CARPENTER & CONTACT TRACING: PRIVACY RIGHTS IN THE TIME OF A GLOBAL PANDEMIC

Shannon K. Cox[†]

INTRODUCTION

In 2020, the world was disrupted by the outbreak of the novel coronavirus, also called COVID-19. In the United States, the first documented case of the virus was announced on January 21, 2020, just north of Seattle.[1] As of February 2022, almost two years after that first case, there have been over 77.8 million reported U.S. cases, with the total deaths from COVID-19 above 920,000.[2] As new variants of the virus develop and spread, cases continue to increase.[3]As of early 2022, the United States was averaging more than 500,000 new cases per day, which was more than any previous time in the pandemic.[4] Early in his presidency, President Joe Biden discussed plans to reassert a federal strategy to bring the virus under control, differing from the previous

[†] Shannon K. Cox was born and raised in Millbrook, NY. She is a graduate of Marist College, where she majored in English Literature and received her Paralegal certification. As a student at Syracuse University College of Law she earned her Juris Doctor and a certificate of advanced study in National Security Law and Policy. Shannon also served as a Lead Articles Editor for *Syracuse Law Review*, an Academic Success Fellow, and as a Research Assistant for the Institute for Security Policy and Law. Shannon is a recent graduate of Syracuse University College of Law Class of 2022 where she graduated Magna Cum Laude, and she has accepted a commission as an Officer in the U.S. Army Judge Advocate General Corps.

1. Sarah Mervosh et al., *One Year, 400,000 Coronavirus Deaths: How the U.S. Guaranteed its Own Failure*, N.Y. TIMES, (last updated Oct. 26, 2021), https://www.nytimes.com/2021/01/17/us/covid-deaths-2020.html.

2. Jordan Allen, et al., *Coronavirus in the U.S.: Latest Map and Case Count*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html (last visited June 3, 2022).

3. *See* Mervosh et al., *supra* note 1.

4. Allen, et al., *supra* note 2.

administration, which largely relegated virus containment to the states, leaving state governors to lead the charge against COVID-19.[5]

Many scholars have pointed the United States' failure to quickly create a nation-wide contact tracing system as one of the missteps in containing the virus.[6] The goal of contact tracing is to identify areas of infection and inform individuals near those areas of their possible exposure to the virus.[7] However, many people in the United States have concerns about contact tracing technology and the privacy rights that are necessarily implicated in the tracing of citizen's cell phones.[8] In this article, I will first describe the rights implicit in the Fourth Amendment and their relation to privacy.[9] I will explore the possibility of there being a national security exception that could be used to allow for contact tracing to combat biological threats to the United States.[10] Next, I will discuss the different technologies that could be used, namely in contact tracing apps, and the various legal implications that could arise depending on the technology and the type of app used.[11] Lastly, I will discuss my recommendations for contact tracing moving forward.[12] Now that there is a vaccine available for COVID-19, the issues associated with contact tracing may appear to be irrelevant. However, the United States must plan for the next biological threat to the country and the world, so that we are more prepared in the future.

I. FOURTH AMENDMENT DOCTRINE & *CARPENTER*

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[13] The basic purpose of the Fourth Amendment is to safeguard the privacy of individuals against arbitrary invasions by governmental officials.[14] For much of this nation's history, Fourth Amendment search doctrine was tied to common law trespass and focused on whether the government

5. *See* Mervosh et al., *supra* note 1.

6. *See id.*

7. *See* Jennifer Daskal, *COVID-19 Special Edition: Part II: Response Issues: Good Health and Good Privacy Go Hand-in-Hand,* 11 J. NAT'L SEC. L. & POL'Y 131, 137 (2020).

8. *See id.* at 138–39.

9. *See infra* Section I.

10. *See infra* Section I(A).

11. *See infra* Sections II, III.

12. *See infra* Section VI.

13. U.S. CONST. amend. IV.

14. Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967).

obtained information by physically intruding on a constitutionally protected area.[15] Recently, the Court has acknowledged that "property rights are not the sole measure of Fourth Amendment violations."[16] The Court expanded the Fourth Amendment to include certain expectations of privacy.[17] There is not one metric for deciding what is a reasonable expectation of privacy, but the Court will often look to a historical understanding of "what was deemed an unreasonable search when [the Fourth Amendment] was adopted."[18]

The Fourth Amendment does not apply to the conduct of private persons or entities, but only to the Government or its actors.[19] When determining whether a party is an agent of the Government in Fourth Amendment inquiries, the inquiry turns on the degree of the Government's participation in the private actor's activities.[20] Relevant factors for determining this include "whether a government agent directed, requested, or incentivized the search, whether the private actor believed at the time that she was acting under the direction or authority of the government agent, and whether a government agent had notice of the search."[21]

The Court considers advancing technologies by looking at the principal of privacy as it was seen when the Fourth Amendment was adopted. In *Kyllo v. United States*, the Court held that the use of thermal imaging technology to detect heat coming from the side of the defendant's home was a search.[22] Any other holding would have left the homeowners "at the mercy of advancing technology."[23] Similarly, the Court has taken unique characteristics of technology into account, such as the immense storage capacity of cell phones.[24] The nature of cell phones allows for a vast storage of private and sensitive information.[25] Therefore, officers must generally obtain a warrant to search through the information contained on a person's cell phone.[26]

15. United States v. Jones, 565 U.S. 400, 405 (2012).
16. Soldal v. Cook Cnty., 506 U.S. 56, 64 (1992).
17. *See* Katz v. United States, 389 U.S. 347, 351 (1967).
18. Carroll v. United States, 267 U.S. 132, 149 (1925).
19. Natalie Ram & David Gray, *Mass Surveillance in the Age of COVID-19*, 7 J. L. BIOSCIENCE 1, 5 (2020).
20. *Id.* (citing Skinner v. Ry Lab. Execs. Ass'n, 489 U.S. 602, 614–15 (1989)).
21. *Id.*
22. Kyllo v. United States, 533 U.S. 27, 34–35 (2001).
23. *Id.* at 35–36.
24. *See* Riley v. California, 573 U.S. 373, 393 (2014).
25. *Id.* at 396–97.
26. *Id.* at 386.

The initial question to determine whether the Fourth Amendment applies to a case is whether a "search" or a "seizure" occurred.[27] An action by the government is a search if it involves a government trespass or infringes upon a reasonable expectation of privacy.[28] A search can either be a physical intrusion into a constitutionally protected area, or an intrusion upon subjectively manifested expectations of privacy that society recognizes as reasonable.[29] A seizure is a material interference with property or liberty.[30]

Before the landmark case *Carpenter v. United States*, which established a warrant requirement for law enforcement to acquire a person's cell-site location information (CSLI), other cases guided the Supreme Court's rulings on Fourth Amendment privacy protections.[31] While CSLI, which is personal location information maintained by a third-party, does not fit neatly into a category of data pre-*Carpenter*, it can be viewed as an intersection of two lines of cases—the first of which address a person's expectation of privacy in his physical location, and the second of which addresses what a person keeps to himself and what he shares with others.[32]

The first set of cases has to do with a person's reasonable expectation of privacy regarding his or her physical location or movements. In one instance, the Supreme Court declared that the use of beeper technology to follow a car did not constitute a search, since "a person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[33] The movements of the vehicle and the occupant were "voluntarily conveyed to anyone who wanted to look."[34] Although this was not deemed a search, the Court was careful to distinguish between tracking with a beeper and more sweeping forms of surveillance, emphasizing the limited use the government made of the beeper.[35]

Next, in *United States v. Jones*, the Court looked at an instance where FBI agents installed a GPS tracking device in a vehicle and

27. *See* Alan Z. Rozenshtein, *Disease Surveillance and the Fourth Amendment*, LAWFARE (Apr. 7, 2020, 1:54 PM), https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment.

28. *Id.*

29. Ram & Gray, *supra* note 19 at 7.

30. *Id.*

31. *See generally* 138 S. Ct. 2206 (2018); Katz v. United States, 389 U.S. 347 (1967); United States v. Jones, 565 U.S. 400 (2012).

32. *Carpenter*, 138 S. Ct. at 2214–16.

33. United States v. Knotts, 460 U.S. 276, 281 (1983).

34. *Id.*

35. *See id.* at 284–85.

monitored it for twenty-eight days.[36] While the Court found that this constituted a search based on the government's physical trespass of the vehicle, five justices agreed that related privacy concerns could be raised by, for example, activating the stolen vehicle detection in the car to track Jones himself, or using his cell phone for GPS tracking.[37] Justice Alito, in his concurrence, wrote that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[38]

In the second group of early decisions, the Court distinguishes between what a person keeps to himself and what he decides to share with others. Under the third-party doctrine, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[39] This is true, even if the information is given while the person is under the assumption that it will only be used for a limited purpose.[40] In *United States v. Miller*, the government subpoenaed bank records, seeking several months of transactional history.[41] The Court rejected a Fourth Amendment claim to the documents, saying that the documents were business records of the bank, which Miller could assert neither ownership nor possession.[42] The Court concluded that Miller, by using the bank, had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government."[43]

The Court has also applied the third-party doctrine to records held by a telephone company.[44] The Court decided that the government's use of a pen register, which is a device that kept a record of dialed outgoing phone numbers on landline telephone, was not a violation of the Fourth Amendment.[45] Of importance in the Court's decision was the pen register's "limited capabilities" and that the Court doubted that people have any actual expectation of privacy in the numbers they dial

36. 565 U.S. at 400.
37. *Id.* at 404–05; *Id.* at 428–29 (Alito, J., concurring).
38. *Id.* at 430 (Alito, J., concurring).
39. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
40. United States v. Miller, 425 U.S. 435, 443 (1976).
41. *Id.* at 437–38.
42. *Id.* at 440.
43. *Id.* at 443.
44. *Smith*, 442 U.S. at 744.
45. *Id.* at 744, 745–46.

from their landline.[46] When a person makes a call, he voluntarily conveys the dialed numbers to the phone company.[47]

However, a person does not surrender all Fourth Amendment rights when he or she enters the public sphere.[48] To the contrary, individuals have a reasonable expectation of privacy in their physical movements, and information that one seeks to preserve as private, even in public areas, may be constitutionally protected.[49] Before the digital age, law enforcement was able to follow the movements of a suspect, but, given the practical constraints of traditional policing, only for a brief period of time.[50] Therefore, the expectation is that law enforcement would not monitor and catalogue every single movement of a person for an extended period of time.[51]

Carpenter changed the way the courts look at the Fourth Amendment in relation to emerging technologies and privacy rights. In *Carpenter,* investigators looking into a robbery applied for court orders under the Stored Communications Act to obtain cell phone records for several suspects, including Carpenter.[52] The Stored Communications Act allows the government to compel disclosure of telecommunication records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought by the government are "relevant and material to an ongoing . . . investigation."[53] Overall, the government obtained 12,898 of Carpenter's location points, which equals about 101 locations points per day.[54]

The Supreme Court used this case to explore a new phenomenon, namely, the ability to chronicle a person's past movements though the use of his cell phone CSLI.[55] This case was similar to *Jones* due to the GPS nature of the data, and that "much like the GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled."[56] The Court reasoned that when *Smith* was

46. *Id.* at 742.
47. *Id.* at 744.
48. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
49. United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring); Katz v. United States, 389 U.S. 347, 351 (1967).
50. *Jones*, 565 U.S. at 429 (Alito, J., concurring).
51. *Id.* at 430.
52. *Carpenter*, 138 S. Ct. at 2212.
53. 18 U.S.C. § 2703(d) (2021).
54. *Carpenter,* 138 S. Ct. at 2212.
55. *See id.* at 2216.
56. *Id.*

decided in 1979, very few people could have imagined a future in which wireless carriers not only kept records of dialed numbers, but also detailed and comprehensive records of a person's movements.[57] The third-party doctrine was not extended to cover the circumstances seen in *Carpenter*.[58]

The Court held that an individual maintains a legitimate expectation of privacy in the record of his physical movements as displayed through his cell phone CSLI.[59] Therefore, the location information that the government obtained from Carpenter's cell phone was the product of a search and required a warrant.[60] The risk of the government accessing CSLI without a warrant raises even greater concerns than the GPS tracking in *Jones*.[61] Unlike the car in *Jones*, a cell phone is almost a feature of human anatomy.[62] While people will leave their vehicles or their homes, they will rarely go anyplace without their cell phone, which is compulsively carried by most people at all times.[63] A person will carry their phone without thinking, even to revealing places such as private residences, doctor's offices, political headquarters, and other locales that may reveal information about a person's personal life.[64] Accordingly, when the government tracks a person's cell phone, it achieves "near perfect surveillance," which has the same effect as if it had attached an ankle monitor to the person being tracked.[65]

In addition, the retrospective quality of the data at hand concerned the Court.[66] By using CSLI, the government may travel back in time to trace a person's location, subject only to the retention policies of the wireless carriers, which typically maintain records for five years.[67] The potential surveillance would be "tireless and absolute."[68] The rule the Court adopted in this case "must take account of [the] more sophisticated systems that are already in use or in development."[69]

57. *Id.* at 2217.
58. *See id.*
59. *Carpenter*, 138 S. Ct. at 2217.
60. *See id.*
61. *Id.* at 2218.
62. *Id.* (citing Riley v. California, 573 U.S. 373, 385 (2014)).
63. *Id.*
64. *Carpenter*, 138 S. Ct. at 2218.
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Carpenter*, 138 S. Ct. at 2218–19 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

Cell-site location information is rapidly approaching GPS-level precision.[70] Additionally, new technology measures the time and angle of signals hitting their towers.[71]

The Court rejected the government's view that the third-party doctrine governed the case, concluding that the government's argument "fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years."[72] Unlike other kinds of witnesses that may be called during the course of a criminal trial, wireless carriers supplying CSLI are "ever alert, and their memory is nearly infallible."[73] Therefore, applying the third-party doctrine to cover CSLI from cell phones would not be a straight forward application of the third-party doctrine, but instead for a significant extension of the third-party doctrine to a distinct and new category of information.[74]

Although the Court declined to extend the third-party doctrine to cover CSLI in this instance, the majority made it clear that this was a narrow opinion based on the specific facts of the case.[75] The Court declined to express any opinion on matters that were not before it, such as real-time CSLI or tower dumps, which are a download of information on all the devices that connected to a specific tower during a specific interval of time.[76] Furthermore, the case does not call into question surveillance for the techniques for the purpose of national security.[77]

A. The National Security Exception

The Court in *Carpenter* expressly declined to comment on whether the government could pull a person's CSLI or other technological data for purposes relating to national security.[78] This leaves questions regarding what would constitute a national security exception. National security objectives include traditional notions of protecting the country from invasion from other countries, but it also

70. *Id.* at 2219.
71. *Id.*
72. *Id.*
73. *Id.*
74. *Carpenter*, 138 S. Ct. at 2219.
75. *Id.* at 2220.
76. *Id.*
77. *Id.*
78. *Id.*

involves other objectives that have the goal of protecting the people in the United States.[79]

The outbreak of COVID-19 has impacted national security in several ways. First, the pandemic has harmed military readiness.[80] In order to maintain a military that is ready to address any arising national security threats, large groups of service members must live, train, and work together in close proximity.[81] While the number of cases of COVID-19 increased every day, the Department of Defense announced in December of 2020 that the U.S. military's total number of coronavirus cases exceeded 100,000.[82] The outbreak of COVID-19 forced the military to postpone exercises that are important to ensure military readiness, and social distancing measures interrupted military recruitment, which lead to a decrease in the number of people entering military training.[83]

Additionally, the pandemic has shown the United States' susceptibility to a targeted biological attack, which could potentially be deadlier than the COVID-19 virus.[84] It is possible that the failure of governments around the world to contain the spread of COVID-19 quickly and efficiently may make biological attacks more attractive to those seeking to cause harm.[85] More than 920,000 lives in the United States have been lost to COVID-19 as of February 2022, demonstrating that a biological event has the possibility of causing deaths on a large scale.[86]

Since COVID-19 has impacted both the military and civilian populations of the United States, President Biden acknowledged the pandemic as a top concern of national security.[87] The first National Security Memorandum (NSM-1) put forth by the new administration notes that the pandemic "is a grave reminder that biological threats, whether naturally occurring, accidental, or deliberate, can have

79. Eric M. Salwell & R. Kyle Alagood, *Biological Threats are National Security Risks: Why COVID-19 Should Be a Wake-up Call for Policy Makers*, 77 WASH. & LEE L. REV. ONLINE 217, 218 (2020).

80. *Id.* at 233.

81. *Id.*

82. Patricia Kime, *COVID-19 Cases Among U.S. Military Personnel Top 100,000*, MILITARY.COM (Dec. 23, 2020), https://www.military.com/daily-news/2020/12/23/covid-19-cases-among-us-military-personnel-top-100000.html.

83. Salwell & Alagood, *supra* note 79, at 235.

84. *Id.*

85. *See id.* at 235–36.

86. *See* Allen, et al., *supra* note 2.

87. Steven Aftergood, *Biden Issues National Security Directive 1*, FED'N OF AM. SCIENTISTS (Jan. 25, 2021), https://fas.org/blogs/secrecy/2021/01/biden-nsd/.

significant and potentially existential consequences for humanity."[88] In the memorandum, President Biden announced that his administration "will treat epidemic and pandemic preparedness, health security, and global health as top national security priorities, and will work with other nations to combat COVID-19 and seek to create a world that is safe and secure from biological threats."[89] The memo details the actions that the Biden administration plans to undertake to address the current pandemic, and addresses plans to prepare for any future crisis of the same nature.[90] This is not the first instance in which the spread of infectious disease has been treated as a national security issue. In Executive Order 13747, President Obama declared, "promoting global heath security is a core tenant of our national strategy for countering biological threats."[91] While the current global pandemic has brought health sharply into focus as a national security event, threats from infectious disease have long been regarded as possible national security issues.

While it is not clear if a global pandemic was originally envisioned as a national security exception, the destruction caused by the COVID-19 pandemic and the governmental response indicates that a global pandemic is a national security event. Even when something is considered a national security event, the Court may engage in a balancing test.[92] In the *Keith* case, the Court considered wiretapping a national security threat and balanced the government's duty to protect the domestic security, and the potential danger imposed by unreasonable surveillance to individual privacy.[93] Due to the sensitive nature of security surveillances and the "inherent vagueness of the domestic security concept," the Court held that surveillance for the purposes of national security does not justify a departure from the customary Fourth Amendment requirements.[94] However, the nature of the national security issue in this instance is different than in the *Keith* case. While *Keith* addressed a bombing of a CIA office, a global pandemic will by definition have devastating impacts on many people.

88. JOSEPH R. BIDEN, JR., NATIONAL SECURITY MEMORANDUM ON UNITED STATES GLOBAL LEADERSHIP TO STRENGTHEN THE INTERNATIONAL COVID-19 RESPONSE AND TO ADVANCE GLOBAL HEALTH SECURITY AND BIOLOGICAL PREPAREDNESS (2021), https://fas.org/irp/offdocs/nsm/nsm-1.pdf.

89. *Id.*

90. *See id.*

91. Exec. Order No. 13747, 3 C.F.R. 13747 (2017).

92. *See* United States v. United States Dist. Ct. for the E. Dist. of Mich., 407 U.S. 297, 314–15 (1972).

93. *See id.*

94. *Id.* at 320.

Both instances have the potential to cause mass casualties but given the gravity of a death toll that could be imposed by a biological threat, the balancing may be more complex than that described in *Keith.* This balancing would likely consider the nature of the infectious disease at hand. While the national security interest in the case of a biological threat might be greater, the public's interest in the privacy of their own data is not insubstantial. The Court has consistently been hesitant to invade the privacy of citizens through the use of increasingly invasive technology.[95] Therefore, although the pandemic and spread of infectious disease is a national security concern, it is not likely that a Fourth Amendment analysis would differ substantially from the analysis in *Carpenter.*

II. COVID-19 CONTACT TRACING

A. Methods

Contact tracing has always played an important role in public health responses to infectious disease.[96] Often, public health officials will conduct field investigations in which they will interview infected persons to identify the places they have been and the people they have been in close contact with.[97] According to the CDC, contact tracers and case investigators must possess skills such as an understanding of patient confidentiality, including the ability to conduct interviews without violating confidentiality, excellent and sensitive interpersonal, cultural sensitivity, and interviewing skills, and cultural competency.[98] Thus, the CDC recognizes that real privacy concerns surround the practice of contact tracing as it stands.

As Robert Chesney outlines, there are two main issues with the traditional model of contact tracing when applied to COVID-19.[99] First, there is an issue with the scale of the virus.[100] Given the number of people who have been infected, there are not enough field investigators to implement the traditional approach of interviewing

95. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

96. Robert Chesney, *COVID-19 Contact Tracing We Can Live With: A Roadmap and Recommendations*, LAWFARE (Apr. 14, 2020, 12:29 PM), https://www.lawfareblog.com/covid-19-contact-tracing-we-can-live-roadmap-and-recommendations.

97. *Id.*

98. CASE INVESTIGATION AND CONTACT TRACING, CENTER FOR DISEASE CONTROL, https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/principles-contact-tracing-booklet.pdf (last visited June 3, 2022).

99. Chesney, *supra* note 96.

100. *Id.*

each relevant person.[101] Second, even if the traditional approach could be implemented at such a large scale, there are inherent weaknesses with this model of contact tracing.[102] Not every person is willing to cooperate with contact tracers for various reasons, which leads to critical omissions.[103] Even if every single person did their best to remember, memories are fallible, and certain details over the course of several days are bound to be forgotten.[104]

The purpose and the goal of contact tracing is to be able to identify all of the persons at risk of infection.[105] Thus, theoretically, the best system of contact tracing is one that produces a "comprehensive, time-stamped and spatially precise" record of everyone's movements.[106] However, this theoretical model of contact tracing is only ideal when seen in a vacuum, taking into account no other competing interests, such as privacy rights.[107] Some scholars have posited that the longer the pandemic goes on, the more willing Americans will be to trade their privacy for the ability to work and move around as they did before the pandemic began.[108]

However, such a comprehensive system would have extraordinary potential for abuse, whether from the people running the system or the people who could potentially gain unauthorized access to it.[109] As noted in *Carpenter*, a person's location shows intimate details about his or her life, such as who he or she chooses to spend time with, including "familial, political, professional, religious, and sexual associations."[110] Therefore, a system in which every person's every movement is tracked could, in theory, be used to "compromise, embarrass, extort, or otherwise cause harm."[111] Without extraordinary safeguards, a program such as this could have the unintended effect of causing people to cease their regular lawful activities for fear of being exposed.[112]

101. *Id.*
102. *Id.*
103. *Id.*
104. Chesney, *supra* note 96.
105. *Id.*
106. *Id.*
107. *Id.*
108. Rozenshtein, *supra* note 27.
109. Chesney, *supra* note 96.
110. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (citing United States v. Jones, 565 U.S. 400, 492 (2012)).
111. Chesney, *supra* note 96.
112. *See id.*

As an initial matter, interviews with contact tracers are not currently mandatory. Theoretically, Congress could make them mandatory in the future. If this were to happen, it is possible that any person who is non-compliant could be subject to penalties such as civil or criminal sanctions.[113] However, even imposing legal sanctions would not solve the problem of scalability, nor would it prevent natural errors in memory.[114] Therefore, merely making contact tracing interviews mandatory does not solve the problem.

Instead, the government could try to access information that is held by third-party actors. This includes information such as cell-site location information, credit card histories, or bank statements.[115] Even if the government was willing to go through a warrant process to gain access to this information, there might still be *Carpenter*-related concerns with this approach.[116]

B. Technology

Today, there is talk of creating contact tracing apps, most notably by big tech companies such as Apple and Google.[117] Apple and Google partnered to create a novel contact tracing app, which by its terms stipulate that the collection of location data is prohibited, data must only be used in relation to COVID-19 response efforts, and developers must follow their retention limitation.[118] The app also currently requires user consent for app installation as well as for the processing of a positive result.[119]

However, logistical issues still arise when dealing with contact tracing apps. As an initial matter, contact tracing apps will generally use either Bluetooth or GPS technology.[120] The technology used by an app determines the functionality of that app. An app that uses Bluetooth technology can use location data to map one cell phone's proximity to another that belongs to a person who may have tested positive for COVID-19.[121] Therefore, Bluetooth data can be used to show who went to a specific grocery store or bar, without showing the

113. *Id.*
114. *Id.*
115. *Id.*
116. Chesney, *supra* note 96.
117. Divya Ramjee et al., *COVID-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance*, 2021 CARDOZO L. REV. 101, 106.
118. *Id.* at 106–07.
119. *Id.* at 107.
120. Daskal, *supra* note 7, at 137.
121. *See id.*

precise location of contacts.[122] On the other hand, GPS monitoring maps locations as opposed to contacts.[123] The CSLI described in *Carpenter* falls into the category of GPS technology, because it is a time stamped record of geographic data that is held by a service provider.[124] Although Bluetooth monitoring raises fewer privacy concerns than GPS monitoring, Bluetooth could be combined with other data, which could reveal a significant amount of information about a person over time.[125]

Many of the current app models have opted to use Bluetooth technology because it is associated with fewer privacy risks.[126] Additionally, while Bluetooth technology tends to have a shorter range than GPS technology, it may generate more accurate data due to its increased precision.[127] However, Bluetooth does require a time lag in order to update the most recent contacts, and has trouble determining relevant factors to the spread of disease, such as when there is a barrier between two people.[128] Bluetooth-based technology apps have the possibility of being overinclusive. They are overinclusive in that they may include contacts, such as when two cars are stopped at the same traffic light, who do not necessarily need to be grouped in with your contacts.[129] Another example is that the app will not consider whether you and the contact were wearing personal protective equipment (PPE) at the time the contact was made, thus eliminating any serious risk of infection.[130]

For an app to work, whether it be using Bluetooth or GPS technology, a large portion of the population would need to first, have a smart phone, next, download the app to their phones, and third, keep their phones on themselves at all times while moving around.[131] As an initial matter, not every person has a phone that is capable of downloading apps.[132] This is especially true for the population of

122. *Id.*

123. *Id.*

124. *See* Michael Price, Carpenter v. United States *and the Future Fourth Amendment*, THE CHAMPION, 48, 48 (June 2018) https://www.nacdl.org/getattachment/cf9ebc32-4f50-498c-bece-19e5f66719af/p48-50_Price_Michael_Carpenter-v-United_States_June_2018_Champion.pdf?lang=en-US.

125. Daskal, *supra* note 7, at 137.

126. *See* Ramjee et al., *supra* note 117, at 113.

127. *Id.*

128. *See id.* at 113–14.

129. *See* Chesney, *supra* note 96.

130. *Id.*

131. *See id.*

132. *Id.*

elderly people in the country, who are most at risk for COVID-19.[133] Additionally, if the app is not mandatory, not every person will download the app onto their phones.[134] While it is possible that not everybody will then carry their phone with them to each place they go, as *Carpenter* notes, a cell phone has become almost an extension of one's self, since almost every person is always carrying one.[135] Therefore, this seems to be the least concerning of the issues with the app model.

Currently, the app promulgated by Apple and Google is downloaded by a voluntary opt-in to the app.[136] It is possible that the app model may become mandatory. Even early in the beginning of the pandemic, Congress appropriated over $500,000,000 for public health data and surveillance infrastructure modernization.[137]

III. CURRENT CONTACT TRACING

In September 2020, Apple and Google launched their partner system, called Exposure Notification Express.[138] In a statement on the website, the app is proclaimed to work in conjunction with the government, saying "Google and Apple jointly created the Exposure Notifications System out of a shared sense of responsibility to help governments and our global community fight this pandemic through contact tracing."[139] Users of Apple products past a certain generation of technology can access this technology without needing to download an app to their phone.[140] Android users will need to download the app in order to gain the benefits from the technology.[141] However, the technology is claimed to be designed with privacy in mind, and does

133. *COVID-19 Risks and Vaccine Information for Older Adults*, CDC, https://www.cdc.gov/aging/covid19/covid19-older-adults.html (last visited June 3, 2022).

134. Chesney, *supra* note 96.

135. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

136. Ramjee et al., *supra* note 117, at 107.

137. Ram & Gray, supra note 19, at 2.

138. Ramjee et al., *supra* note 117; *see also Exposure Notifications: Help Slow the Spread of COVID-19, With One Step on Your Phone*, GOOGLE, https://www.google.com/covid19/exposurenotifications/ (last visited June 3, 2022) (describing the functions and overview of Exposure Notification Express) [hereinafter GOOGLE, *Exposure Notifications*].

139. GOOGLE, *Exposure Notifications*, *supra* note 138.

140. *See Supporting Exposure Notifications Express*, APPLE, https://developer.apple.com/documentation/exposurenotification/supporting_exposure_notifications_express (last visited June 3, 2022).

141. GOOGLE, *Exposure Notifications*, *supra* note 138.

not share your identity with other users, Google, or Apple.[142] Additionally, the Exposure Notifications System will not track location as a GPS app might, but only tracks contacts.[143]

So far, the federal government has not implemented a national app for contact tracing among states.[144] Some scholars have noted that for the best success in contact tracing, an app implemented by one state must be cross-compatible with apps from other states.[145] People increasingly travel across state borders, so the ability for apps in different states to interact with each other is crucial to the success of contact tracing apps.[146]

Within the United States, North Dakota, South Dakota, Utah, and Rhode Island were the first states to implement contact tracing apps that are separate and distinct from the Apple/Google collaborative technology.[147] Each of these state apps operate on a voluntary opt-in basis, and each respective website declares that any person may delete their data and opt out at any time.[148] However, there are problems with the lack of cohesion between states when it comes to contact tracing apps, despite the fact that health and wellness is an area that is often left to the states to regulate.[149] First, there is an imbalance between states with varying levels of funding within each state's health departments.[150] States that have smaller budgets must resort to leaning on private tech companies for app development and storage of data, which could potentially lead less secure databases or potential hacking issues.[151] Additionally, different state apps with varying levels of privacy and security for storage of information could result in multiple apps with different security issues.[152]

However, there are a range of different functions for which the government could use contact tracing. While contact tracing via app has only been used to detect clusters of the virus and inform the public, it is possible to envision a scenario in which contact tracing is used to

142. Jennifer Olivia, *Public Health Surveillance in the Context of COVID-19*, 18 IND. HEALTH L. REV. 107, 115 (2020).
143. *See* Ramjee et al., *supra* note 117, at 106–07.
144. *Id.* at 110.
145. *Id.* at 108.
146. *Id.*
147. *Id.* at 109.
148. *See* Ramjee et al., *supra* note 117, at 107.
149. *Id.* at 108.
150. *See id.* at 110.
151. *Id.* at 110–11.
152. *Id.* at 111.

enforce quarantine orders. This has been done in other countries, including South Korea and Poland.[153] In Poland, there is an app called "Home Quarantine."[154] Quarantined individuals must use this app, and are sent random requests to upload geo-located photos to ensure they are maintaining quarantine.[155] Similarly, in Hong Kong quarantined individuals have their locations tracked and also are required to check in several times a day by app.[156] This level of tracking via app has not been addressed in the United States to date, but judges have found unique ways to enforce quarantine orders in certain circumstances. For example, in Louisville, Kentucky, residents who have been exposed to COVID-19 but refuse to quarantine have been forced by court order to wear ankle monitors.[157] Surveillance in these instances is being used as an enforcement mechanism, allowing violators to face possible criminal charges.[158]

Other countries, such as South Korea, have implemented contact tracing measures that have significantly reduced the spread of the virus at an extremely successful rate.[159] Some scholars believe that in order to have success with disease prevention and control, the United States must adopt policies akin to South Korea's, while ignoring "fetishized notion[s] of individual privacy."[160]

From the beginning of the pandemic, South Korea took the threat of infection seriously.[161] However, the early actions taken by the South Korean government posed a substantial threat to individual privacy.[162] The efforts taken by the South Korean government to contact trace

153. *See* Daskal, *supra* note 7, at 140.

154. *Id.*

155. *Id.*

156. *Id.*

157. Mallika Kallingal, *Ankle Monitors Ordered for Louisville, Kentucky Residents Exposed to COVID-19 Who Refuse to Stay Home*, CNN (updated Apr. 3, 2020), https://perma.cc/BKE4-724M.

158. *Id.; see* Daskal, supra note 7, at 140.

159. *See* Susan Landau, *Contact-Tracing Apps: What's Needed to Be an Effective Public Health Tool*, LAWFARE (Jan. 19, 2021, 11:39 AM), https://www.lawfareblog.com/contact-tracing-apps-whats-needed-be-effective-public-health-tool.

160. Jane Bambauer & Brian Ray, *COVID-19 Apps are Terrible—They Didn't Have to Be*, THE DIGIT. SOC. CONT.: A LAWFARE PAPER SERIES 1, 2 (Nov. 2020), https://assets.documentcloud.org/documents/20424830/bambauer-and-ray-final-2.pdf.

161. Landau, *supra* note 159.

162. *Id.*; Mark Zastrow, *South Korea is Reporting Intimate Details of COVID-19 Cases: Has it Helped?*, NATURE (Mar. 18, 2020), https://www.nature.com/articles/d41586-020-00740-y.

infected individuals included publishing a website detailing the movements and patterns of infected persons that contained information such as the person's age and gender, a detailed log of their movements down to the minute using closed circuit television (CCTV), and credit card transactions.[163] In South Korea, contact tracing began much faster than in the United States, and contained much more personal information.[164] One of the reasons that South Korea was able to take this quick action was that in 2015, they changed their laws to allow the Ministry of Health and Welfare to quickly access CSLI and credit card records during the outbreak of an infectious disease.[165] Additionally, the South Korean population showed a willingness to isolate, avoid contact with other people, and wear masks, a willingness that is still not currently seen in the United States population at large.[166] The government of South Korea says that the public is more likely to trust it if it releases more transparent information about the virus, which includes information about people with confirmed cases.[167]

IV. POLICY LIMITATIONS & RECOMMENDATIONS

It is not likely that a model such as the one promulgated in South Korea would be upheld in the United States. The methods used in South Korea to contact trace do not align with the U.S. Constitution or the cultural values of many Americans. To begin, the American population as a whole would likely not support any government action compelling such extensive contact tracing as to allow for CCTV footage, CSLI, and credit card information to be compiled and the information then disseminated to citizens.[168] As noted in *Carpenter*, GPS information provides an intimate look into a person's life, and can reveal things such as a person's "familial, political, professional, religious, and sexual preferences."[169] This near-perfect mode of surveillance, especially when coupled with other surveillance tools such as CCTV and credit card records, appears to far exceed the bounds of the Fourth Amendment.

163. Zastrow, *supra* note 162.
164. Landau, *supra* note 159.
165. *Id.*
166. *Id.*
167. Zastrow, *supra* note 162.
168. Landau, *supra*, note 159.
169. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

The willingness of a population to comply with mandatory contact tracing must be taken into consideration. In South Korea, even before COVID-19 was understood to be spread through airborne transmission, about fifty percent of South Korean citizens reported cancelling their social events and sixty-three percent reported wearing masks when they left their homes.[170] In contrast, there is still pushback from many Americans on mask mandates, even a year into the pandemic.[171] Importantly, contact tracing is based in a trust between the tracer and the person being traced.[172] When human contact tracers are employed, they can create a personal connection with the infected individual or ask how the person is doing and if they can help.[173] This helps to build trust between the contact tracer and the exposed or infected individual—something that contact tracing apps are lacking.[174] In the United States, there are significant trust issues between the government and the people, especially among disenfranchised communities.[175] This is a trend not only in the United States, as data from other countries shows that contact tracing did not gain as much traction among minority communities.[176]

Public opinion aside, it is not likely that the constitutional safeguards established by the Fourth Amendment would allow for such practices. While there might be a national security exception carved out of *Carpenter's* rule against using multiple days of CSLI information, it is not likely that the exception would look as invasive as the techniques used by South Korea's government. As seen in *Carpenter*, applying the third-party doctrine to CSLI or Bluetooth for the purposes of contact tracing would be a significant expansion of the doctrine and would likely not be upheld. Some of the justices have voiced concerns about the longevity of the third-party doctrine when applied to newer and more invasive technologies.[177] Justice Gorsuch notes that in today's society, the internet is used in almost every aspect of our lives, and that our most private documents, which were once kept in desk drawers, are now accessible through online servers.[178]

170. Landau, *supra* note 159.
171. *See id.*
172. *Id.*
173. *Id.*
174. *Id.*
175. Landau, *supra*, note 159.
176. *Id.*
177. *See* Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).
178. *Id.*

Instead of suggesting the third-party doctrine be applied to personal information that is kept on online servers, deciding what privacy rights are recognized often calls for a pure policy decision.[179] It is likely that any policy regarding contact tracing in the future is going to weigh the rights of citizens to maintain privacy in their online records against the need of the government to protect its citizens against biological threat.

With the introduction of the vaccine for COVID-19, many people question the need for expansive contact tracing systems.[180] If we are to properly prepare for the next biological threat, many questions about the permissibility of contact tracing in American society must still be answered. Since contact tracing raises substantial privacy issues under Fourth Amendment law, what other methods can we use to be better prepared for the next biological threat? Under *Carpenter*, the government may not pull a person's CSLI records without a probable cause and a warrant.[181] However, if the government suspects a person of breaking quarantine and wishes to impose civil sanctions or criminal penalties, the government may request a warrant for the CSLI of that person and show probable cause. Moving forward, the nature of the threat of disease is going to impact the balancing test employed. The deadlier the virus in question, the more likely it is that the public would be accepting of more invasive contact tracing technology.

With the introduction of a vaccine to combat COVID-19, it appears as though a mandatory contact tracing app will not be employed to track the current virus. The government will likely continue to use a combination of voluntary contact tracing with widespread dissemination of the vaccine. However, it is important to ask and answer policy questions relating to the acceptability of mandatory contact tracing in the future, should the occasion for it arise. While the government may require citizens to download a contact tracing app at some point, there are many things that must happen before the government imposes that kind of mandate. Appropriate safeguards must be put into place in order to allow for privacy to be maintained. Unlike the contact tracing employed in South Korea, any contact tracing information gathered and published should not include a person's identifying information. Policies on the

179. *Id.* at 2265.

180. *See* Caitlin Owens, *Contact Tracing Fizzles Across America*, AXIOS (Jan. 28, 2022), https://www.axios.com/coronavirus-contact-tracing-public-health-omicron-61231b48-b17b-4455-aa6a-a0fbf8400678.html.

181. *Carpenter*, 138 S. Ct. at 2221.

collection, retention, dissemination, and deletion of data must be established.

While all this will take time, it is recommended that the government sticks to a voluntary method of contact tracing apps while implementing the required safeguards. While a voluntary method of contact tracing may be less efficient, contact tracing should not be the sole method used for fighting the virus. The outbreak of COVID-19 has brought sharply into focus issues concerning American privacy values and raised issues that must be addressed before the next biological threat occurs.