] This section first requires "prior affirmative express consent" before an individual may be enrolled in an AENS.[143] This section also gives the user the power to determine whether the AENS processes their authorized diagnosis.[144] This means that even if an individual consensually enrolls in an AENS, the individual, who has received a positive diagnosis, could choose to not have other users alerted of that diagnosis. Even if an individual provides their consent to enroll in an AENS, the ENPA requires an operator to provide to the individual "a clear and conspicuous means to withdraw" their affirmative express consent of enrollment.[145]

Section 4 also requires an operator to make publicly available a privacy policy detailing how the operator will collect, process, and transfer an individual's covered data.[146] This privacy policy shall include: the operators identity and contact information, the processing purpose for which covered data is collected, whether that data is transferred, the operator's data minimization

---

[141] *Id.* (stating Section 2 of the ENPA defines a "service provider" as an entity that processes data for an operator or PHA for the performance of an automated exposure notification service).

[142] *Id.* at § 4.

[143] *Id. see also Id.* at § 2 (defining "affirmative express consent" as "an affirmative act by an individual that clearly communicates the individual's authorization for an act or practice…"). Does this need to be cited?

[144] *Id.* at § 4.

[145] *Id.*

[146] *Id. see also Id.* at § 2 (defining "covered data" as "any information that is linked or reasonably linkable to an individual…"). Does this need to be cited?

and retention policies, how an individual can exercise their rights under the ENPA, the operator's data security policies, and the privacy policies effective date.[147] This section also requires that the privacy policy be made available in all languages of the people to whom the AENS is provided.[148]

Section 5 of the ENPA focuses on restricting the amount of data an AENS can collect and how that data is used after collection.[149] First, the section prohibits an operator from collecting or processing any covered data beyond what is necessary for the implementation of the AENS for public health purposes.[150] An operator is also restricted from collecting data for any "commercial purpose."[151] Next, this section restricts operators from transferring any covered data, with exceptions.[152] These exceptions allow an operator to transfer covered data to notify an enrolled individual of a potential exposure, to a PHA for "purposes related to an infectious disease," or to a service provider for system maintenance or incident response.[153] There is also an exception for data transfers that are required for the operator to comply with a legal claim.[154]

---

[147] *Id.* at § 4.

[148] *Id.*

[149] *Id.* at § 5.

[150] *Id.*

[151] *Id.* "Commercial purpose" is not defined within Section 2 of the ENPA.

[152] *Id.*

[153] *Id.* "Purposes related to an infectious disease" is not defined within Section 2 of the ENPA and begs the question of what circumstances would allow an operator to transfer information to a PHA, and whether consent is necessary from the individual from whom the data was collected. Does this need to be cited?

[154] *Id.*

The section then continues to restrict the transfer of data, deeming it unlawful for any entity, including Executive agencies, to transfer covered data unless it "is transferred in connection with an investigation or enforcement proceeding…"[155] The section then singles out Executive agencies, prohibiting them from processing or transferring covered data unless it is "for a public health purpose related to an infectious disease" or "in connection with an investigation or enforcement proceeding…"[156] Lastly, the Section allows data collection, processing, or transfers for applicable research purposes, one of which being for "development…of a…vaccine that relates to an infectious disease.[157]

Section 6 allows an individual to delete, or requires an operator to delete all covered data of an individual, upon the request of the individual.[158] This section also requires an operator to delete an individual's data within 30 days of receiving it.[159] Operators also have to instruct their service providers to delete covered data in accordance with this section.[160] As in Section 5, there is an exception for applicable research purposes.[161]

---

[155] *Id.*

[156] *Id.* ENPA Section 5(c)(2)(B) is redundant with Section 5(c)(1), and Section 5(c)(2)(A) fails to specify what a "public health purpose related to an infectious disease" is. Also, the Section fails to explain or limit to "*whom"* an Executive agency may transfer covered data. Does this need to be cited?

[157] *Id.* Section 5(d) allows data collection, processing, or transfers for research conducted pursuant to 45 C.F.R. § 46 and 21 C.F.R. § 50. Does this need to be cited?

[158] *Id.* at § 6.

[159] *Id.* The deletion of an individual's data within 30 days of receipt can occur on a rolling basis or at times consistent with a PHA published standard. *Id.*

[160] *Id.*

[161] *Id.*

Section 7 requires operators of an AENS to "establish, implement, and maintain data security practices" to protect covered data.[162] Such practices must include: (1) risk and vulnerability assessment, (2) preventative and corrective action to mitigate such risks and vulnerabilities, and (3) adequate notifications to individuals and law enforcement when a data breach occurs.[163] This section requires that the above data security practices "be consistent with standards generally accepted by experts in the information security field."[164] Lastly, this section makes it unlawful for "any person or entity to transmit signals with the intent to cause an automated exposure notification service to produce inaccurate notifications or to otherwise interfere with the intended functioning of such a service."[165]

Section 8 makes unlawful the segregation or discrimination of an individual "based on covered data collected or processed through an automated exposure notification service (AENS).[166] This section also makes unlawful the segregation or discrimination of any individual based on whether or not that individual uses an AENS.[167]

Section 9 amends Section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 to add language regarding responses to health epidemics.[168] These amendments include

---

[162] *Id.* at § 7.

[163] *Id.*

[164] *Id.* This standard would likely become relevant when a data breach occurs regarding covered data held by an operator of an AENS. *Id.*

[165] *Id.* Section 2 of the ENPA does not define "signals." Also note that intent is required to be found in violation of this section. Does this need to be cited?

[166] *Id.* at § 8.

[167] *Id.*

[168] *Id.* at § 9.

mandatory reports "assessing the impact on privacy and civil liberties of Government activities in response to the public health emergency related to the Coronavirus 2019 (COVID-19)".[169]

ii. Public Health Emergency Privacy Act (PHEPA)

The "Public Health Emergency Privacy Act" (PHEPA) was introduced on May 14, 2020, by Senator Richard Blumenthal of Connecticut.[170] Enforceable by the FTC, this Act focuses on protecting user data (referred to in the Act as "Emergency Health Data"), that is collected by covered organizations, concerning the COVID-19 pandemic.[171] "Emergency Health Data" is defined in the Act as data that is "linked or reasonably linkable to an individual or device…, that concerns the public COVID-19 health emergency."[172] A "covered organization" is defined in the Act as "any person (including a government entity) that collects, uses, or discloses emergency health data electronically or through communication by wire or radio," or that develops, amongst other things, mobile applications for responding to the COVID-19 public health emergency.[173] Unlike the ENPA,[174] these definitions encompass not only operators of an automated exposure notification service, but all organizations that collect emergency health data.[175] Additionally, PHEPA's definition of emergency health data tells us that the Act only applies to data that is collected concerning COVID-19. The ENPA, on the other hand, applies to data that is collected

[169] *Id.*

[170] Public Health Emergency Privacy Act [PHEPA], S. Res. S.3749, 116th Cong. (2020).

[171] *Id*. at § 1,2,6.

[172] *Id.* at § 2.

[173] *Id.*

[174] ENPA, *supra* note 128. at § 1.

[175] PHEPA, at § 2.

by an automated exposure notification service (AENS). Although AENS are currently being used to collect data concerning COVID-19, they could be used in the future to collect different kinds of data.

Section 3, the most robust section of the Act, focuses on protecting collected emergency health data.[176] The Section begins by establishing a right to privacy (subsection (a)) and a right to security (subsection (b)).[177] Under the right to privacy, covered organizations that collect emergency health data shall only collect, use, or disclose data that is "necessary, proportionate, and limited for a good faith public health purpose."[178] These organizations must also ensure the accuracy of their data and safeguard against the use of that data for discriminatory purposes.[179] The right to privacy also restricts covered organizations from disclosing this data to a government entity, unless that entity is a public health authority and the disclosure "is made in solely for good faith public health purposes and in direct response to exigent circumstances."[180] Similar to the phrase "purposes related to an infectious disease" that appears in the ENPA,[181] a "good faith public health purpose" is not defined within the PHEPA. This phrase begs the question of what purpose would satisfy this standard. Under the Section 3 right to security, these

[176] *Id.* at § 3.

[177] *Id.*

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] ENPA, at § 5.

organizations must "establish and implement reasonable data security policies, practices, and procedures to protect the security and confidentiality of emergency health data."[182]

Section 3(c) prohibits covered organizations from collecting, using, or disclosing emergency health data for any purpose not authorized within the Act. Where the ENPA is quite general with its prohibition of collection for any "commercial purpose,"[183] the PHEPA specifically prohibits collection, use, or disclosure for the following: (1) commercial advertising and e-commerce (including the training of machine learning algorithms related to commercial advertising and e-commerce), (2) "soliciting, offering, selling, leasing, licensing, renting, advertising, marketing, or otherwise commercially contracting for employment, finance, credit, insurance, housing, or education opportunities in a manner that discriminates or otherwise makes opportunities unavailable on the basis of emergency health data", and (3) making unavailable "the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation."[184] Section 4 of the PHEPA further addresses discrimination by prohibiting government entities and covered organizations from restricting or denying the right to vote in a federal, state, or local election on the basis of an individual's emergency health data.[185] If such discrimination were to occur, the individual has the right to bring civil action to obtain appropriate relief.[186]

---

[182] PHEPA, at § 3.

[183] ENPA, at § 5.

[184] PHEPA, at § 3.

[185] *Id.* at § 4.

[186] *Id.*

Section 3(d) makes it unlawful for any covered organization to collect, use, or disclose emergency health data unless "the individual to whom the data pertains has given affirmative express consent."[187] However, three other reasons could allow covered organizations to collect, use, or disclose without an individual's consent. These exceptions are when such is necessary and for the sole purpose of protecting against "…illegal activity", "…responding to… information security incidents…," or when the organization is required to by law. [188] After consent is given, the individual can revoke that consent and the covered organization must provide a mechanism for doing so.[189] Once consent has been revoked, the organization has thirty (30) days to destroy (or render not linkable to the individual) the emergency health data.[190] Absent revocation of the user's consent, three provisions in Section 3(g) dictate when user data must be deleted. These provisions demand that emergency health data be deleted sixty (60) days after collection or sixty (60) days after the Secretary of Health and Human Services, or individual state governor, declares the termination of the public health emergency.[191]

Section 3(e) requires covered organizations to provide to users a privacy policy.[192] This policy must be clear and conspicuous, must describe how and for what purposes data is

[187] *Id.* at § 3.

[188] *Id.*

[189] *Id.*

[190] *Id.* Once consent is revoked, collection must cease as soon as practicable, but within 15 days. *Id.*

[191] *Id.*

[192] *Id.*

collected, to whom the data is disclosed to and why, the organizations data retention policies, and how the individual may exercise their rights under the PHEPA.[193]

Section 3(f) requires organizations that collect the data of more than 100,000 individuals to issue a public report every ninety (90) days stating the number of individuals that organization collected, used, or disclosed emergency health data from, as well as the categories of data, the purpose for the collection, use, or disclosure, and the third parties to whom it was disclosed.

Sections 3(i) and 3(j) provide that the PHEPA should not be construed to limit manual contact tracing or to prohibit research.

Section 5 of the PHEPA requires that the Secretary of Health and Human Services, in consultation with the U.S. Commission on Civil Rights and the Federal Trade Commission (FTC), shall submit a report to Congress examining "the civil rights impact of the collection, use, and disclosure of health information in response to the COVID-19 health emergency."[194] This report is different than the one provided for under the ENPA. The report provided in Section 9 of the ENPA assesses the impact on "privacy and civil liberties,"[195] whereas the required PHEPA report would only address the civil rights impact.[196]

Section 6 gives individuals a private right of action for violations of the PHEPA. Section 6(c)(1)(A) says that "Any individual alleging a violation of this Act may bring a civil action in

[193] *Id.*

[194] *Id.* at § 5.

[195] ENPA, at § 9.

[196] PHEPA, at § 5.

any court of competent jurisdiction…"[197] This is different than the enforcement authority granted to the FTC under the ENPA.[198] This means that instead of relying on the FTC to enforce and punish PHEPA violators, the individual who was harmed by the violation may sue the covered organization.[199] Section 6(b) of the PHEPA also allows the States to bring an action on behalf of their residents when they believe their residents have been threatened or adversely affected by a violation of this Act, by any person subject to this Act.[200]

Part IV – Implementing Digital Contact Tracing in the United States

This part of the Note will analyze which provisions of the proposed bill, the PHEPA or the ENPA, would best regulate the efforts taken in South Korea and Singapore, should the United States implement similar efforts to attempt to control the COVID-19 pandemic.

A. Regulating South Korean Efforts in the United States

South Korea implemented a comprehensive, multiple angle approach to contact tracing. This approach included non-mobile application based efforts such as GPS, cell phone location tracking, and credit card usage data, as well as websites that help individuals avoid high risk areas.[201] South Korea also used mobile applications to keep individuals in contact with case workers and to ensure infected, or potentially infected, residents did not break their quarantine.[202]

---

[197] *Id.* at § 6.

[198] ENPA, at § 10.

[199] PHEPA, at § 6.

[200] *Id.*

[201] Park et al., *supra* note 61. *See also* Zastrow, *supra* note 66.

[202] Wray, *supra* note 61.

Such efforts should be implemented in the United States to supplement the Bluetooth exposure notification frameworks that are already being used.

i. Regulating Non-Mobile Application Based Efforts

Implementation of digital contact tracing ("DCT") through GPS, cell phone location, and credit card data in the United States would have to be governed under a regulation such as the Public Health Emergency Privacy Act (PHEPA). In fact, between the two bills dissected above, such efforts could only be governed by a PHEPA-like regulation because it regulates any entity that collects emergency health data,[203] whereas the Exposure Notification Privacy Act (ENPA) only regulates health data collected by automated exposure notification services (such as the Google Apple exposure notification mobile framework).[204]

A PHEPA-like regulation would put in place many safeguards that could help mitigate the distrust of the government and big tech companies that many Americans have. PHEPA Section 3(a) allows more Americans to feel that the collection of their private affairs will remain limited and secure.[205] Furthermore, the Act's consent requirements, disclosure restrictions, and mandatory publication of public reports would help Americans feel confident in the privacy of their data and the impact their data is making. Lastly, Americans can feel safe knowing that, should they suffer harm through a violation of PHEPA, the Act ensures that they have the power

[203] PHPEA, *supra* note 165. at § 2.

[204] ENPA, *supra* note 128. at § 2.

[205] PHEPA , *supra* note 165. at § 3.

to bring a civil action against the violator.[206] All of the above provisions is necessary for a federal regulation to adequately safeguard people's privacy.

However, the PHEPA is not without its faults. Section 3 of the Act provides that a covered organization may not disclose emergency health data to a government entity unless that entity is a public health authority ("PHA") and the disclosure "is made [solely] for good faith public health purposes and in direct response to exigent circumstances."[207] However, the quoted phrase is undefined. This means that emergency health data could be disclosed to a PHA in instances not intended by the legislators. If this exception were to exist in a data privacy bill, it is recommended that "public health purpose" be defined narrowly to only cover purposes of protecting the health and safety of the people. It is also recommended that "exigent circumstances" be defined narrowly to encompass specific, identifiable events that directly harm or threaten to harm the health and safety of the people. Lastly, a qualifier should be added to ensure this exception is only allowed to be used if it is reasonable that the disclosure of data would help mitigate the threat or harm imposed by the exigent circumstances. This means that such an exception would only be available in circumstances where the people's health and safety were threatened, a specific and identifiable event was causing the threat, and it is reasonable that the disclosure of data would help mitigate the looming harm.

The non-mobile application based DCT efforts implemented by South Korea should be implemented in the United States. These efforts should include the tracking of GPS, cell phone location data, and credit card usage. However, these efforts must be restrained by a regulation akin to the Public Health Emergency Privacy Act. With minor modifications, the PHEPA would

[206] *Id.*

[207] *Id.*

adequately cover all potential collectors of data to ensure the protection of all American's privacy rights.

ii. Regulating Mobile Application Based Efforts

Since the PHEPA covers any entity that collects emergency health data,[208] and the ENPA covers entities that operate an automated exposure notification service,[209] both bills are viable methods of restraining DCT mobile applications. These bills are similar to each other in that they both, amongst other things: require affirmative consent, restrict data collection to only what is necessary, restrict data disclosure to only what is necessary, and give the user control over their data.[210] Both bills would adequately restrain these applications; however, a combination of both would be ideal. Although both bills require some kind of reporting, the ENPA requires reporting on the impact of both "privacy and civil liberties,"[211] whereas the PHEPA requires reporting on only the civil rights impact.[212] On the other hand, language defining what data is collected should come from the PHEPA. The PHEPA's definition of "emergency health data" is narrow in that it only covers data "that concerns the public COVID-19 health emergency."[213] The ENPA's definition of "covered data" is much broader in that it is "any information that is…collected…with an automated exposure notification service."[214] The narrower definition of

---

[208] *Id.*

[209] ENPA, *supra* note 128. at § 2.

[210] *See* PHEPA, *supra* note 165. *See also* ENPA, *supra* note 128.

[211] ENPA, *supra* note 128. at § 9.

[212] PHEPA, *supra* note 165. at § 5.

[213] *Id.*

[214] ENPA, *supra* note 128. at § 2.

the PHEPA would help to ensure that only user data pertaining to the COVID-19 pandemic, and no additional and unnecessary information, is collected.

Furthermore, regulations, such as the ENPA or PHEPA, could raise DCT application participation through adequate privacy policies. Whether a privacy policy exists for a given DCT application varies by the state,[215] and this can make it hard to determine whether and to whom collected data may be shared. Although GAEN boasts privacy protection,[216] applications, such as The Corona 100m (Co100) application (to help individuals contact case workers), or the "self-quarantine safety protection" application (used to track quarantined individuals), could be implemented and brought up to a similar standard through proper legislation.

B. Regulating Singaporean Efforts Under the Proposed Legislation

Singapore's key to success in fighting COVID-19 has been its mandatory TraceTogether program. This program is implemented through either a smartphone app or Bluetooth device provided by the government.[217] Because any Bluetooth device that does not rely on a mobile application would also fall outside the scope of the ENPA,[218] a hybrid ENPA/PHEPA regulation is necessary to adequately restrain such an effort. All the provisions described in Part IV(A)(i)-(ii) above would be essential for this hybrid regulation. These provisions include narrow data

---

[215] Laura Hecht-Felella and Kaylana Mueller-Hsia, *Rating the Privacy Protections of State Covid-19 Tracking Apps*, BRENNAN CENTER FOR JUSTICE, https://www.brennancenter.org/our-work/research-reports/rating-privacy-protections-state-covid-19-tracking-apps (last visited Feb 28, 2021).

[216] EXPOSURE NOTIFICATIONS: HELPING FIGHT COVID-19 - GOOGLE, *supra* note 28.

[217] TRACETOGETHER FAQS, *supra* note 77.

[218] *See* ENPA, *supra* note 128.

collection, limited data disclosure, an even more limited data disclosure exception, mandatory impact reports, and a detailed privacy policy.

Although postponed, Singapore is aiming to make the TraceTogether program mandatory.[219] A mandatory contact tracing program in the United States is unlikely. However, given the smartphone usage in the United States,[220] providing a Bluetooth device to those who want one would be a step closer to the public participation percentage required for DCT studies.[221] The TraceTogether program is, in part, a centralized method of contact tracing because it allows the Ministry of Health to access user information to identify close-contacts.[222] Additionally, because of the decentralized Bluetooth exposure notification system,[223] this type of program could alleviate some privacy concerns that would occur under a South Korean-like effort.

Whenever a user consents to having his data decrypted under Singapore's TraceTogether program, that decrypted data includes the identities of users that person has come into contact with (so long as they use the application or TraceTogether Token).[224] A program implemented in the United States would need a way to confirm that no user's identity is revealed, passively, through the consent of a different user. This could be easily accomplished through a second affirmative consent. For example, if User A receives a positive diagnosis and consents to his data

---

[219] Hermesauto, *supra* note 89.

[220] PEW RESEARCH CENTER: INTERNET, SCIENCE & TECH, *supra* note 11.

[221] Univ. of Oxford, *supra* note 51.

[222] Bay et al., *supra* note 85.

[223] TRACETOGETHER FAQS, *supra* note 82.

[224] Asghar and Kaafar, *supra* note 108.

log being decrypted by the operator, User B could receive an automated request (via a smartphone through the DCT app or an automated phone call for users of a Token-like device) first notifying them of a possible exposure, and then asking if User B wants to consent to having their identify revealed for contact tracing purposes. This consent request would protect the identity of User B because it would be automated and sent to the user alongside the anonymous exposure notification prior to decryption.

Under the ENPA, this program would have to be implemented by a non-government entity. This is because ENPA Section 2(11) defines an operator as something "other than a public health authority."[225] Under the PHEPA, however, the "covered organization" could be a government entity. The United States government would need to decide whether a government agency or a private company would be more effective in gaining user support.

Part V – Conclusion

Digital contact tracing has the ability to "substantially reduce" the spread of COVID-19,[226] and the efforts of South Korea and Singapore have proven as such.[227] Because of the slow roll out of state digital contact tracing programs,[228] the efforts by South Korea and Singapore that are described in this Note should be implemented by the United States. These efforts are GPS and cell phone location tracking, analysis of credit card usage data, websites that help individuals

[225] ENPA, *supra* note 128. at § 2.

[226] Univ. of Oxford, *supra* note 31. "Our models show we can stop the epidemic if approximately 60% of the whole population use the app and adhere to the app's recommendations. Lower numbers of app users will also have a positive effect; we estimate that one infection will be averted for every one to two users.'"

[227] HARVARD BUSINESS REVIEW, *supra* note 9.

[228] Parshin, *supra* note 118.

avoid high risk areas, mobile applications to keep individuals in contact with case workers and to ensure infected or potentially infected residents do not break their quarantine, and the dispersing of Bluetooth devices to Americans without constant access to a smartphone. The goal of this implementation should be to lawfully expand digital contact tracing to as many consenting Americans as possible. This program should be a joint operation between the private sector and the federal government,[229] funded by the government.[230] Such a program may be able to increase the percentage of willing participants to a number that will better combat the virus.[231] However, many Americans distrust of the government and Big Tech.[232] Therefore, the United States must pass a federal regulation to restrain potential misuse and protect the privacy of its people. The two federal privacy bills currently proposed, the Exposure Notification Privacy Act (ENPA) and the Public Health Emergency Privacy Act (PHEPA), do not individually go far enough to protect privacy alone. However, a combination of the Acts, as well as added language to further protect user data, could convince concerned Americans that their privacy will be protected, while actually protecting that privacy.

[229] *See* Kat Jercich, *supra* note 151.

[230] ASPA, *supra* note 155.

[231] BAOBAO ZHANG ET AL., *Americans' perceptions of privacy and surveillance in the COVID-19 Pandemic* (2020), https://osf.io/9wz3y (last visited Dec 9, 2020).

[232] De La Garza, *supra* note 124.