EMORY | LAW

Emory Law Journal

Volume 71 | Issue 3

2022

A New Normal: How COVID-19 and Digital Contact Tracing Highlight a Need for New Fourth Amendment Norms

Danielle J. Fong

A NEW NORMAL: HOW COVID-19 AND DIGITAL CONTACT TRACING HIGHLIGHT A NEED FOR NEW FOURTH AMENDMENT NORMS

ABSTRACT

Contact tracing helps epidemiologists identify individuals who have been exposed to a virus. Manual contact tracing has been used for decades to interrupt the transmission of disease and reduce the number of infections within a population. It is a pillar of disease control. But the manual process has certain limitations—it is time-intensive, expensive, and subject to human error. Digital contact tracing overcomes these limitations. Using GPS and Bluetooth technologies, digital contact tracing applications automate and expedite the tracing and notification processes, with life-saving implications. In 2020, countries that implemented contact tracing technology in response to COVID-19 contained outbreaks, minimized incidence of the virus, and kept death tolls comparatively low.

Notwithstanding the urgent public health need COVID-19 created, privacy-minded Americans were and continue to be resistant to digital contact tracing. Instead of widespread adoption of the technology, there is widespread concern that data collected via contact tracing apps will be co-opted, de-anonymized, and used by law enforcement for non-public health purposes.

Is this concern warranted? Can the government demand a record of your location data from Apple and Google without implicating your Fourth Amendment rights? Can it secure this data without a warrant or probable cause? The answer to all these questions is, most likely, yes. Although the Fourth Amendment limits the government's search and seizure powers, Americans who opt to use contact tracing apps—for the sake of their health and the public health at large—position themselves outside the bounds of Fourth Amendment protections. In other words, Americans can choose health or privacy, but not both.

Surely, that should not be our norm. We need a new normal. This Comment, therefore, discusses how jurisprudence fails to protect the rights of U.S. citizens using contact tracing applications. It details the current Fourth Amendment tests and doctrines, including the Katz *test (which centers around reasonable expectations of privacy) and the third-party doctrine (which says a person has no legitimate expectation of privacy in information supplied to third parties). Given the public health benefits of an effective contact tracing system, this*

Comment considers why changes to the Fourth Amendment framework—ones that accommodate the competing privacy and welfare needs of the twenty-first century—are warranted. Ultimately, this Comment proposes that the Supreme Court eliminate the Katz *test and overturn the third-party doctrine to extend Fourth Amendment protections to information like location data captured by life-saving technologies.*

INTRODUCTION

The first U.S. case of COVID-19 was reported in January 2020.[1] Since then, more than half a million Americans have died.[2] Contact tracing applications, which use digital technology to help track and limit the spread of disease, have proven effective.[3] But in the United States, privacy concerns[4] severely stunt their life-saving potential.[5] Rejection of this technology—despite the pressing need a pandemic presents—highlights significant flaws and room for improvement in Fourth Amendment jurisprudence.

This Comment is divided into four parts. Part I pertains to contact tracing and COVID-19. Section A introduces traditional contact tracing, its function during a public health crisis, and its limitations. Section B discusses a new form of contact tracing—digital contact tracing, which relies on the adoption of either GPS or Bluetooth technologies—and its implementation in the United States. Section C outlines the privacy concerns associated with digital contact tracing, and section D identifies the implications of those concerns in the context of COVID-19. Section E considers how developers of contact tracing apps have sought to address privacy concerns in the United States.

Given that digital contact tracing is a new technology, Part II examines Fourth Amendment precedent concerning new technologies. Section A considers the types of questions courts might be asked with respect to digital contact tracing. Section B provides an analysis of major Fourth Amendment cases that address new technologies with similar characteristics to digital contact tracing. Section C makes note of additional Fourth Amendment doctrine relevant to digital contact tracing.

Part III applies Fourth Amendment jurisprudence to digital contact tracing technology. Highlighting key parts of preeminent cases, this Part considers how precedent might be used to decide a case involving digital contact tracing applications.

---

[1] *First Travel-Related Case of 2019 Novel Coronavirus Detected in United States*, CTRS. FOR DISEASE CONTROL & PREVENTION (Jan. 21, 2020), https://www.cdc.gov/media/releases/2020/p0121-novel-coronavirus-travel-case.html.

[2] *COVID Data Tracker*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://covid.cdc.gov/covid-data-tracker/#datatracker-home (last visited Dec. 17, 2021).

[3] U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-666SP, CONTACT TRACING APPS 1–2 (2020).

[4] Adam Janos, *If Google Can Have Your Data, Can Police Investigating Crimes Have It Too?*, A&E: TRUE CRIME BLOG (Apr. 23, 2018), https://www.aetv.com/real-crime/smart-wearable-home-technology-apps-data-solving-crimes.

[5] I. Glenn Cohen, Lawrence O. Gostin & Daniel J. Weitzner, *Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension*, 323 JAMA 2371, 2371 (2020).

To conclude, Part IV proposes an alternative theory to Fourth Amendment jurisprudence. Section A outlines concurrences and dissents that have come out of landmark Fourth Amendment cases, and section B uses the ideas proposed to suggest alternatives to current jurisprudence.

I. CONTACT TRACING AND COVID-19

This Part describes traditional contact tracing, its function during a public health crisis, and its limitations. It then discusses a new form of contact tracing that relies on GPS or Bluetooth technologies—digital contact tracing—and its implementation in the United States. Next, it outlines privacy concerns associated with digital contact tracing and considers how those concerns curtail user adoption and have negative implications in the context of COVID-19. Finally, this Part considers how developers of contact tracing apps have sought to address privacy concerns.

A. Traditional Contact Tracing

Contact tracing is a public health tool used to interrupt the transmission of disease and reduce the number of infections within a population.[6] Traditionally, contact tracing has been conducted manually by human tracers, who are usually public health officials trained to identify infected individuals, track down their contacts, notify those contacts of potential exposure, and propose measures—such as quarantines—to prevent or limit the spread of disease.[7] For decades, epidemiologists have used contact tracing "to tackle everything from foodborne illnesses to sexually transmitted diseases, as well as recent outbreaks of SARS and Ebola."[8]

Although manual contact tracing is a pillar of disease control, it has limitations.[9] Interviewing infectious patients and retracing their interactions can be time-intensive, and if the particular disease spreads easily, the list of potential contacts can be overwhelming.[10] Indeed, in a report published in April 2020,

---

[6] PATRICIA MOLONEY FIGLIOLA, CONG. RSCH. SERV., IF11559, DIGITAL CONTACT TRACING TECHNOLOGY: OVERVIEW AND CONSIDERATIONS FOR IMPLEMENTATION 1 (2020).

[7] *See* ERIC N. HOLMES & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10511, COVID-19: DIGITAL CONTACT TRACING AND PRIVACY LAW 1 (2020).

[8] Christie Aschwanden, *Contact Tracing, a Key Way to Slow COVID-19, Is Badly Underused by the U.S.*, SCI. AM. (July 21, 2020), https://www.scientificamerican.com/article/contact-tracing-a-key-way-to-slow-covid-19-is-badly-underused-by-the-u-s/.

[9] *See* Alejandro De La Garza, *What Is Contact Tracing? Here's How It Could Be Used to Help Fight Coronavirus*, TIME (Apr. 22, 2020, 11:29 AM), https://time.com/5825140/what-is-contact-tracing-coronavirus/.

[10] *Id.*

shortly after the outbreak of COVID-19, the Johns Hopkins Bloomberg School of Public Health's Center for Health Security recommended that 100,000 contact tracers be added to the U.S. workforce to make COVID-19 contact tracing initiatives effective.[11] It was estimated that implementing a recommendation of this magnitude would cost $3.6 billion.[12] In addition, manual contact tracing is limited because infected individuals might misreport where they have been or who they have seen, either intentionally or unintentionally, which diminishes the effectiveness of the process.[13]

B. Digital Contact Tracing

Given the inefficiencies and costs associated with manual contact tracing, there has been a push to digitize the process with smartphone applications (apps)[14]—a development made possible by new technologies.[15] Using Global Positioning System (GPS) signals, Bluetooth capabilities, or a combination of the two,[16] contact tracing apps identify people who have come in close contact. GPS apps log a user's location, whereas Bluetooth apps collect identifiers of the smartphones that cross paths.[17] In either case, information is digitally stored.[18] Then, if an app user receives an positive diagnosis and voluntarily reports their infection, the stored data is leveraged to notify other users of their exposure.[19] By automating the process, apps expedite contact tracing, eliminating some of the inefficiencies inherent in a manual approach.[20] In the face of communicable disease, apps are able to notify a greater proportion of exposed individuals more

---

[11] CRYSTAL WATSON, ANITA CICERO, JAMES BLUMENSTOCK & MICHAEL FRASER, A NATIONAL PLAN TO ENABLE COMPREHENSIVE COVID-19 CASE FINDING AND CONTACT TRACING IN THE U.S. 10 (2020), https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf.

[12] *Id.* at 3.

[13] *See, e.g.*, Jaclyn Diaz, *Australian State Cuts COVID Lockdown Short, Saying Man Lied to Contact Tracers*, NPR (Nov. 20, 2020, 4:03 AM), https://www.npr.org/sections/coronavirus-live-updates/2020/11/20/936957351/australian-state-cuts-covid-lockdown-short-saying-man-lied-to-contact-tracers.

[14] FIGLIOLA, *supra* note 6.

[15] *Id.*

[16] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 3.

[17] Jack Morse, *Sorry, Contact-Tracing Apps Are Not Coming to the Rescue*, MASHABLE (May 13, 2020), https://mashable.com/article/contact-tracing-apps-will-not-stop-coronavirus/.

[18] 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; Yoshua Bengio, Daphne Ippolito, Richard Janda, Max Jarvine, Benjamin Prud'homme, Jean-François Rousseau, Abhinav Sharma & Yun William Yu, *Inherent Privacy Limitations of Decentralized Contact Tracing Apps*, 28 JAMA 193, 193–94 (2021).

[19] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 3.

[20] *Id.*

quickly and more accurately, without the expense of a workforce of manual tracers.[21]

In light of these benefits, digital contact tracing carried huge public health potential with respect to COVID-19, both when the virus first emerged and as new variants developed.[22] At the height of the of outbreak, experts argued COVID-19 could be suppressed if digital contact tracing was implemented.[23] But this seemingly simple solution was complicated by two factors. The effectiveness of contact tracing apps depends on: (1) the level of adoption within a particular population and (2) the type of technology—GPS or Bluetooth—used. Decisions related to these factors prevented digital contact tracing from reaching its potential in the United States.

1. Factors Affecting App Potential

Research suggests contact tracing apps have "an effect at all levels of uptake."[24] However, digital contact tracing is most effective when a large proportion of the population consistently carries a compatible mobile device and enables contact tracing functionality.[25] From a public health lens, high levels of app adoption are ideal because suppression is the utmost goal.[26] The more people enrolled as potential contacts, the more complete the tracing, and the better the app is at identifying exposure.[27] For context, a simulation conducted in response to COVID-19 found the pandemic could have been suppressed if eighty percent of all smartphone users utilized contact tracing apps.[28]

Effectiveness also depends on whether a contact tracing app is built with GPS or Bluetooth capabilities. In their first iteration, most contact tracing apps

---

[21] *Id.*

[22] *Id.*

[23] Cohen et al., *supra* note 5.

[24] Patrick Howell O'Neill, *No, Coronavirus Apps Don't Need 60% Adoption to be Effective*, MIT TECH. REV. (June 5, 2020), https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.

[25] Andrew Lee, *Contact Tracing Is Working Around the World—Here's What the UK Needs to Do to Succeed Too*, CONVERSATION (June 9, 2020, 9:05 AM), https://theconversation.com/contact-tracing-is-working-around-the-world-heres-what-the-uk-needs-to-do-to-succeed-too-140293.

[26] *See Tracking COVID-19: Contact Tracing in the Digital Age*, WORLD HEALTH ORG. (Sept. 9, 2020), https://www.who.int/news-room/feature-stories/detail/tracking-covid-19-contact-tracing-in-the-digital-age.

[27] Chiara Farronato, Marco Iansiti, Marcin Bartosiak, Stefano Denicolai, Luca Ferretti & Roberto Fontana, *How to Get People to Actually Use Contact-Tracing Apps*, HARV. BUS. REV. (July 15, 2020), https://hbr.org/2020/07/how-to-get-people-to-actually-use-contact-tracing-apps.

[28] Cohen et al., *supra* note 5, at 2732.

were designed to capture GPS data.[29] GPS-based apps record a user's location.[30] Location data is useful to public health officials because it reveals "hotspots"—physical areas of elevated disease occurrence or risk.[31] Opportunities for notification are not limited to app users if location information is collected.[32] Meaning, infected individuals who have not installed contact tracing apps can still aid in digital notification efforts.[33] Those without an app who receive a diagnosis can let health professionals know where they have been.[34] After, an alert can be sent to those with apps who visited the same locations according to their stored GPS data.[35] For this reason, GPS-based apps are helpful in contact tracing efforts.

Contact tracing apps built with Bluetooth technology capture less information than those using GPS data.[36] Bluetooth-based apps keep a record of devices that have been in close proximity.[37] These apps notify users of potential exposure based on person-to-person encounters, not app users' locations.[38] Without location data, Bluetooth-based apps overlook cases of "environmental transmission," where disease passes between individuals even though their phones are not within the proximity needed for Bluetooth recognition.[39] Moreover, technology experts worry about the general accuracy of Bluetooth technology.[40] The strength of a phone's Bluetooth signal varies from time to time, and Bluetooth transmission is vulnerable to interference from other signals.[41] As a result, data collected by Bluetooth-based apps is often incomplete

---

[29] Jack Morse, *North Dakota Launched a Contact-Tracing App. It's Not Going Well*, MASHABLE (May 6, 2020), https://mashable.com/article/north-dakota-contact-tracing-app/.

[30] *Id.*

[31] Shannon Bond, *Apple, Google Coronavirus Tool Won't Track Your Location. That Worries Some States*, NPR (May 13, 2020, 2:42 PM), https://www.npr.org/2020/05/13/855064165/apple-google-coronavirus-tech-wont-track-your-location-that-worries-some-states.

[32] Matteo Luccio, *Using Contact Tracing and GPS to Fight Spread of COVID-19*, GPS WORLD (June 3, 2020), https://www.gpsworld.com/using-contact-tracing-and-gps-to-fight-spread-of-covid-19/.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] Mark Zastrow, *Coronavirus Contact-Tracing Apps: Can They Slow the Spread of Covid-19?*, NATURE (May 19, 2020), https://www.nature.com/articles/d41586-020-01514-2.

[37] Kylie Foy, *Bluetooth Signals from Your Smartphone Could Automate Covid-19 Contact Tracing While Preserving Privacy*, MIT NEWS (Apr. 8, 2020), https://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409.

[38] *Id.*

[39] Andy Greenberg, *How Apple and Google Are Enabling Covid-19 Contact-Tracing*, WIRED (Apr. 10, 2020, 3:37 PM), https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/.

[40] Sam Biddle, *The Inventors of Bluetooth Say There Could Be Problems Using Their Tech for Coronavirus Contact Tracing*, INTERCEPT (May 5, 2020, 6:00 AM), https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/.

[41] Adam Vaughan, *Bluetooth May Not Work Well Enough to Trace Coronavirus Contacts*,

and may reflect more false negatives than GPS-based data.[42] Overall, with regard to disease control, Bluetooth-based apps are less effective.[43]

2. Implementation in the United States

On April 10, 2020, Apple and Google announced a partnership to support the United States in the development of digital contact tracing apps.[44] Their app—Exposure Notification—utilized Bluetooth technology, not GPS data.[45] In the companies' joint statement, Exposure Notification was described as follows:

> Once enabled, users' devices will regularly send out a beacon via Bluetooth that includes a random Bluetooth identifier—basically, a string of random numbers that aren't tied to a user's identity and change every 10–20 minutes for additional protection. Other phones will be listening for these beacons and broadcasting theirs as well. When each phone receives another beacon, it will record and securely store that beacon on the device. At least once per day, the system will download a list of the keys for the beacons that have been verified as belonging to people confirmed as positive for COVID-19. Each device will check the list of beacons it has recorded against the list downloaded from the server. If there is a match between the beacons stored on the device and the positive diagnosis list, the user may be notified and advised on steps to take next.[46]

To summarize, Apple and Google's Exposure Notification technology enables contact tracing based on the physical proximity of smartphones.[47] Apple and Google's decision to use Bluetooth technology over GPS technology and their repeated assertions that contact data is "securely store[d]" are intended to minimize privacy concerns and increase user adoption in the United States.[48] But the privacy concerns raised by this technology are objectively valid and have

---

NEWSCIENTIST (May 12, 2020), https://www.newscientist.com/article/2243137-bluetooth-may-not-work-well-enough-to-trace-coronavirus-contacts/.

[42] *See id.*

[43] Stephen Nellis & Paresh Dave, *Apple, Google Ban Use of Location Tracking in Contact Tracing Apps*, REUTERS (May 4, 2020, 12:50 PM), https://www.reuters.com/article/us-health-coronavirus-usa-apps/apple-google-ban-use-of-location-tracking-in-contact-tracing-apps-idUSKBN22G28W.

[44] Press Release, Apple & Google, Exposure Notifications Frequently Asked Questions (Sept. 2020) (on file at https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf).

[45] *Id.*

[46] *Id.*

[47] Gregory Barber, *Google and Apple Change Tactics on Contact Tracing Tech*, WIRED (Sept. 1, 2020, 2:42 PM), https://www.wired.com/story/google-apple-change-tactics-contact-tracing-tech/.

[48] *Id.*

not been reconciled.[49] As a result, contact tracing apps were not widely implemented in the United States in response to the pandemic.

C. Privacy Concerns Associated with Digital Contact Tracing

Contact tracing apps, whether of the GPS or Bluetooth variety, compile huge databases ripe for misuse by public entities.[50] Apps that use GPS technology present risks of government surveillance because they track a user's movements and activities.[51] Apps that use Bluetooth technology present indirect but similar risks because Bluetooth data can be used to create "social graphs" that unveil a user's social interactions.[52] As one privacy group suggests, people are "open to traditional contact tracing involving individuals working under the auspices of the health department" but are generally distrustful of electronic contact tracing.[53] Many worry contact tracing is "basically electronic surveillance."[54] The American Civil Liberties Union (ACLU) and a group of 200 scientists, for example, expressed hesitation with respect to contact tracing apps given the potential for overreach.[55] In a joint white paper, these advocates argued that "[w]hile some of these systems may offer public health benefits, they may also cause significant risks to privacy, civil rights, and civil liberties."[56]

The response to contact tracing apps in Norway, an early adopter of the technology, lends credence to the privacy concerns expressed by the ACLU.[57]

---

[49] Laura Hecht-Felella & Kaylana Mueller-Hsia, *Rating the Privacy Protections of State Covid-19 Tracking Apps*, BRENNAN CTR. (Nov. 5, 2020), https://www.brennancenter.org/our-work/research-reports/rating-privacy-protections-state-covid-19-tracking-apps.

[50] *Contact Tracing Apps: Which Countries Are Doing What*, MED. XPRESS (Apr. 28, 2020), https://medicalxpress.com/news/2020-04-contact-apps-countries.html.

[51] NORTON ROSE FULBRIGHT, CONTACT TRACING APPS: A NEW WORLD FOR DATA PRIVACY (2021), https://www.nortonrosefulbright.com/en-us/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy.

[52] Natasha Lomas, *EU Privacy Experts Push a Decentralized Approach to COVID-19 Contacts Tracing*, TECH CRUNCH (Apr. 6, 2020, 2:42 PM), https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/.

[53] Amy Lauren Fairchild, Lawrence O. Gostin & Ronald Bayer, *Contact Tracing's Long, Turbulent History Holds Lessons for COVID-19*, CONVERSATION (July 16, 2020, 8:15 AM), https://theconversation.com/contact-tracings-long-turbulent-history-holds-lessons-for-covid-19-142511.

[54] *Id.*

[55] Jessica Davis, *ACLU, Scientists Urge Privacy Focus for COVID-19 Tracing Technology*, HEALTH IT SEC. (Apr. 20, 2020), https://healthitsecurity.com/news/aclu-scientists-urge-privacy-focus-for-covid-19-tracing-technology.

[56] DANIEL KAHN GILLMOR, PRINCIPLES FOR TECHNOLOGY-ASSISTED CONTACT-TRACING 1 (2020), https://www.aclu.org/sites/default/files/field_document/aclu_white_paper_-_contact_tracing_principles.pdf.

[57] Todd Ehret, *Data Privacy Laws Collide with Contact Tracing Efforts; Privacy is Prevailing*, REUTERS (July 21, 2020, 2:36 PM), https://www.reuters.com/article/bc-finreg-data-privacy-contact-tracing/data-privacy-laws-collide-with-contact-tracing-efforts-privacy-is-prevailing-idUSKCN24M1NL.

In June 2020, the Norwegian Data Protection Authority ordered the Norwegian Institute of Public Health to suspend use of and delete all data collected via contact tracing technology.[58] The Norwegian Data Protection Authority said digital contact tracing presents a disproportionate risk to privacy.[59]

Other countries decided the risk was worthwhile.[60] In particular, East Asian countries responded to COVID-19 in a way that plainly favors public health over privacy, and the COVID-19 related benefits have been clear.[61] In March 2020, a contact tracing app called TraceTogether launched in Singapore to supplement manual contact tracing efforts.[62] By December 2020, 3.4 million people (approximately sixty percent of Singapore's population) downloaded TraceTogether, which uses Bluetooth signals.[63] Singapore's success is in part attributable to other measures—such as strict lockdowns and mask requirements—but government officials and experts maintain that participation in TraceTogether was a key factor in Singapore's ability to minimize incidence of the virus and reopen relatively quickly.[64] As a point of comparison, Singapore's and Norway's populations are comparable in size but their mortality rates (per 100,000 people) a year into the COVID-19 pandemic differed drastically, standing at 0.56% and 9.58% respectively.[65]

However, there is a tradeoff. Singapore had one of the lowest COVID-19 fatality rates globally and was recognized by the World Health Organization for its pandemic response.[66] But with the virus at bay, the country has been criticized

---

[58] *Id.*

[59] *Id.*

[60] *See* Tim McDonnell, *How Finland Got 20% of Its Population to Download a Contact Tracing App in One Day*, QUARTZ (Sept. 2, 2020), https://qz.com/1898960/whats-behind-finlands-contact-tracing-app-success-user-privacy/.

[61] *See* Yasheng Huang, Meicen Sun & Yuze Sui, *How Digital Contact Tracing Slowed Covid-19 in East Asia*, HARV. BUS. REV. (Apr. 15, 2020), https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia.

[62] *Covid-19 Apps Need Due Diligence*, 580 NATURE 563, 563 (2020).

[63] Yoolim Lee, *Singapore App Halves Contact Tracing Time Leading Engineer Says*, BLOOMBERG (Dec. 8, 2020, 7:54 AM), https://www.bloomberg.com/news/articles/2020-12-08/singapore-app-halves-contact-tracing-time-leading-engineer-says.

[64] Laurel Wamsley, *Singapore Says COVID-19 Contact-Tracing Data Can Be Requested by Police*, NPR (Jan. 5, 2021, 3:42 PM), https://www.npr.org/sections/coronavirus-live-updates/2021/01/05/953604553/singapore-says-covid-19-contact-tracing-data-can-be-requested-by-police; Hallam Stevens, *Does the Take-up of Singapore's TraceTogether Really Show Increased Trust in the Government?*, S. CHINA MORNING POST (Dec. 31, 2020, 8:00 AM), https://www.scmp.com/week-asia/opinion/article/3115863/does-take-singapores-tracetogether-really-show-increased-trust.

[65] *Mortality Analyses*, JOHNS HOPKINS UNIV. & MED.: CORONAVIRUS RES. CTR., https://coronavirus.jhu.edu/data/mortality (last visited Dec. 17, 2021).

[66] Jason Beaubien, *Singapore Was a Shining Star In COVID-19 Control—Until It Wasn't*, NPR (May 3, 2020, 7:00 AM), https://www.npr.org/sections/goatsandsoda/2020/05/03/849135036/singapore-was-a-shining-

with regard to privacy.[67] In the early days of the COVID-19 pandemic, the government assured Singaporeans that TraceTogether was anonymized and encrypted and that the data would be used "purely for contact tracing, period."[68] But in January 2021, it was reported that COVID-19 contact tracing data was available to police.[69] The government announced that data could be accessed in criminal investigations under the country's Criminal Procedure Code, which provides government officials the "power to order production of any document or other thing."[70] After this announcement, officials revealed contact tracing data had "already been used [by police] in a murder investigation."[71] Although Singaporeans have been described as not "particularly privacy conscious," the use of contact tracing data for this end "triggered public anger."[72]

The circumstances in Singapore and Norway emphasize the competing interests at play—contact tracing apps can be quite effective in combating COVID-19 (or other viruses) with a certain amount of buy-in, but they inherently infringe on users' privacy interests.

D. The Implications of Privacy Concerns

Privacy interests warrant attention—particularly in the United States—for two reasons. First, the U.S. Constitution affords a right to be "secure [in] 'the privacies of life' against 'arbitrary power.'"[73] Disregard for privacy directly impacts constitutional rights.[74] Second, the privacy concerns raised by contact tracing apps have negative implications for public health.[75] Public concern in the context of a pandemic is problematic because the more distrust there is in contact tracing technology, the less likely people are to use these apps and the less helpful the technology can be in flattening the curve of disease incidence.[76]

---

star-in-covid-control-until-it-wasnt.

67 Wamsley, *supra* note 64 (quoting Foreign Minister Vivian Balakrishanan).

68 *Id.*

69 *Id.*

70 *Id.*

71 Kristen Han, *Broken Promises: How Singapore Lost Trust on Contact Tracing Privacy*, MIT TECH. REV. (Jan. 11, 2021), https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police/.

72 *Id.*

73 Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

74 Joel R. Reidenberg, *Privacy in Public*, 69 U. MIA. L. REV. 141, 152 (2014).

75 *Tracking COVID-19*, *supra* note 26.

76 Farronato et al., *supra* note 27.

The partnership between Apple and Google made digital contact tracing functional with both iOS and Android operating systems, which cover nearly the entire mobile phone market in the United States.[77] That means widespread use of these apps was certainly possible throughout the duration of the pandemic.[78] But "[s]tates [were] slow to develop contact tracing apps, and people [were] slow to use them."[79] Although apps purported to protect privacy, there was too much concern that collected data would be co-opted, de-anonymized, and used by law enforcement and intelligence for non-public health purposes.[80] This concern is warranted—in this context and in the context of similar technology, like the new Apple AirTag.[81] According to Professor Andrew Ferguson, "The general public's move to smart digital technology is 'going to radically change criminal prosecution'" at the expense of Fourth Amendment rights.[82]

E. Current Privacy Protections

Both the World Health Organization and the Centers for Disease Control acknowledge the privacy risks associated with digital contact tracing.[83] But faced with COVID-19's persistence, they still advocate for widespread adoption of the technology because of the public health benefits.[84] In an attempt to achieve these benefits but also address the privacy concerns, Apple and Google promoted user privacy and security as central to their design.[85] They argued two features of their technology in particular were "privacy preserving": (1) the

---

[77] FIGLIOLA, *supra* note 6.

[78] *See id.*

[79] Christine Lehmann, *Privacy Concerns Hindering Digital Contact Tracing*, WEBMD (Sept. 25, 2020), https://www.webmd.com/lung/news/20200928/privacy-concerns-hindering-digital-contact-tracing.

[80] Lomas, *supra* note 52.

[81] AirTags are tracking devices developed by Apple and released in 2021. *See, e.g.*, Aaron Holmes, *New Records Show Google, Microsoft, and Amazon Have Thousands of Previously Unreported Military and Law Enforcement Contracts*, BUS. INSIDER (July 8, 2020, 1:27 PM), https://www.businessinsider.com/microsoft-google-amazon-pentagon-law-enforcement-contracts-2020-7; Tyler Sonnemaker, *Law Enforcement Agencies Are Using a Legal Loophole to Buy Up Personal Data Exposed by Hackers*, BUS. INSIDER (July 8, 2020, 4:54 PM), https://www.businessinsider.com/police-buying-hacked-data-bypassing-legal-processes-2020-7; Deanna Paul, *The Battle Between Privacy and Enforcement Isn't Going Away*, GUARDIAN (June 26, 2018), https://www.theguardian.com/commentisfree/2018/jun/26/battle-between-privacy-law-enforcement-carpenter.

[82] Janos, *supra* note 4.

[83] *See Tracking COVID-19*, *supra* note 26; *Digital Contact Tracing Tools*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/digital-contact-tracing-tools.html (May 26, 2020).

[84] *Id.*

[85] Press Release, Apple Newsroom, Apple and Google Partner on COVID-19 Contact Tracing Technology (Apr. 10, 2020) (on file at https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/).

reliance on Bluetooth signals as opposed to GPS data and (2) its opt-in nature.[86] First, Bluetooth technology is considered more "privacy-friendly" because, unlike GPS data, it does not store the "location of possible contacts, only that two users have been proximate."[87] Second, "[c]hoice is key."[88] In a country like the United States, it is understood that "[p]eople will avoid participation in a privacy-sensitive scheme that seems compulsory."[89] Therefore, Exposure Notification requires that users "download and opt in to an appropriate state or regional tracing app as well as opt in to the Apple-Google tracking feature in the operating system."[90] Although Bluetooth functionality and opt in requirements limit how completely contact tracing apps identify points of exposure,[91] apps that protect users' privacy garner public trust and, in turn, higher rates of adoption.[92] Since high rates of adoption give contact tracing apps their best chance at flattening the curve,[93] the hope was that "privacy-preserving contact tracing" would build buy-in and thereby most effectively contain the spread of COVID-19.[94]

However, buy-in is not a short-term goal. It is important that "privacy-preserving contact tracing" warrants public trust within the legal framework that governs.[95] If purported privacy protections fail to provide actual protection, it might hamper adoption of contact tracing apps—now, while COVID-19 is still pressing, and in the future, should other threats to public health surface.[96]

This Comment's primary purpose is to consider whether "privacy-preserving contact tracing" offers real protection within the framework of Fourth Amendment jurisprudence. Ultimately, this Comment concludes that the answer is no. Fourth Amendment jurisprudence, instead, exacerbates the privacy risks that curtail digital contact tracing's potential. In turn, this Comment argues that reassessing Fourth Amendment jurisprudence is necessary not only to promote the right guaranteed by the text of the Fourth Amendment, but also to advance a strong governmental interest in public health and enable the nation to control the

---

86 *Id.*

87 FIGLIOLA, *supra* note 6.

88 Foy, *supra* note 37.

89 GILLMOR, *supra* note 56.

90 FIGLIOLA, *supra* note 6.

91 Foy, *supra* note 37.

92 Ian Barker, *Contact Tracing Apps Raise Privacy Fears*, BETANEWS (Sept. 15, 2020), https://betanews.com/2020/09/15/contact-tracing-privacy-fears/.

93 Farronato et al., *supra* note 27.

94 Foy, *supra* note 37.

95 *Privacy-Preserving Contact Tracing*, APPLE, https://covid19.apple.com/contacttracing (last visited Dec. 17, 2021).

96 Barker, *supra* note 92.

spread of disease and end a pandemic. Finally, this Comment reasons that the Supreme Court should eliminate the *Katz* test, expand the *Carpenter* holding to apply generally to digital location data (including location data captured by Bluetooth technology), and overturn the third-party doctrine.

II. FOURTH AMENDMENT JURISPRUDENCE

A. The Twenty-First Century Plaintiff

"Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause?"[97] These are questions Justice Gorsuch posed in his recent dissent from the Supreme Court's majority opinion in *Carpenter v. United States*.[98] They parallel the questions raised by COVID-19 digital contact tracing in the United States: Can the government demand a record of your location data from Apple and Google without implicating your Fourth Amendment rights? Can it secure this data without a warrant or probable cause? These questions, which lie at the intersection of new technology and the Fourth Amendment, are difficult to answer. The public health benefits of contact tracing add certain intricacies to an already complex analysis.

Contact tracing data could be useful to law enforcement officials in a variety of situations. Location data might put someone at the scene of a crime,[99] establish incriminating communications,[100] or—in the "new normal"[101]—show that an individual violated quarantines measures.[102] Although quarantine measures have not been legally enforced since the early 1900s,[103] every state has codified punishments that range in severity.[104] Individuals in New Hampshire, Mississippi, South Carolina, and Texas, for example, can face felony charges for

---

97 Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).

98 *Id.*

99 United States v. Jones, 565 U.S. 400, 403–04 (2012); *Carpenter*, 138 S. Ct. at 2212.

100 Smith v. Maryland, 442 U.S. 735, 737 (1979).

101 "New normal" is a term that has been used to describe life after the outbreak of COVID-19. Lisa Lockerd Maragakis, *The New Normal and Coronavirus*, JOHNS HOPKINS MED., https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/coronavirus-new-normal (Aug. 14, 2020).

102 Paulina Cachero, *Yes, You Can Face Criminal Charges, Be Fined, and Even Jailed for Breaking a Coronavirus Quarantine*, INSIDER (Mar. 12, 2020, 12:27 PM), https://www.insider.com/breaking-coronavirus-quarantine-in-us-jail-charges-fines-2020-3.

103 *Legal Authorities: Isolation and Quarantine*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/quarantine/aboutlawsregulationsquarantineisolation.html (last visited Dec. 17, 2021).

104 *State Quarantine and Isolation Statutes*, NAT'L CONF. OF STATE LEGS. (Aug. 7, 2021), https://www.ncsl.org/research/health/state-quarantine-and-isolation-statutes.aspx.

knowingly and willfully disobeying a health authority order.[105] In Wyoming, a person can face up to a year in prison or a $10,000 fine.[106] In a case where the government seeks to use contact tracing data to establish this sort of violation, a court would be asked to consider whether the app data implicates the Fourth Amendment and requires a warrant based on probable cause.

B. Katz*,* Smith*,* Jones*, and* Carpenter

The Fourth Amendment limits the government's search and seizure powers. The Amendment provides the following:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[107]

Until the 1960s, the Supreme Court interpreted the Amendment's property-centric text quite literally.[108] In *Olmstead v. United States*, for example, the Supreme Court held that wiretapping without trespass did not amount to a search or seizure within the meaning of the Fourth Amendment.[109] Relying on this decision, the Fourth Amendment would be irrelevant for regulating the use of new technologies to monitor conversations unless the government trespassed on private property to set up the wiretap.[110]

Dissenting, Justice Brandeis reiterated the renowned words of Chief Justice Marshall: "We must never forget . . . that it is a constitution we are expounding."[111] The Fourth Amendment guarantees certain protections and those guarantees, he argued, must be upheld in a "changing world."[112] Quoting from the majority opinion in *Weems v. United States*, Justice Brandeis emphasized that "[t]ime works changes, [and] brings into existence new conditions and purposes," and so, a principle "must be capable of wider application than the mischief which gave it birth."[113] The need for wider

---

105 Cachero, *supra* note 102.

106 *Id.*

107 U.S. CONST. amend. IV.

108 *See* Olmstead v. United States, 277 U.S. 438, 457 (1928); Katz v. United States, 389 U.S. 347, 353 (1967).

109 *Olmstead*, 277 U.S. at 457–58.

110 *See id.*

111 *Id.* at 472 (Brandeis, J., dissenting) (quoting McCulloch v. Maryland, 17 U.S. 316, 407 (1819)).

112 *Id.*

113 *Id.* at 472–73 (citing Weems v. United States, 217 U.S. 349, 373 (1910)).

application of the Fourth Amendment became more apparent as technology continued to advance.

In 1967, the Court overturned *Olmstead*.[114] But instead of simply adapting the Fourth Amendment's protection of "persons, houses, papers, and effects" to accord with modern day intrusions as Justice Brandeis suggested, the Court rejected the property-based approach entirely.[115] In *Katz v. United States*, a seminal case, the Supreme Court held "the Fourth Amendment protects people, not places."[116]

The majority opinion in *Katz* did not lay out a framework for analyzing potential Fourth Amendment violations based on its "people, not places" holding.[117] However, cases that followed relied upon the reasonable expectation of privacy test set forth in Justice Harlan's concurrence.[118] This test asks courts to consider whether "a person ha[s] exhibited an actual (subjective) expectation of privacy" and whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[119] The adoption of Justice Harlan's test transparently underscored privacy as a tenet of Fourth Amendment jurisprudence, even though the word "privacy" does not appear in the text of the Amendment itself.[120]

The *Katz* decision guided the Supreme Court in *Smith v. Maryland* in 1979.[121] This case concerned Patricia McDonough, the victim of a robbery.[122] McDonough gave police officers a description of the person who had robbed her and identified the make and model of the car he was driving.[123] In the days

---

[114] Katz v. United States, 389 U.S. 347, 353 (1967) ("We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").

[115] Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, CATO SUP. CT. REV. 79, 83 (2018).

[116] *Katz*, 389 U.S. at 351.

[117] *Id.*

[118] *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 9 (1968) ("We have recently held [in Katz v. United States] that 'the Fourth Amendment protects people, not places,' and wherever an individual may harbor a reasonable 'expectation of privacy,' he is entitled to be free from unreasonable governmental intrusion." (citations omitted)).

[119] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

[120] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) ("To withdraw protection of this minimum expectation would be to permit police technology to erode the *privacy* guaranteed by the Fourth Amendment." (emphasis added)).

[121] Smith v. Maryland, 442 U.S. 735, 739 (1979).

[122] *Id.* at 737.

[123] *Id.*

following the robbery, McDonough began receiving threatening calls.[124] The caller identified himself as the robber.[125]

Soon after, the police spotted a man who matched McDonough's description and drove the type of car she identified.[126] Officers ran the plates and, after obtaining Smith's name, requested—without a warrant or court order—that the telephone company install a pen register.[127] A pen register is an electronic device that records the numbers dialed from a particular phone number.[128] The pen register revealed Smith made calls to McDonough.[129]

In this case, the pen register was installed on telephone company property so there was no physical intrusion of Smith's property.[130] Nevertheless, Smith sought to exclude evidence of his calls to McDonough, asserting the police violated his Fourth Amendment right when they used the pen register without a warrant.[131] Smith argued he had a "legitimate expectation of privacy" in the phone numbers he dialed from the privacy of his own home.[132] The Court held that "the site of the call [was] immaterial for purposes of analysis in this case," and instead considered what a pen register reveals.[133] Justice Blackmun emphasized the following:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the called and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.[134]

The majority concluded the general public does not have "any actual expectation of privacy in the numbers they dial" because it is understood that telephone companies see those numbers when calls are connected.[135] His conduct was not and could not have been calculated to preserve the privacy of the number he

---

124 *Id.*
125 *Id.*
126 *Id.*
127 *Id.*
128 *Id.*
129 *Id.*
130 *Id.* at 741.
131 *Id.* at 737.
132 *Id.* at 743.
133 *Id.*
134 *Id.* at 741 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).
135 *Id.* at 742.

dialed[136] because numbers dialed are kept in company records and used by companies in a variety of ways.[137] This holding falls under the third-party doctrine, which says "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[138] As such, the Court emphasized that risk is assumed when a person gives information to a third party:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[139]

Furthermore, the Court highlighted the utility of a pen register in identifying persons making annoying or obscene calls and pointed out that most phone books let subscribers know that telephone companies often help law enforcement identify those making "unwelcome and troublesome calls."[140]

The decisions in *Katz* and *Smith* seemed to suggest that privacy concepts superseded property principles in Fourth Amendment jurisprudence. However, in *United States v. Jones*, the Court revitalized the ties between Fourth Amendment jurisprudence and common law trespass (a property-based approach).[141]

In *Jones*, respondent Antoine Jones was the target of a joint FBI and Washington, D.C. Metropolitan Police Department task force.[142] He was suspected of trafficking narcotics.[143] As part of their investigation, law enforcement officials attached a GPS tracking device to a vehicle Jones drove frequently.[144] Using satellite technology, law enforcement tracked the vehicle's

---

136 *Id.* at 743.

137 *Id.* at 741.

138 *Id.* at 743–44.

139 *Id.* at 744 (quoting United States v. Miller 425 U.S. 435, 443 (1976)).

140 *Id.* at 742–43.

141 United States v. Jones, 565 U.S. 400, 405 (2012) ("[O]ur law holds the property of every man so sacred." (citation omitted)).

142 *Id.* at 402.

143 *Id.*

144 *Id.*

location.[145] They collected "more than 2,000 pages of data over [a] 4-week period."[146]

The Court considered whether attachment of a GPS tracking device to the underside of an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements, constituted a search or seizure within the meaning of the Fourth Amendment.[147] Guided by the *Katz* reasonable expectation of privacy test, the Government maintained no search had occurred with respect to the GPS tracking device because Jones did not have a "'reasonable expectation of privacy' in the area of the [vehicle] accessed by Government agents (its underbody) and in the locations of the [vehicle] on the public roads, which were visible to all."[148] The Court did not address this contention.[149] Instead, Justice Scalia, writing for the majority,[150] relied on traditional concepts of property law.[151]

First, the Court held that a vehicle unequivocally qualifies as an "effect" under the Fourth Amendment.[152] Then, Justice Scalia emphasized that in this case, the Government physically intruded on private property to secure the GPS device to the vehicle.[153] He concluded that this physical intrusion undoubtedly amounted to a "search" within the meaning of the Fourth Amendment.[154] Furthermore, Justice Scalia clarified that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[155]

Though the *Jones* decision was unanimous, the Justices were divisively split in their reasoning. Justice Sotomayor joined Justice Scalia's opinion but wrote a pointed concurrence.[156] She affirmed Jones's property right, but also concluded that the government intruded upon privacy interests afforded protection under

---

145 *Id.* at 403.

146 *Id.*

147 *Id.* at 402–03.

148 *Id.* at 406 (citation omitted).

149 *Id.* ("But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (citation omitted)).

150 Chief Justice Roberts, Justice Kennedy, Justice Thomas, and Justice Sotomayor joined the majority opinion. *Id.* at 401.

151 Notably, the decision was unanimous. But Justice Sotomayor and Justice Alito wrote concurring opinions. Justice Breyer, Justice Ginsburg, and Justice Kagan joined Justice Alito's concurrence. *Id.* at 418.

152 *Id.* at 404.

153 *Id.*

154 *Id.* at 404–05.

155 *Id.* at 411.

156 *Id.* at 413 (Sotomayor, J., concurring).

the Fourth Amendment.[157] She emphasized that "*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it."[158] Moreover, Justice Sotomayor criticized both Justice Alito's concurring opinion and the majority opinion.[159] By her measure, Justice Alito's concurrence "discounts altogether the constitutional relevance of the Government's physical intrusion" and the majority's opinion reflects an "irreducible constitutional minimum."[160]

Because the majority did not assess whether GPS monitoring implicates a reasonable expectation of privacy, Justice Sotomayor offered some considerations.[161] She acknowledged that GPS monitoring captures a great deal of public movements.[162] Therefore, she would consider "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[163] Furthermore, her concurrence prompted the Court to reconsider the third-party doctrine.[164] In the digital age, it is commonplace for individuals to voluntarily turn over personal information in the course of everyday activities.[165] Justice Sotomayor suggested the third-party doctrine might be outdated and not representative of actual expectations associated with the voluntary disclosure of information to a third party.[166]

Justice Alito concurred solely in the judgment.[167] He argued that the only factor the Court needs to consider is whether the Government's long-term monitoring violated Jones's reasonable expectation of privacy with respect to his vehicle.[168] According to Justice Alito, *Katz* did away with the old approach requiring a property violation in the form of a trespass.[169] After *Katz*, the question to be decided was not property-related (as Justice Scalia reasoned), but

---

157 *Id.*

158 *Id.* at 414.

159 *Id.*

160 *Id.*

161 *Id.* at 415.

162 *Id.* ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

163 *Id.* at 416.

164 *Id.* at 417.

165 *Id.*

166 *Id.* at 417–18.

167 *Id.* at 418 (Alito, J., concurring in the judgment).

168 *Id.* at 419.

169 *Id.* at 421–22 ("*Katz v. United States* finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation.").

rather whether the potential intrusion violated the privacy upon which the individual justifiably relied.[170]

Justice Alito acknowledged that the *Katz* test is imperfect.[171] He noted that Justice Harlan's test assumes somewhat stable privacy expectations, but in reality, new technology might make it hard to pinpoint fluctuating popular expectations.[172] Justice Alito wrote the following:

> Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[173]

Justice Sotomayor responded to this point, writing that "[p]erhaps . . . some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' and perhaps not."[174]

The Supreme Court's next landmark privacy decision was *Carpenter v. United States*.[175] In *Carpenter*, petitioner Timothy Carpenter challenged the government's use of 12,898 location points cataloging his movements over a 127-day period, which were used to place him near four robberies he was charged with committing.[176] The Court considered whether accessing historical cell phone records that provide the Government with a comprehensive chronicle of the user's past movements constitutes a search under the Fourth Amendment.[177] As the Court explained, cell phones continuously connect to cell sites.[178] Every time a smartphone connects to a cell-site signal it generates a time-stamped location point, which can be used to approximate a phone's physical location.[179]

---

170 *Id.* at 423.
171 *Id.* at 427.
172 *Id.*
173 *Id.*
174 *Id.* at 417–18 (Sotomayor, J., concurring) (citation omitted).
175 Carpenter v. United States, 138 S. Ct. 2206 (2018).
176 *Id*. at 2212.
177 *Id.* at 2211.
178 *Id.*
179 *Id.*

Writing for the majority, Chief Justice Roberts began his analysis summarizing Fourth Amendment doctrine.[180] First, he explained that property rights are one measure, but not the sole measure, of Fourth Amendment violations.[181] He reaffirmed the *Katz* test: when an individual has the subjective intention to preserve something as private, and that expectation of privacy is one society deems reasonable, "[governmental] intrusion into that sphere qualifies as a search and requires a warrant supported by probable cause."[182] The Chief Justice also paid tribute to the Framers' intentions to "secure 'the privacies of life' against 'arbitrary power'"[183] and implement safeguards against "permeating police surveillance."[184]

Then, Chief Justice Roberts highlighted certain characteristics of the data. First, he observed that cell-site records revealing the location of a cell phone is a particular sort of digital data—"personal location information maintained by a third party"—not addressed by existing precedents.[185] He acknowledged that the data was similar to the data in *Jones*.[186] But emphasized that *Jones* was different from the case at hand because it implicated the third-party doctrine, whereby individuals give up their expectation of privacy when they offer information to third parties.[187] Chief Justice Roberts considered societal expectations regarding surveillance in the pre-digital age, the fact that digital data provides such an intimate and comprehensive picture of a person's life (because of our ubiquitous use of cell phones), and the retrospective nature of the digital information (because police do not need to identify a target prior to investigating; the data can be retrieved after the events they document).[188]

---

[180] *Id.* at 2213.

[181] *Id.* (citing Soldal v. Cook County, 506 U.S. 56, 64 (1992)).

[182] *Id.* at 2213 ("For much of our history, Fourth Amendment search doctrine was 'tied to common-law trespass' and focused on whether the Government 'obtains information by physically intruding on a constitutionally protected area.' More recently, the Court has recognized that 'property rights are not the sole measure of Fourth Amendment violations.'" (quoting United States v. Jones, 565 U.S. 400, 405, 406 n.3 (2012) and *Soldal*, 506 U.S. at 64)).

[183] *Id.* at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[184] *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

[185] *Id.*

[186] *Id.* at 2216 ("Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.").

[187] *Id.* (citing United States v. Miller, 425, U.S. 435 (1976) (where the Court found no reasonable expectation of privacy in financial records accessible to a third-party bank) and Smith v. Maryland, 442 U.S. 735 (1979) (where the Court found no reasonable expectation of privacy in records of phone numbers dialed accessible to a third-party telephone company)).

[188] *Id.* at 2218.

Although the *Carpenter* Court did not overrule the third-party doctrine, it did not apply the doctrine to the presented circumstances.[189] Before *Carpenter*, the third-party doctrine seemed relatively clear (despite Justice Sotomayor's attempt to poke holes[190])—information revealed to a third party and then conveyed to Government authorities loses any Fourth Amendment protection normally afforded.[191] In *Carpenter*, the Court decided the unique nature of cell phone location records meant the involvement of a third party could not, on its own, overcome Carpenter's claim to Fourth Amendment protection.[192] The Court decided an individual maintains a legitimate expectation of privacy in physical movements recorded in cell-site location information whether the Government obtains the information through its own surveillance or indirectly from a wireless carrier.[193] Chief Justice Roberts reasoned that cell phone location data "is not truly 'shared' as one normally understands the term."[194] In some sense, this was not just a decision about the application of the doctrine, but a departure from it. The third-party doctrine rests on "the [idea] that an individual has a reduced expectation of privacy in information [they] knowingly share[s]."[195] But here, the Court looked beyond the act of sharing to the type of information shared and whether a legitimate expectation of privacy attaches.[196] Looking to the type of information shared has huge—albeit unclear—implications, given that 2.5 quintillion bytes of data are produced by humans every day.[197] *Carpenter* is still considered "one of the most consequential rulings regarding privacy in the digital age."[198]

C. The Special Needs Doctrine

In addition to being governed by *Katz*, *Smith*, *Jones*, and *Carpenter*, privacy in the digital age is affected by the special needs doctrine, which developed in a

---

189 *Id.* at 2220 ("We therefore decline to extend *Smith* and *Miller* to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection.").

190 United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

191 Smith v. Maryland, 442 U.S. 735, 744 (1979).

192 *Carpenter*, 138 S. Ct. at 2217.

193 *Id.*

194 *Id.* at 2220.

195 *Id.* at 2219.

196 *Id.* (citing United States v. Miller, 425 U.S. 435, 442 (1976)).

197 Jacquelyn Bulao, *How Much Data Is Created Every Day in 2021?*, TECHJURY, https://techjury.net/blog/how-much-data-is-created-every-day/#gref (Dec. 7, 2021).

198 Nathan Freed Wessler, *The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In*, ACLU (June 28, 2019, 4:30 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-most-consequential-ruling-privacy-digital.

separate line of cases.[199] The special needs doctrine is an exception to the Fourth Amendment's requirement that law enforcement obtain a warrant based on probable cause prior to conducting a search or seizure.[200] A search or seizure qualifies for this exception when there is a perceived need that falls outside the bounds of normal law enforcement and involves an important governmental interest.[201] This exception is not granted often.[202] The following section will apply Fourth Amendment doctrine as it has developed in *Katz*, *Smith*, *Jones*, and *Carpenter* to digital contact tracing technology. It will also address the third-party doctrine and special needs doctrine because individuals voluntarily give contact tracing app information to a third-party entity and the context of a global pandemic, though unprecedented, might amount to a special need.

III. APPLYING CURRENT FOURTH AMENDMENT JURISPRUDENCE

There are inherent difficulties in interpreting the Fourth Amendment. The text is ambiguous and new technologies create circumstances beyond anything the framers might have considered.[203] In theory, Fourth Amendment jurisprudence, delineated in *Katz*, *Smith*, *Jones*, and *Carpenter*, provides an analytical framework. However, applying Fourth Amendment jurisprudence to contact tracing apps raises several questions. At best, these questions are not answered by existing cases. At worst, they demonstrate profound flaws in Fourth Amendment doctrine.

A. Katz *and Contact Tracing: Perhaps and Perhaps Not*

In the United States, contact tracing apps are downloaded by the user.[204] They implicate the mere transmission of electronic signals without trespass, as described by Justice Scalia in *Jones*.[205] Therefore, whether the use of digital data collected via contact tracing apps constitutes a search within the meaning of the Fourth Amendment would be subject to a *Katz* analysis.[206] In a case involving

---

199 *See* Lauren Kobrick, *I Am Not Law Enforcement! Why the Special Needs Exception to the Fourth Amendment Should Apply to Caseworkers Investigating Allegations of Child Abuse*, 38 CARDOZO L. REV. 1505, 1509 (2017).

200 *Id.*

201 *Id.*

202 Off. State Att'y, W. Palm Beach, Fla., *Special Needs Exception*, LEGAL EAGLE (Aug. 2014), http://www.sa15.state.fl.us/stateattorney/ResourceInformation/_content/LegalEagle2014/Aug2014.pdf.

203 David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L. 581, 581 ("The doctrinal incoherence of Fourth Amendment law disturbs many judges and scholars.").

204 FIGLIOLA, *supra* note 6.

205 United States v. Jones, 565 U.S. 400, 411 (2012).

206 *Id.*

the government's collection of contact tracing data, a Court must consider whether "a person exhibited an actual (subjective) expectation of privacy" and whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[207]

Notably, the first prong of the *Katz* test has been criticized by legal scholars, even outside the context of contact tracing. Many argue that a constitutional right should not rest on an individual's subjective understanding.[208] For example, according to Professor Anthony Amsterdam, "An actual, subjective expectation of privacy obviously has no place in a statement of what *Katz* held or in a theory of what the fourth amendment protects. It can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection."[209] Still, the *Katz* test remains the law. So, we must ask whether digital contact tracing app users "exhibit an actual (subjective) expectation of privacy."[210]

As discussed in Part I, the opt-in nature of contact tracing apps has been at the forefront of all digital contact tracing conversations.[211] Agreements emphasize that users must opt in to data collection and can opt out at any point.[212] A diagnosis is only captured when a user chooses to report it.[213] In addition, app developers have stressed that information collected will remain private.[214] The apps are clearly designed and marketed to make people feel in control of their personal information.[215] Arguably then, users exhibit an actual (subjective) expectation of privacy. There is a general understanding that their digital data is only being collected for a public health-related purpose and will not be dispersed for other reasons.

However, the opt-in feature is only emphasized in user agreements and press coverage because privacy concerns have also been at the forefront of conversations surrounding this technology.[216] A typical app user understands that downloading, using, and reporting results via contact tracing apps is a choice because that choice puts their privacy at some risk.[217] In fact, the privacy

---

207 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

208 Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974).

209 *Id.*

210 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

211 *Supra* Part I.E.

212 Brian Fung, *Apple and Google's Contact Tracing System Gets Deeper Integration into iOS, Android*, CNN BUS., https://www.cnn.com/2020/09/01/tech/apple-google-contact-tracing/index.html (Sept. 1, 2020).

213 *Id.*

214 Press Release, Apple & Google, *supra* note 44.

215 *Id.*

216 Foy, *supra* note 37.

217 Lehmann, *supra* note 79.

framework for Apple and Google informs users of the following: "Information such as location history, symptom reports, demographic information, or similar shared with public health officials or researchers must never be linked back to or used to re-identify individuals, even by entities legally allowed to perform such linkage."[218] At first glance, this might seem to offer privacy protections. But on its face, this statement clearly indicates that there might be entities legally allowed to link private information to users.[219] Therefore, if presented with a digital contact tracing case, a Court might find that the user did not exhibit an actual (subjective) expectation of privacy because there is so much information circulating about how *un-private* these apps are.

The second prong of the *Katz* test asks whether "the expectation of privacy [is] one that society is prepared to recognize as 'reasonable.'"[220] In the case of digital contact tracing, the issues raised by this prong are similar to those raised by the first prong of the *Katz* test.[221] The technology is so new that society's expectations are just as unformed as the expectations of individuals. If the general public is encouraged to use these apps—touted as being "designed with privacy in mind"—is there an expectation that privacy is protected or that privacy is at stake despite best intentions?

Ultimately, there is no clear answer. As Justice Sotomayor proclaimed in *Jones*, in an attempt to apply the *Katz* test, "Perhaps, some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' and perhaps not."[222]

B. Smith *and Contact Tracing: It's Ambiguous*

Under the existing rollout of digital contact tracing in the United States, Apple and Google control a central server where contact data is stored.[223] Therefore, the third-party doctrine requires some consideration. According to this doctrine, "[a] person has no legitimate expectation of privacy in information

---

[218] *Data Rights for Exposure Notification*, EXPOSURE NOTIFICATION, http://exposurenotification.org/ (May 20, 2020).

[219] *Id.*

[220] Smith v. Maryland, 442 U.S. 735, 743 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

[221] The two prongs—whether "a person ha[s] exhibited an actual (subjective) expectation of privacy and whether the expectation" is "one that society is prepared to recognize as 'reasonable'"—are equally ambiguous. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[222] United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring).

[223] Barber, *supra* note 47.

he voluntarily turns over to third parties."[224] When information is shared, the risk might be assumed.[225]

The *Katz* reasonable expectation of privacy test and the third-party doctrine were applied to new technologies in *Smith* and *Carpenter*.[226] Therefore, these cases offer precedential value for assessing digital contact tracing apps under the Fourth Amendment. In the following paragraphs, this Comment will discuss why the case of digital contact tracing is similar to *Smith* (where the Supreme Court held there was no legitimate expectation of privacy)[227] and how it might be distinguished from *Carpenter* (where the Supreme Court held there was a legitimate expectation of privacy).[228]

Smith presents a similar case to digital contact tracing because (1) the information revealed was ambiguous,[229] (2) there was a public interest in collecting the information,[230] and (3) there was notice to users about access by other entities.[231] In *Smith*, the Supreme Court decided that installation and use of a pen register did not require a warrant.[232] Digital contact tracing apps and the pen register implicated in *Smith* share certain commonalities. Like pen registers, contact tracing apps reveal parties that have come in contact with each other.[233] Of course, contacts recorded by these technologies might mean different things—a pen register's records imply communication between parties,[234] whereas contact tracing data captures physical proximity and includes circumstances where parties may have been close enough to spread COVID-19 but never actually engaged in conversation.[235] Still, the pen register and contact tracing apps are similar in that they capture some sort of interaction. And the ambiguity involved in each makes these recorded contacts more alike for purposes of Fourth Amendment analysis. In each case, much about the interaction documented by the technology is left undisclosed. According to the Court in *Smith*, the pen register data was somewhat ambiguous because "[n]either the purport of any communication between the called and the recipient

---

224 *Smith*, 442 U.S. at 743–44.
225 *Id.* at 744.
226 *Id.* at 740–44; Carpenter v. United States, 138 S. Ct. 2206, 2213–16 (2018).
227 *Smith*, 442 U.S. at 745.
228 *Carpenter*, 138 S. Ct. at 2219.
229 *Smith*, 442 U.S. at 741.
230 *Id.* at 742.
231 *Id.* at 743.
232 *Id.* at 745–46.
233 Press Release, Apple & Google, *supra* note 44.
234 *Smith*, 442 U.S. at 741.
235 Press Release, Apple & Google, *supra* note 44.

of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[236] The same can be said of contact tracing apps. The conversation is not recorded, the parties are anonymous,[237] and whether substantial interaction occurred is unclear.

Pen registers and contact tracing are also similar because the information collected by each serves a state interest. In *Smith*, the Supreme Court noted that pen registers might be helpful in identifying parties making annoying or obscene calls when deciding whether a Fourth Amendment violation had occurred.[238] Indisputably, the state interest served through contact tracing apps is much more serious and pressing. Worldwide, COVID-19 caused over 5 million deaths and over 200 million more have suffered from non-fatal cases.[239] It must not be forgotten that contact tracing apps are a response to these deaths. Both research and global anecdotes indicate apps have potential when it comes to flattening the curve and saving lives and could serve their greatest purpose when society reopens and people are out and about but still risk spreading disease.[240] Although the *Smith* Court was not explicit about how state interest factored into its assessment of whether a legitimate expectation of privacy existed,[241] its inclusion of this fact suggests it is a valid, if not important, consideration. Whether digital contact tracing involves a legitimate expectation of privacy and whether the data can be obtained without a warrant would involve some attention to the public health crisis and the social need this technology attempts to address.

Finally, the *Smith* Court stressed that phone books indicated to subscribers that telephone companies often help law enforcement officers identify those making unwanted calls.[242] Ultimately, the Court decided the use of a pen register did not violate an individual's Fourth Amendment right, and law enforcement could collect that data without a warrant and use it as evidence against a defendant in a criminal case.[243] Again, a comparison can be drawn between this fact and contact tracing as it has been implemented in the United States. Written disclaimers for Apple and Google's digital contact tracing technology suggest there are some entities legally allowed to de-anonymize the information

---

236 *Smith*, 442 U.S. at 741 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

237 Press Release, Apple & Google, *supra* note 44.

238 *Smith*, 442 U.S. at 743.

239 *Mortality Analyses*, *supra* note 65.

240 Mia Sato, *Contact Tracing Apps Now Cover Nearly Half of America. It's Not Too Late to Use One*, MIT TECH. REV. (Dec. 14, 2020), https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/.

241 *See Smith*, 442 U.S. at 742–43.

242 *Id.* at 742 (citing United States v. N.Y. Tel. Co., 434 U.S. 159, 174–75 (1977)).

243 *Id.* at 745–46.

collected.[244] Based on those disclaimers and the public's knowledge surrounding the purpose of these apps, law enforcement could probably use contact tracing data without a warrant for any purpose, whether it be sufficiently related to public health or for the advancement of other law enforcement objectives, like those of the officers in *Smith*.[245]

C. Carpenter *and Contact Tracing: "Shared" as One Normally Understands*

Carpenter involved technology—new to society and the Court—with similarities to contact tracing technology.[246] In *Carpenter*, the Supreme Court decided the government conducts a search under the Fourth Amendment when it accesses historical cell phone records that chronicle its user's detailed movements.[247] In some ways, it might seem like the *Carpenter* decision would foreclose an outcome in any case involving digital contact tracing through smartphones because the data implicated appears to be quite similar. But that case was narrowly decided, applying only to real-time cell-site location information.[248] Digital contact tracing data bears similarities to cell-site location information because it reveals information about a user's location, but there are marked differences in the ways these data sets are collected.[249] In the context of digital contact tracing, *Carpenter* is distinguishable because contact tracing data (1) is truly shared and is understood to reveal some location information, (2) is less intrusive than GPS-data collection, and (3) involves some natural limit, or application to a specific circumstance.[250]

First, as the Court asserted, the location information in *Carpenter* was not information "truly 'shared' as one normally understands the term."[251] The data at issue in *Carpenter* was collected "without any affirmative act on the part of the user" beyond simply using the cell phone.[252] The Court reasoned that

---

244 *Data Rights for Exposure Notification*, *supra* note 218.

245 *Smith*, 442 U.S. at 737.

246 Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

247 *Id.* at 2220.

248 *Id.* ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval).").

249 *Data Rights for Exposure Notification*, *supra* note 218.

250 *Compare Carpenter*, 138 S. Ct. at 2216–18 (involving GPS-data that was not "truly shared" and involved no natural limit), *with* Press Release, Apple & Google, *supra* note 44 (noting that app users choose to share location data via Bluetooth technology for the specific purpose of combatting COVID-19).

251 *Carpenter*, 138 S. Ct. at 2220.

252 *Id.* ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates.").

carrying a cell phone is so commonplace that it is almost necessary to "participation in modern society."[253] Therefore, the Court concluded, Carpenter maintained privacy in his cell phone location information because there had been no meaningful assumption of risk.[254] Carpenter's location was recorded without his explicit permission.[255]

In contrast, digital contact tracing requires an affirmative act on the part of the user. Citizens must opt in by downloading the app or activating its use.[256] Users' information, therefore, is "truly shared" as one normally understands the term[257]—in choosing to use the app, which has a specific purpose, users are opting to share their location information so that it can be compared with the location information of other users.[258] The developers of contact tracing apps—namely Apple and Google in the United States—and activists alike have assured users that contact tracing apps are entirely voluntary.[259] In fact, the voluntary nature of the apps dominates press on this issue in the hope that it will promote buy-in.[260] This aspect of the technology has serious implications under a *Katz* analysis. If users have to opt in when installing the contact tracing app on their mobile devices, once they turn on their phones' Bluetooth capabilities and upload their personal data to the database, they arguably have no subjective expectation of privacy. The first part of Justice Harlan's reasonable expectation of privacy test[261] would have to be answered in the negative. Moreover, users must continue opting in each step of the way, making it abundantly clear to all involved that use of the app is a choice.[262] And even though contact tracing apps are downloaded onto phones, they are distinct from the functioning of the phone itself.[263] While there may be morality-based reasons to use these apps—since public health experts call for widespread adoption of the technology[264]—they are not so ubiquitous or socially expected as to be equivalent to the use of phones generally.[265] Finally, every person who downloads the app can stop sharing data

---

253 *Id.*

254 *Id.* ("[I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

255 *Id.*

256 *Data Rights for Exposure Notification*, *supra* note 218.

257 Chief Justice Roberts considered what it truly means to share data when determining whether an individual had a legitimate expectation of privacy. *Carpenter*, 138 S. Ct. at 2220.

258 *Data Rights for Exposure Notification*, *supra* note 218.

259 Press Release, Apple & Google, *supra* note 44.

260 Foy, *supra* note 37.

261 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

262 Foy, *supra* note 37.

263 *Id.*

264 O'Neill, *supra* note 24.

265 Morse, *supra* note 29.

during particular moments in time or completely delete the technology from their device as they see fit—even though this would limit the usefulness of the contact tracing data.[266]

Second, Apple and Google have asserted that their contact tracing apps are less intrusive than GPS tracking. In *Carpenter*, the Court specifically discussed the "unique nature" of cell phone location records.[267] These records are "detailed, encyclopedic, and effortlessly compiled" because phones are, for the most part, always on an individual's person.[268] The Court decided that Carpenter maintained a reasonable expectation of privacy in his physical location, even though those records were generated for commercial purposes by the carriers, because of this unique nature.[269] Digital contact tracing is distinguishable because tracing technology might be seen as more "rudimentary"[270] than cell-site location information. The Court in *Carpenter* concluded tracking made possible with cell-site location data is, for the purposes of its analysis, equivalent to GPS monitoring.[271] When it comes to contact tracing, app developers with the most prominence in the United States have incontrovertibly differentiated their technology from GPS monitoring.[272] Developers insist that Bluetooth signals are more privacy-friendly than GPS data because Bluetooth signals show the proximity of two users, not an estimate of a user's locations.[273] This contention—that Bluetooth technology protects data privacy more than GPS technology—might mean that under Fourth Amendment analysis, contact tracing data would be classified as less intrusive than the information in *Carpenter*. But it does not take much imagination to see how digital proximity data might be used to determine a person's location, even if in a more roundabout way,[274] or how it directly provides location data if one considers the installation of Bluetooth beacons in various locations.[275] With this in mind, it is

---

266 Press Release, Apple & Google, *supra* note 44.

267 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

268 *Id.* at 2216.

269 *Id.* at 2217 ("Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life . . . .").

270 The Court distinguished cell-site location information from less "sweeping modes of surveillance." *Id.* at 2215.

271 *Id.* at 2217–18.

272 Press Release, Apple & Google, *supra* note 44, at 2–3.

273 FIGLIOLA, *supra* note 6.

274 Christopher McFadden, *Are You Being Tracked by Bluetooth Beacons While Shopping?*, INTERESTING ENG'G (June 20, 2019), https://interestingengineering.com/are-you-being-tracked-by-bluetooth-beacons-while-shopping#:~:text=Unlike%20other%20location%20services%2C%20like,and%20work%20incredibly%20well%20indoors.

275 *Id.*

clear that Bluetooth data yields a pretty comprehensive picture of a person's life, but is probably outside the bounds of protection offered by the Fourth Amendment under Supreme Court precedent, particularly *Carpenter*.[276]

In addition, the purpose for which contact tracing data is collected and stored is the physical location data itself.[277] Therefore, determining that there is an expectation of privacy in those physical locations is not as straightforward as it was in *Carpenter*, where the user's reason for using the technology was unrelated to and not dependent on the company's collection of location data.[278] A court might conclude that the very specific function of these apps results in a different outcome with respect to whether the third-party doctrine overcomes the user's claim to Fourth Amendment protection.

Third, contact tracing and the information at issue in *Carpenter* can be distinguished by the idea of a natural limit.[279] In *Carpenter*, the Court placed significance on the fact that the cell-site records at issue were retrospective.[280] Police officers do not need an established suspect from the outset to make use of cell-site data.[281] Instead, information concerning movements can be retrieved after the person has become the suspect in an investigation[282]—as was the case in *Carpenter*, where law enforcement used Carpenter's phone signals to place him near robberies he was later charged with committing.[283] The Court remarked that because there is no natural limit on this information and because it is extremely revealing, the information should be protected by the Fourth Amendment.[284]

Contact tracing might be viewed differently. First, if contact tracing data was used in a case involving a health-related criminal violation, the Court might determine that this specified charge imposes some sort of natural limit. Instead of being used for a purpose entirely unrelated to the initial reason data was collected, the law enforcement purpose could be rationally linked to the particular purpose the user had in downloading the technology.[285] Second, it

---

276 *Carpenter*, 138 S. Ct. at 2220.

277 *See* Press Release, Apple & Google, *supra* note 44, at 3.

278 *Carpenter*, 138 S. Ct. at 2220.

279 *Id.* at 2218.

280 *Id.*

281 *Id.*

282 *Id.* at 2220 ("[T]his case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years.").

283 *Id.* at 2218.

284 *Id.*

285 For example, law enforcement purpose could be rationally linked to the particular purpose the user had

could be argued that another limit is imposed by the certain context in which these apps are used. Although contact tracing is a smartphone app that lives on an individual's phone, it is not something that society imagines as having an indefinite purpose, like the smartphone itself.[286] The apps are only useful for as long as a virus poses a threat.[287] Furthermore, while cell-site location data is "ever alert,"[288] an individual using contact tracing technology always has the option of turning off the app for a short-term or long-term period.[289] This type of control might distinguish the data collected via contact tracing from the data before the Court in *Carpenter*.[290]

Fourth and finally, in *Carpenter*, the Court considered how the data at issue captured public movements.[291] The Court cited to one of its earlier cases, *United States v. Knotts*, where it was held that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[292] In *Knotts*, the Court declared the government's use of a beeper to track a vehicle's movements did not constitute a search under the Fourth Amendment because those movements would have been visible to anyone with an interest.[293] Therefore, "Knotts could not assert a privacy interest in the information obtained."[294] But the *Carpenter* Court distinguished the case at hand from *Knotts*, with guidance from *Jones*, based on the pervasiveness of the surveillance.[295] The Court reasoned that the government's tracking of Knotts in a particular automotive journey was far less invasive than the long-term surveillance disputed in *Carpenter*.[296] Imposing this analysis on a contact tracing context, authorities might first argue that contact tracing only reveals information that would have been publicly available.[297] That argument would probably fail given the *Carpenter* analysis.[298] But, in the context of quarantine-related charges, proponents of a valid search or seizure might contend that the

---

if the government uses contact tracing data as evidence that an individual violated quarantine measures.

[286] *See Privacy-Preserving Contact Tracing*, *supra* note 95 (announcing Apple's partnership with Google to "slow the spread of COVID-19 and accelerate the return of everyday life").

[287] *See id.* (announcing a collaborative agreement between Apple and Google to use technology "to help governments and health agencies reduce the spread of the virus").

[288] *Carpenter*, 138 S. Ct. at 2219.

[289] Press Release, Apple & Google, *supra* note 44, at 5.

[290] *Carpenter*, 138 S. Ct. at 2220.

[291] *Id.* at 2218.

[292] *Id.* at 2215 (quoting United States v. Knotts, 460 U.S. 276, 281–82 (1983)).

[293] *Id.* at 2219–20.

[294] *Id.* at 2215.

[295] *Id.* at 2219–20.

[296] *Id.*

[297] *See Digital Contact Tracing Tools*, *supra* note 83.

[298] *Carpenter*, 138 S. Ct. at 2220.

intrusion is more limited, like in *Knotts*,[299] if it pertains to the site and fallout of a specific incident of exposure, instead of an individual's entire location history.

D. The Special Needs Doctrine

Outside of the discussions raised by *Smith* and *Carpenter*, another consideration is whether the search and seizure that might arise from contact tracing qualifies for a special needs exception. The answer to this question likely rests on the specific aim for which the contact tracing data was used in a given case.[300] If the data was needed for a health-related purposes "beyond the normal need for law enforcement,"[301] then there might be an exception to the warrant requirement. The Supreme Court has not recognized disease control within the nation as a special need in previous Fourth Amendment cases; but, given the severe consequences of the COVID-19 pandemic, disease control could fit under a general need for public safety.[302] Analysis in the COVID-19 context might also differ because police officers are usually the only ones privy to the needs at hand. Public recognition of a special need—an efficient contact tracing system—might also factor in, either under an analysis of the special needs doctrine or the general analysis of an individual's subjective expectation of privacy and society's objective allowance[303] regarding this expectation.

Ultimately, whether digital contact tracing entails a legitimate expectation of privacy is unclear. The information revealed is ambiguous, advances a public health interest, provides notice to users that it might be used by other entities,[304] and is perceived by society as "unsafe" with respect to app privacy—hence the low adoption rates.[305] The data is "truly shared,"[306] reveals location information, is distinct from GPS data, and comes with some natural limit, or pertinence to specific COVID-19-related circumstances.[307] So, it seems probable that an expectation of privacy would be deemed unreasonable. On the other hand, it seems counter-intuitive to say society is not prepared to recognize expectations of privacy associated with life-saving technology that requires people to volunteer information—especially under an analysis that purports to be reasonable. If the state has an interest in promoting public health and saving

---

299 *Id.* at 2219–20.
300 Ferguson v. City of Charleston, 532 U.S. 67, 78–81 (2001).
301 New Jersey v. T.L.O, 469 U.S. 325, 351–53 (1985) (Blackmun, J., concurring).
302 *Mortality Analyses*, *supra* note 65.
303 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
304 *Data Rights for Exposure Notification*, *supra* note 218.
305 Lehmann, *supra* note 79.
306 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
307 Press Release, Apple & Google, *supra* note 44, at 2–3, 5.

lives, and Supreme Court cases cannot be applied with clarity to this novel situation, Fourth Amendment jurisprudence should be reconsidered.

IV. AN ALTERNATIVE THEORY OF FOURTH AMENDMENT JURISPRUDENCE

A logical place to start in developing an alternative theory of Fourth Amendment jurisprudence is with the concurrences in *Jones* and the dissents in *Carpenter*. These opinions highlight frustration, and, at times, indignation, with current Fourth Amendment jurisprudence.[308]

A. Concurrences and Dissents in Jones *and* Carpenter

In *Jones*, Justice Alito and Justice Sotomayor discussed broad ideas surrounding new technologies and privacy in their respective concurring opinions. Justice Alito suggested that new technology may provide increased convenience or security at the expense of privacy, but that society might consider this tradeoff worthwhile, or, at the very least, inevitable.[309] In response, Justice Sotomayor urged that it might be time to reconsider the third-party doctrine, calling that "approach ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[310] In contrast to Justice Alito, she remarked that the public might not be willing to accept the diminution of privacy as inevitable.[311]

The points raised in the four *Carpenter* dissents are applicable and give a fuller picture of the strongest contentions on each side of the debate in *Carpenter*. The dissents represent proposals or support for other methods of analysis that differ from current Fourth Amendment jurisprudence in the ways it is understood and misunderstood.[312]

Justice Kennedy's dissenting opinion[313] asserted that cell-site records are of the same variety as many other kinds of business records the government has a

---

[308] United States v. Jones, 565 U.S. 400, 413–18 (2012) (Sotomayor, J., concurring); *id.* at 418–31 (Alito, J., concurring in the judgment); *Carpenter*, 138 S. Ct. at 2223–35 (Kennedy, J., dissenting); *id.* at 2235–46 (Thomas, J., dissenting); *id.* at 2246–61 (Alito, J., dissenting); *id.* at 2261–72 (Gorsuch, J., dissenting).

[309] *Jones*, 565 U.S. at 427 (Alito, J., concurring in the judgment).

[310] *Id.* at 417 (Sotomayor, J., concurring).

[311] *Id.* at 417–18.

[312] *Carpenter,* 138 S. Ct. at 2223–35 (Kennedy, J., dissenting); *id.* at 2235–46 (Thomas, J., dissenting); *id.* at 2246–61 (Alito, J., dissenting); *id.* at 2261–72 (Gorsuch, J., dissenting).

[313] Justices Thomas and Alito joined Justice Kennedy's dissent. *Id.* at 2223, 2229–30, 2235 (Kennedy, J., dissenting).

lawful right to obtain.[314] Justice Kennedy concluded that Carpenter did not own, possess, control, or use the contested records, and for that reason Carpenter had no reasonable expectation that disclosure of these records would require a warrant.[315] He argued that the majority's decision offered inconsistent protections,[316] and he would instead limit the Fourth Amendment to its property-based origins.[317] Further, with respect to the cell-site data, he concluded that location information, which is often disclosed to the public at large, is not more private than financial and telephonic records, which are available without a warrant.[318]

Justice Thomas's dissenting opinion emphasized the property-based approach to Fourth Amendment questions.[319] In Justice Thomas's view, the case could not be resolved by asking whether a search occurred.[320] Instead, he argued the case should turn on whose property was searched.[321] Justice Thomas argued overtly that *Katz* should be rejected and concluded *Carpenter* involved no Fourth Amendment violation because the information retrieved did not belong to Carpenter.[322]

Justice Alito's dissenting opinion[323] distinguished between an actual search involving law enforcement officers entering private premises and an order "merely requiring a party to look through its own records and produce specified documents"—with the former being more intrusive than the latter.[324] Justice Alito criticized the majority for broadening the Fourth Amendment's reach and departing from long-established tradition.[325] He emphasized that the *Carpenter* decision inappropriately "allow[ed] a defendant to object to the search of a third party's property."[326] He defended this point with reference to the text of the

---

[314] *Id.* at 2223 (Kennedy, J., dissenting) ("The Court has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party.").

[315] *Id.* at 2228–29.

[316] *Id.* at 2224 ("[I]t draws an unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other. . . . That distinction is illogical and will frustrate principled application of the Fourth Amendment in many routine yet vital law enforcement operations.").

[317] *Id.* at 2235.

[318] *Id.* at 2233.

[319] *Id.* at 2235 (Thomas, J., dissenting) ("This case . . . should turn on . . . *whose* property was searched. . . . By obtaining the cell-site records of MetroPCS and Sprint, the Government did not search Carpenter's property.").

[320] *Id.*

[321] *Id.*

[322] *Id.* at 2235–36.

[323] *Id.* at 2246 (Alito, J., dissenting).

[324] *Id.* at 2247.

[325] *Id.*

[326] *Id.*

Amendment, asserting that "[t]he Fourth Amendment protects '[t]he right of the people to be secure in *their* persons, houses, papers, and effects' . . . , not the persons, houses, papers and effects of others."[327] According to Justice Alito, the third-party doctrine is not a new, judge-made theory.[328] Rather, it is a direct reading of what the Amendment protects.[329]

Finally, Justice Gorsuch's dissenting opinion[330] disagreed with the majority's notion that the third-party doctrine could be overcome based on the nature of the information.[331] Instead, he read *Smith* and *Miller* as having announced a categorical rule that was likely misguided.[332] Justice Gorsuch also asserted that the *Katz* test is neither sufficiently justified nor successful.[333] However, in his view, a solution exists:[334] returning to the traditional approach.[335] Under the traditional approach, the Fourth Amendment was triggered simply if the house, paper, or effect belonged to the individual claiming a violation.[336] And protections for papers and effects did not dissipate just because they were shared with other parties.[337]

In short, all four *Carpenter* dissents suggested alternate ways of interpreting the Fourth Amendment and proposed that the Court go in a different direction.

B. A Needed "New Normal"

The failure of digital contact tracing in the United States—despite the pressing need presented by the COVID-19 pandemic—highlights significant flaws in Fourth Amendment jurisprudence. Even though changes to the Fourth Amendment framework might not encourage privacy-minded Americans to opt in to life-saving technology, the Americans who do opt in should be afforded reasonable Fourth Amendment protections. Currently, precedents do the opposite.

---

327 *Id.* (quoting U.S. CONST. amend. IV).

328 *Id.* at 2255.

329 *Id.*

330 *Id.* at 2261 (Gorsuch, J., dissenting).

331 *Id.* at 2262.

332 *Id.*

333 *Id.* at 2264–65.

334 *Id.* at 2262 (suggesting the Court could "maintain *Smith* and *Miller*, and live with the consequences," "set *Smith* and *Miller* aside and try again using the *Katz* 'reasonable expectation of privacy' jurisprudence," or "look for answers elsewhere").

335 *Id.* at 2267–71.

336 *Id.* at 2267–68.

337 *Id.* at 2268 ("[T]he fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them . . . . Entrusting your stuff to others is a *bailment*.").

First, the *Katz* test should be overturned. Digital contact tracing aside, a constitutional right should not rest on an individual's subjective expectation of privacy.[338] When digital contact tracing is considered, the subjective nature of the test is entirely unworkable. As Justice Alito pointed out, technology changes dramatically all the time.[339] It is almost inevitable that "popular expectations" will consistently be in flux.[340] Press coverage surrounding contact tracing apps highlights real-time fluctuation. And in this period of flux, whether it is more reasonable to consider the data private or public is anyone's guess. Any attempt to answer this question—the question posed by the *Katz* test[341]—is not appropriately founded on legal, or even normative, reasoning.

In addition, the *Katz* test results in bad policy. Justice Alito suggested that many will find privacy tradeoffs worthwhile as technology advances,[342] but this has not been the case with respect to digital contact tracing. In the United States, adoption of digital contact tracing has been much lower than in other countries,[343] which is reflected in the United States' absolute and relative failure in responding to COVID-19.[344] As Justice Sotomayor said, "Perhaps . . . some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' and perhaps not."[345] Surveys show that privacy is a concern for the majority of Americans.[346] Attempting to base Fourth Amendment protections on reasonable expectations of privacy tradeoffs is too arbitrary and leaves individuals feeling unprotected. Understanding how beneficial and needed new technologies can be, it stands to reason that the law surrounding these technologies should encourage participation, not make citizens wary.

Second, the Court should overturn the third-party doctrine. As Justice Sotomayor noted, the doctrine no longer functions.[347] Today, relinquishment of personal information is required in too many instances to make the third-party doctrine worthwhile. As Chief Justice Roberts reasoned, "Cell phone location

---

338 Amsterdam, *supra* note 208, at 384.

339 United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring in the judgment).

340 *Id.*

341 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

342 *Jones*, 565 U.S. at 427 (Alito, J., concurring in the judgment).

343 Lehmann, *supra* note 79.

344 Barber, *supra* note 47.

345 *Jones*, 565 U.S. at 417–18.

346 Brooke Auxier, *How Americans See Digital Privacy Issues Amid the COVID-19 Outbreak*, PEW RSCH. CTR. (May 4, 2020), https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/.

347 *Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring).

information is not really 'shared' as one normally understands the term."[348] Justice Kennedy noted that "draw[ing] an unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other" is illogical.[349] And Justice Gorsuch acknowledged "the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them."[350] In the modern era, data circulates from party to party without much intention or thought, so elimination of this doctrine is more true to the original rationale for the doctrine itself.[351]

Third and finally, the limited holding in *Carpenter*—specific to cell-site location information[352]—should be extended. Bluetooth data, both in the context of digital contact tracing and in other contexts, is not really "shared." Although the information it provides is more ambiguous than cell-site location information or GPS data, the Court should acknowledge that Bluetooth data can be used to create "social graphs" that unveil a user's social interactions[353] and that this indirect access violates the Fourth Amendment to the same extent as free flowing location data.

CONCLUSION

Dissents and concurrences in Fourth Amendment digital technology cases highlight frustration, and at times indignation, with current Fourth Amendment jurisprudence. Digital contact tracing—and a desire to make it more attractive to individuals for the sake of public health—provides clear justifications for making changes to the existing Fourth Amendment framework. A "new normal" in Fourth Amendment jurisprudence will help ensure the government is able to not only protect Fourth Amendment rights but also promote public health and save lives.

As it stands, Fourth Amendment jurisprudence forces U.S. citizens to choose between health and privacy. Eliminating the *Katz* test and the third-party doctrine might not result in widespread adoption of contact tracing apps overnight but will protect those who choose to use this life-saving technology, whether in the current context of COVID-19 or in the future. The law should not

348 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

349 *Id.* at 2224.

350 *Id.* at 2268 (Gorsuch, J., dissenting).

351 The third-party doctrine is underscored by the notion that an individual has control over their information and can maintain or relinquish that control. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

352 *Carpenter*, 138 S. Ct. at 2220.

353 Lomas, *supra* note 52.

be so fickle and should not disadvantage those who try to promote the common good—both in general and when public health is at stake. Fourth Amendment protections should extend to location data collected by this technology.

DANIELLE J. FONG*

* J.D. Candidate, Emory University School of Law, Class of 2022; City University of New York Hunter College, M.Ed. 2016; Northwestern University, B.A. 2014. Thank you to my faculty advisor, Professor Morgan Cloud, for his guidance and encouragement, and Danielle Kerker Goldstein, Samantha Leff, and the editorial staff of *Emory Law Journal* Volume 71 for their hard work and contributions. A special thank you to Claire Scavone, for her invaluable camaraderie and support during the Comment writing process and law school generally. And of course, thank you to my family, particularly my parents and grandparents—your work ethic inspires and motivates me in all that I do.