TRACING THE INVISIBLE: INFORMATION FIDUCIARIES AND THE PANDEMIC

ANNE L. WASHINGTON & LAUREN RHUE*

ABSTRACT

Predictive data technology designed to contain the COVID-19 pandemic was not as successful as promised. Data-centric solutions to providing testing and tracing did little to limit the virus's spread in part because they served only the most visible parts of society. This Article argues for more robust solutions to protect individuals' privacy—whether those individuals are currently visible or invisible to pandemic technology—if pandemic technology is to provide the universal coverage necessary for a public health emergency, such as the COVID-19 pandemic. First, we contend that current pandemic data technology operates under rigid technical and social assumptions that thwart participation from all population groups. Second, we demonstrate that the organizations associated with pandemic data technology have financial incentives that could be in opposition to protecting anyone susceptible to the virus. Third, we consider how the need for someone to protect data to allow for medically necessary access to data could be an onramp for a pilot implementation of legal theory on information fiduciaries. Finally, we offer two tangible policy suggestions: conflict-of-interest notices released as open data and a public health fiduciary that has legal responsibility to protect data relevant to epidemiological outbreaks. A public health fiduciary working in the public interest would be more likely to gather sufficiently accurate data than would a fiduciary working within the organizations collecting data themselves. Technology has a vital role to play in managing the pandemic, but in the hands of some organizations, it may encourage

* Anne L. Washington, PhD, is an Assistant Professor of Data Policy at *New York University*. Lauren Rhue, PhD, is an Assistant Professor of Information Systems at the *University of Maryland*'s *Robert H. Smith School of Business*. This work draws on a presentation we made at the Future of Privacy Forum's International Tech & Data Conference in October 2020. We would like to thank Charles T. Stokes, 2019 graduate of *Stevenson University* in Baltimore, Maryland, for research assistance.

behavior that counters public health goals. Trusted data technology solutions in conjunction with predictive epidemiology models could contribute to reducing the spread of the virus more holistically and with fewer privacy-related consequences.

TABLE OF CONTENTS

INTRODUCTION

The global pandemic that spread an infectious respiratory disease beginning in 2019[1] was unlike earlier pandemics.[2] Other public health

1. *About COVID-19*, CTRS. FOR DISEASE CONTROL & PREVENTION (Sept. 1, 2020), https://www.cdc.gov/coronavirus/2019-ncov/cdcresponse/about-COVID-19.html [https://perma.cc/885L-ZK9T]. Throughout this Article, we refer to this event as "the pandemic," "the virus," or "COVID-19" interchangeably.

2. *See generally* Michael S. Rosenwald, *History's Deadliest Pandemics, from Ancient Rome to Modern America*, WASH. POST (Apr. 7, 2020), https://www.washingtonpost.com/graphics/2020/local/retropolis/coronavirus-deadliest-pandemics/ (providing a comparative history of respiratory diseases that occurred prior to the outbreak of the novel coronavirus, including the 1918 Flu, Asian Flu, and Swine Flu); Lauren M. Sauer, *What Is Coronavirus?*, JOHNS HOPKINS MED. (Mar. 31, 2021), https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus [https://perma.cc/6JXE-P8AH].

emergencies occurred within a concentrated geographic region[3] or before the digital era.[4] Most importantly, past emergencies rarely impacted Silicon Valley organizations building digital platforms and data technology. Major technology companies turned their attention to data innovations that could help to ameliorate the pandemic.[5] The personal experiences of people designing the newest mobile phone technology motivated innovative data solutions; however, this may have obscured the visibility of other populations.[6]

Interpreting data has been essential to understanding the progression of the deadly pandemic's spread. Daily analysis of the number of cases, hospital capacity, and deaths were part of regular media reports.[7] Interest in COVID-19 data was not a matter of idle curiosity; rather, the data directly impacted behavior, and fear of contracting the virus controlled the economy.[8] Everyone eagerly consumed data to grapple

---

3. *See What Is Ebola Virus Disease?*, CTRS. FOR DISEASE CONTROL & PREVENTION (Dec. 1, 2020), https://www.cdc.gov/vhf/ebola/about.html [https://perma.cc/H9FC-4V4E] (explaining that Ebola outbreaks occur primarily in Africa); *CDC SARS Response Timeline*, CTRS. FOR DISEASE CONTROL & PREVENTION (Apr. 26, 2013), https://www.cdc.gov/about/history/sars/timeline.htm [https://perma.cc/4ECL-6BDG] (following the SARS outbreak in the early 2000s through two-dozen countries after it was first discovered in Asia).

4. *See* Rosenwald, *supra* note 2 (acknowledging that the 1918 Flu killed roughly fifty million people); *HIV and AIDS—United States, 1981–2000*, CTRS. FOR DISEASE CONTROL & PREVENTION (June 1, 2001), https://www.cdc.gov/mmwr/preview/mmwrhtml/mm5021a2.htm (noting the rapid peak of HIV and AIDS through the 1980s and 1990s).

5. *See, e.g.*, 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 [https://perma.cc/WC2R-JM7R] (commenting on the rise in availability and use of contact tracing apps throughout various states).

6. *Design Bias Is Harmful, and in Some Cases May Be Lethal*, ECONOMIST (Apr. 10, 2021), https://www.economist.com/leaders/2021/04/10/design-bias-is-harmful-and-in-some-cases-may-be-lethal.

7. *See COVID-19 United States Cases by County*, JOHNS HOPKINS UNIV. & MED. CORONAVIRUS RES. CTR. (Feb. 16, 2021), https://coronavirus.jhu.edu/us-map [hereinafter JOHNS HOPKINS, *COVID-19 Tracker*]; *see, e.g.*, Antonia Noori Farzan et al., *U.S. Hits All-Time High in New Coronavirus Cases, Exceeding 80,000 in a Day for the First Time*, WASH. POST (Oct. 24, 2020, 6:57 AM), https://www.washingtonpost.com/nation/2020/10/23/coronavirus-covid-live-updates-us (reporting the United States' highest positive COVID-19 cases recorded in one day and that states saw new highs in hospitalizations).

8. Akrur Barua & David Levin, *What's Weighing on Consumer Spending: Fear of COVID-19 and Its Economic Impact*, DELOITTE (Aug. 28, 2020), https://www2.deloitte.com/us/en/insights/economy/spotlight/economics-insights-analysis-08-2020.html [https://perma.cc/F54M-RTFW].

with the risk of infection. Conflicting advice and contradictory regulatory guidance across regional and local authorities, coupled with a decentralized federal response, further contributed to the need for data and research across the United States.[9] As fear spread and the economy slowed, businesses,[10] schools,[11] municipalities,[12] and other organizations were left on their own to combat the pandemic's effects. Many were looking for an easy solution and a savior.

At first glance, the technology industry was an ideal hero for managing public health problems. The industry can deliver solutions at scale and reach millions of people simultaneously. Technological solutions began to surface: websites to triage patients for testing,[13] mobile device applications ("apps") for contact tracing,[14] and smart

---

9. *See* Charlotte Alter & Lissandra Villa, *'You Must Act Now.' How States and Cities Have Responded to the Coronavirus Pandemic*, TIME (Mar. 14, 2020, 7:55 PM), https://time.com/5803334/coronavirus-pandemic-local-governments [https://perma.cc/5X3S-GLXC] (discussing the "patchwork" of responses that states adopted to "combat COVID-19"); Eric Lipton et al., *The C.D.C. Waited 'Its Entire Existence for This Moment.' What Went Wrong?*, N.Y. TIMES (Aug. 14, 2020), https://www.nytimes.com/2020/06/03/us/cdc-coronavirus.html?searchResultPosition (explaining the breakdown of the "Data Pipeline" between the CDC and state officials as states "demand[ed] information to make key decisions," and discussing how the federal government's failure to provide adequate guidance forced medical practitioners to "look elsewhere for detailed recommendations about how to safely care for infected patients").

10. Jeanna Smialek, *Major Employers Left out of Government's Coronavirus Relief Plan*, N.Y. TIMES (June 18, 2020), https://www.nytimes.com/2020/06/02/business/economy/major-employers-coronavirus-relief.html (stating potential effects of the government's direct relief options' exclusion of many businesses).

11. *See* Hannah Natanson & Valerie Strauss, *America Is About to Start Online Learning, Round 2. For Millions of Students, It Won't Be Any Better*, WASH. POST (Aug. 5, 2020, 5:58 PM), https://www.washingtonpost.com/local/education/america-is-about-to-start-online-learning-round-2-for-millions-of-students-it-wont-be-any-better/2020/08/05/20aaabea-d1ae-11ea-8c55-61e7fa5e82ab_story.html (identifying pressures that schools faced in creating online curriculums and deciding if in-person learning was safe with little to no guidance from officials).

12. *See* Alter & Villa, *supra* note 9 (illustrating "disjointed local efforts" stemming from a lack of federal guidance).

13. *Baseline COVID-19 Testing Program*, PROJECT BASELINE, https://www.projectbaseline.com/studies/covid-19 [https://perma.cc/SCP3-9XZ3]; *see* Daisuke Wakabayashi & Natasha Singer, *Coronavirus Testing Website Goes Live and Quickly Hits Capacity*, N.Y. TIMES (Mar. 16, 2020), https://www.nytimes.com/2020/03/16/technology/coronavirus-testing-website-google.html (discussing the privacy concerns that arose when Google's sister company, Verily, launched the testing website, Project Baseline).

14. *See, e.g.*, *Apple and Google Partner on COVID-19 Contact Tracing Technology*, APPLE (Apr. 10, 2020), https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology [https://perma.cc/97BG-7MCS] (announcing

medical devices for monitoring symptoms.[15] Readily available mobile phone technology[16] is similar around the globe, and apps can be easily delivered anywhere.[17] The reuse of existing devices solves a critical logistics problem with relatively little effort. The technology industry, which dominates worldwide markets,[18] already has the physical infrastructure to deploy solutions through software and firmware updates to billions of devices.[19] Because of the ubiquity of mobile technology, data from consumer devices could easily generate population-level public health statistics.

The benefits of offering solutions at scale come with a cost: a diminished ability to respond to individual experiences and preferences. As much as data collection may contribute to solving public health crises, it may also provoke personal privacy concerns.[20] This places the onus on individuals to determine whether they feel comfortable downloading an app or sharing information through digital contact tracing.[21] Regulatory systems around sensitive data,

---

efforts to "enable interoperability between Android and iOS devices using apps from public health authorities" and enable "broader Bluetooth-based contact tracing . . . [allowing] interaction with a broader ecosystem of apps").

15. *See, e.g.*, Donald G. McNeil, Jr., *Can Smart Thermometers Track the Spread of the Coronavirus?*, N.Y. TIMES (Mar. 18, 2020), https://www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html (detailing the fever-tracking device from Kinsa Health that helps predict the spread of flus).

16. *See* Lauren Rhue & Arun Sundararajan, *Digital Access, Political Networks and the Diffusion of Democracy*, 36 SOC. NETWORKS 40, 46–47 (2014) (showing how every continent has seen a drastic increase in mobile phone availability since the turn of the century).

17. *See* Sato, *supra* note 5 (examining the widespread implementation of COVID-19 contact tracing apps across the United States).

18. *See generally* Luca Ventura, *World's Largest Companies 2020*, GLOB. FIN. (Nov. 30, 2020), https://www.gfmag.com/global-data/economic-data/largest-companies [https://perma.cc/PJ3N-3WEK] (providing an overview of the world's largest companies by market capitalization in 2020, of which seven of the top ten are technology companies or consumer services companies heavily involved in technology).

19. *See* Joe Harpaz, *Apple iOS 13.5 Is Ready for COVID-19 Contact Tracing—Are You?*, FORBES (May 22, 2020, 7:10 AM), https://www.forbes.com/sites/joeharpaz/2020/05/21/apple-ios-135-is-ready-for-covid-19-contact-tracing/?sh=6b75aedb1b4b [https://perma.cc/L823-YTXL] (discussing updates Apple made to its software to provide COVID-19 exposure notifications).

20. *See* Billy Perrigo, *U.S. States Are Rolling out COVID-19 Contact Tracing Apps. Months of Evidence from Europe Shows They're No Silver Bullet*, TIME (Oct. 9, 2020, 2:22 PM), https://time.com/5898559/covid-19-contact-tracing-apps-privacy [https://perma.cc/7JRH-689L] (contending that contact tracing apps "involve[] a tradeoff between privacy and public health").

21. *Cf.* Craig Timberg, Drew Harwell, & Alauna Safarpour, *Most Americans Are Not Willing or Able to Use an App Tracking Coronavirus Infections. That's a Problem for Big Tech's*

outside of the tech industry, generally provide guidelines on maintaining privacy. For example, medical organizations that share health data must protect patient privacy under the Health Insurance Portability and Accountability Act of 1996[22] (HIPAA). Given the fragmented regulatory structure across industries, however, HIPAA's privacy rules that govern medical organizations do not apply to many tech companies.[23]

Considering the great extent to which large companies already reuse data they collect, privacy concerns may hamper widespread use of the tools that these companies provide. It is reasonable to presume that enough individuals would hesitate to opt in, limiting the ultimate usefulness of these tools. If organizations building pandemic data technology were required to act as fiduciaries[24] for this information, then the organizations, not the individuals, would bear the consequences for data misuse.[25]

This Article reviews the viability of using mobile technology and data in the COVID-19 pandemic. The technology solutions we discuss include mobile phone call records, smartphone applications, Bluetooth proximity data, and third-party health applications such as smart thermometers. Two primary issues with these technology solutions exist. First, these solutions are based on inaccurate assumptions and thus do not fulfill the technology's intended purpose. Specifically, the solutions rely upon broad participation, but pandemic technology only operates under rigid technical and social conditions that thwart

---

Plan to Slow the Pandemic, WASH. POST (Apr. 29, 2020, 1:03 PM), https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic ("Nearly 3 in 5 Americans say they are either unable or unwilling to use the infection-alert system under development by Google and Apple, suggesting that it will be difficult to persuade enough people to use the app to make it effective against the coronavirus pandemic . . . .").

22. Pub. L. No. 104-191, 110 Stat. 1936 (1996); *see Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL & PREVENTION (Sept. 14, 2018), https://www.cdc.gov/phlp/publications/topic/hipaa.html [https://perma.cc/UP2R-32Z3] (outlining HIPAA protections and their application to healthcare providers, health plans, healthcare clearinghouses, and business associates receiving health information in the course of business).

23. Stacy A. Tovino, *Assumed Compliance*, 72 ALA. L. REV. 279, 282 (2020).

24. *See* Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 144–45 (2020) (defining a fiduciary relationship as one where the fiduciary "has discretionary power over another party's (the entrustor) important practical interests").

25. *See id.* at 145 ("Fiduciary duties would mean expanded liability for data protection failures for companies.").

participation from all population groups. Second, the entities behind these technology solutions, including digital technology companies and private hospitals, have financial incentives that are inherent conflicts of interest that may further compromise public health goals.

More robust solutions are necessary if pandemic technology is to provide the universal coverage that a public health emergency demands. For instance, one privacy-related challenge facing individuals is the perceived infallibility of data organizations' proprietary algorithms, which makes it difficult for individuals to challenge the legality of the use of their data.[26] Further complicating this is the "third-party doctrine," which dictates that information shared with a third party is discoverable by law enforcement.[27] If organizations currently collecting data refuse to exercise a duty of care over the information they collect, then the data steward should be another entity that is able to perform information fiduciary responsibilities.[28] The current technology solutions provide individuals little insight into what happens to their health data and even less recourse if something goes wrong. We consider whether these realities support an alternative policy response.

This Article evaluates current legal scholarship on the concept of an information fiduciary and argues that it may be a better model for deploying pandemic data technology. We conclude our analysis with tangible policy suggestions, such as conflict-of-interest notices and the creation of new public health information fiduciary organizations that maintain pandemic data, have long-term fiduciary responsibilities, and provide just-in-time access to data for medical or public health reasons.

Data technology could play a vital role in resolving the pandemic if the technology were in the hands of an information fiduciary responsible for gathering accurate information across all populations without penalty. Technology should be part of the public health solution; however, pandemic data technology should not be driven by

---

26. *See* Anne L. Washington, *How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate*, 17 COLO. TECH. L.J. 131, 133–34, 145 (2018) (suggesting potential difficulties in challenging an algorithm's validity given the difficulty in accessing its underlying information, which vendors claim as "trade secrets that cannot be shared").

27. Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 614–15 (2015).

28. *See* Christine L. Borgman, *Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier*, 33 BERKELEY TECH. L.J. 365, 370–71, 375 (2018) (discussing data stewardship and the protection of certain types of university data from third parties seeking to exploit that information).

the desire to reach a niche group of consumers or extend digital business models. Investing in an entity with fiduciary responsibility for pandemic information would support a faster reduction in the spread of the virus. An information fiduciary would limit the reuse of data for purposes beyond public health ones and would be loyal both to individuals and to whole communities, thereby instilling greater confidence in and adoption of data technology solutions to the pandemic.

I. PANDEMIC DATA TECHNOLOGY

During a public health crisis, trust is essential, and those tasked with ameliorating the crisis must earn the trust of millions with life-or-death consequences. However, large technology companies, colloquially known as Big Tech, have a track record of squandering trust for profit.[29] This pattern of behavior may limit the effectiveness of data technology in lessening the pandemic's spread and diminishing its negative consequences. Given the realities of public health emergencies, the pandemic data technology solutions emerging from Big Tech may not meet their most altruistic goals.

A. The Public Health Crisis

Containing the spread of an infectious disease is always the central goal of fighting a pandemic, and the coronavirus pandemic has been no different. Because a respiratory virus easily transmits between people, understanding who is in contact with whom is important for anticipating future spread and providing early warning to those at risk.[30] The goal of many non-pharmaceutical interventions ("NPIs"), such as social distancing, is to stop disease spread by reducing contact

29. *E.g.*, *An Examination of Facebook and Its Impact on the Financial Services and Housing Sectors: Hearing Before the H. Comm. on Fin. Servs.*, 116th Cong. 1–2 (2019) (statement of Rep. Maxine Waters, Chairwoman, H. Comm. on Fin. Servs.) ("[Facebook is] willing to step on or over anyone, including [its] competitors, women, people of color, [its] own users, and even our Democracy, to get what [it] want[s].").

30. *Case Investigation and Contact Tracing: Part of a Multipronged Approach to Fight the COVID-19 Pandemic*, CTRS. FOR DISEASE CONTROL & PREVENTION (Dec. 3, 2020), https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html [https://perma.cc/78B4-4YER]; *see Transmission of SARS-CoV-2: Implications for Infection Prevention Precautions*, WORLD HEALTH ORG. (July 9, 2020), https://www.who.int/news-room/commentaries/detail/transmission-of-sars-cov-2-implications-for-infection-prevention-precautions [https://perma.cc/U53R-647K].

between infected and non-infected people.[31] By acquiring population-level views of positive cases and potential spread, pandemic data technology seeks to illuminate the effectiveness of NPIs.

Technology enables organizations and societies to handle problems at scale, and the scale of the pandemic within the United States reached across all states, communities, and populations.[32] As of January 1, 2021, the United States had suffered 350,000 deaths.[33] A population of approximately 330 million people[34] had 29 million diagnosed cases by March 2021.[35] As the coronavirus situation has worsened, the U.S. federal, state, and local governments adopted guidelines to prevent the virus's spread, such as mask-wearing mandates. Businesses, if they were allowed to open, operated at reduced capacity and enforced social distancing measures requiring a six-foot distance between people within the physical space.[36]

Advances in technology drove hopes for eradicating the virus quickly. Biomedical advances made it possible to produce vaccines within twelve months instead of multiple years.[37] Supply chain and production expertise facilitated distribution of vaccines as soon as regulatory authorities approved them.[38] School robotics clubs turned

---

31. *Community NPIs: Flu Prevention in Community Settings*, CTRS. FOR DISEASE CONTROL & PREVENTION (Aug. 26, 2019), https://www.cdc.gov/nonpharmaceutical-interventions/community/index.html [https://perma.cc/B5MP-69VQ].

32. *See* JOHNS HOPKINS, *COVID-19 Tracker*, *supra* note 7.

33. Meryl Kornfield & Shayna Jacobs, *As Coronavirus Death Toll Surpasses 350,000, Trump Calls U.S. Count 'Far Exaggerated'*, WASH. POST (Jan. 3, 2021, 8:22 PM), https://www.washingtonpost.com/health/trump-calls-us-coronavirus-death-toll-fake-news-as-count-surpasses-350000/2021/01/03/6bdc0b08-4e14-11eb-bda4-615aaefd0555_story.html.

34. *U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock (last visited May 14, 2021).

35. *Coronavirus in the U.S.: Latest Map and Case Count*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html (last visited May 14, 2021).

36. *See, e.g.*, *Considerations for Restaurant and Bar Operators*, CTRS. FOR DISEASE CONTROL & PREVENTION (Dec. 16, 2021), https://www.cdc.gov/coronavirus/2019-ncov/community/organizations/business-employers/bars-restaurants.html [https://perma.cc/JWY8-VJDV].

37. *Pfizer-BioNTech COVID-19 Vaccine*, U.S. FOOD & DRUG ADMIN. (Feb. 3, 2021), https://www.fda.gov/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/pfizer-biontech-covid-19-vaccine [https://perma.cc/Q9AB-VMFK]; *About COVID-19*, *supra* note 1.

38. *See* Carolyn Y. Johnson, *A Vial, a Vaccine and Hopes for Slowing a Pandemic—How a Shot Comes to Be*, WASH. POST (Nov. 17, 2020, 6:00 PM), https://www.washingtonpost

their 3D printers into protective equipment for hospitals.[39] Publishers that normally keep academic articles behind paywalls released works for free to the public to increase the speed of scientific discovery.[40] A collaborative and open environment made it possible to more efficiently solve new logistics and medical problems with technology.

Big Tech has notable advantages for managing public health issues. Its products are ubiquitous. Its solutions require little overhead for implementation. An ethos of universal design facilitates quick distribution across geographies and languages. Big Tech envisioned that data technology could easily calculate population-level statistics across local and regional areas, track adherence to medical guidelines, observe the existence of symptoms and spread of the virus through communities, and predict the places where medical equipment is needed.[41] Entrepreneurs located in Silicon Valley—in a state among the most negatively impacted by the pandemic in a country that also struggled at the national level[42]—were ready to lead the charge.

Although Big Tech may assume that it has the solution to all problems, the industry, and the governments that demand its solutions,

---

.com/health/2020/11/17/coronavirus-vaccine-manufacturing (describing the vaccine production and distributions as "a meticulously choreographed high-wire act that must not falter at any juncture").

39. Courtney Borchert, *Local Robotics Team Makes, Donates PPE for COVID-19 Responders*, CTR. TIMES PLUS (Sept. 15, 2020), https://www.utsouthwestern.edu/ctplus/stories/2020/technic-bots.html [https://perma.cc/RF22-2DN5]; Hannah Hagemann, *One Way to Help Strapped Hospitals? Print PPE Using 3D Printers*, NAT'L PUB. RADIO (Mar. 28, 2020, 9:00 AM), https://www.npr.org/2020/03/28/822911643/one-way-to-help-strapped-hospitals-print-ppe-using-3d-printers.

40. Virgie Hoban, *Science, Uninterrupted: Will COVID-19 Mark the End of Scientific Publishing as We Know It?*, BERKELEY LIBR. NEWS (July 30, 2020), https://news.lib.berkeley.edu/covid-oa [https://perma.cc/J559-S9JR].

41. *See* Charlie Warzel, *Can This Thermometer Help America Reopen Safely?*, N.Y. TIMES (June 29, 2020), https://www.nytimes.com/2020/06/29/opinion/coronavirus-kinsa-thermometer.html (detailing the Kinsa thermometer that helped identify new spikes in COVID-19 epicenters); Kyra H. Grantz et al., *The Use of Mobile Phone Data to Inform Analysis of COVID-19 Pandemic Epidemiology*, NATURE COMMC'NS 1, 1–4 (2020) (discussing the use of geolocation data in mobile phones to track the spread of COVID-19).

42. *See* Soumya Karlamangla et al., *L.A. County Records 140 COVID-19 Deaths in One Day, a New Record*, L.A. TIMES (Dec. 24, 2020, 8:41 PM), https://www.latimes.com/california/story/2020-12-24/coronavirus-surge-hammering-los-angeles-hospitals (noting the record high number of COVID-19 cases in California); John Elflein, *Number and Change of Coronavirus (COVID-19) Cases and Deaths Among the Most Impacted Countries Worldwide as of April 20, 2021*, STATISTA (Apr. 20, 2021), https://www.statista.com/statistics/1105264/coronavirus-covid-19-cases-most-affected-countries-worldwide [https://perma.cc/8Q8H-LDGZ].

have a checkered record of gaining the public's trust.[43] Instead of relying on medical, public health, logistics, or economics expertise, Silicon Valley relied on its expertise in delivering data technology.[44] The industry assumes that any data-driven response delivered at scale is the solution even in the absence of subject-matter expertise or theory.[45] The assumption that technology is the solution to the public health crisis is no different; however, the public health crisis has aspects that the current landscape of data-driven technology cannot sufficiently address.

---

43. Indeed, the industry has made a considerable impact on various areas of the private and public sectors particularly with AI technology. *See, e.g.*, DAVID FREEMAN ENGSTROM ET AL., GOVERNMENT BY ALGORITHM: ARTIFICIAL INTELLIGENCE IN FEDERAL ADMINISTRATIVE AGENCIES 6 (2020) (federal agencies); *AFP Algorithms*, AM. FAM. PHYSICIAN, https://www.aafp.org/afp/algorithms/viewAll.htm [https://perma.cc/CL8W-Q5QV] (medicine); Victor Antonio, *How AI Is Changing Sales*, HARV. BUS. REV. (July 30, 2018), https://hbr.org/2018/07/how-ai-is-changing-sales (sales and marketing); Rebecca Heilweil, *Artificial Intelligence Will Help Determine if You Get Your Next Job*, VOX (Dec. 12, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen (hiring and recruitment). However, these advancements have not come without presenting issues of their own. *See, e.g.*, Nicol Turner Lee et al., *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, BROOKINGS INST. (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms. Biases stretch across sectors, from law enforcement to healthcare, and directly harm vulnerable populations. *E.g.*, *AI Now 2018 Symposium*, AI NOW INST. (Oct. 16, 2018), https://ainowinstitute.org/symposia/2018-symposium.html [https://perma.cc/7SL3-HGJT] (exposing bias, error, and misuse of AI technologies in the use of algorithms by law enforcement and healthcare). Researchers underscore the need for oversight and urge the AI industry to implement internal auditing structures to improve transparency and accountability. MEREDITH WHITTAKER ET AL., AI NOW REPORT 2018 4, 11 (2018) (offering several improvements such as encouraging developers to "agree to waive any trade secrecy or other legal claim").

44. *See* Peter V. Coveney et al., *Big Data Need Big Theory Too*, 374 PHIL. TRANSACTIONAL ROYAL SOC'Y A 1, 1 (2016) (highlighting "the weaknesses of pure big data approaches with particular focus on biology and medicine, which fail to provide conceptual accounts for the processes to which they are applied."); Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED (June 23, 2008, 12:00 PM), https://www.wired.com/2008/06/pb-theory (explaining Google's applied mathematics advertising approach that ignored the "culture and conventions" of the industry); Fulvio Mazzocchi, *Could Big Data Be the End of Theory in Science?*, 16 EMBO REPS. 1250, 1250–51 (2015) (questioning whether algorithms as "[p]ermanent learning" tools that produce "imperfect but useful knowledge" will replace traditional hypothesis-driven research).

45. *See* Coveney et al., *supra* note 44, at 1.

B. Individual Mobility Data

Mobile phones have the ability to track one person through multiple related sources.[46] Governments and Big Tech assume that mobility data is essential to understanding proximity to infection during a pandemic. This Section evaluates the feasibility of thoroughly addressing public health goals using individual location data—specifically call logs, device location tracking, and health data apps. We argue that these data sources collect relevant information but are not sophisticated enough to work without manual contact tracing and mass testing.[47]

Call logs and phone records have been important data resources in previous public health emergencies. Mobile phone providers have shared logs with public health authorities to help track the spread of disease or adherence to public health guidelines.[48] Analyses of mobile phone data have helped identify the source of malaria outbreaks in Namibia,[49] cholera outbreaks in Senegal,[50] and dengue outbreaks in Pakistan.[51] Public health authorities forged partnerships with mobile

---

46. *See* David Nield, *How Location Tracking Actually Works on Your Smartphone*, GIZMODO (Sept. 3, 2018, 10:30 AM), https://gizmodo.com/how-location-tracking-actually-works-on-your-smartphone-1828356441 (describing interrelated methods of location tracking employed by data technology companies, including direct device tracking, application tracking, and tracking through Apple and Google).

47. *See* discussion *infra* Section I.D (confronting sampling biases and other collection factors that produce imprecise data pools); *see also* Patrick Howell O'Neill, *Contact Tracing Apps Are Only One Part of the Pandemic Fight*, MIT TECH. REV. (Aug. 19, 2020), https://www.technologyreview.com/2020/08/19/1007452/contact-tracing-apps-study [https://perma.cc/48B8-AXX9] ("[D]igital tools can only complement—not replace—the very human work required to beat [COVID]-19.").

48. *See* Grantz et al., *supra* note 41, at 2 (summarizing lessons learned from tracking malaria, cholera, measles, dengue, and Ebola spread using mobile phone data); *see also* Caroline O. Buckee et al., *Aggregated Mobility Data Could Help Fight COVID-19*, SCI. MAG., Apr. 10, 2020, at 145, 145 (explaining how population mobility patterns created from aggregate mobile phone data can be leveraged to determine the efficacy of social distancing interventions).

49. *See* Nick W. Ruktanonchai et al., *Identifying Malaria Transmission Foci for Elimination Using Human Mobility Data*, PLOS COMPUTATIONAL BIOLOGY, Apr. 4, 2016, at 1, 4 (tracing the path of malaria transmission with phone call records to identify "patterns of prevalence").

50. *See* Flavio Finger et al., *Mobile Phone Data Highlights the Role of Mass Gatherings in the Spreading of Cholera Outbreaks*, 113 PROC. NAT'L ACAD. SCIS. 6421, 6421 (2016) (using mobile phone data to "extract human mobility fluxes" and incorporate the extracted information into dynamic epidemiological models).

51. Amy Wesolowski et al., *Impact of Human Mobility on the Emergence of Dengue Epidemics in Pakistan*, 112 PROC. NAT'L ACAD. SCIS. 11887, 11887 (2015) (analyzing phone-based mobility estimates to predict the geographic spread and timing of dengue epidemics).

phone providers to access call log data.[52] Mobile phone providers give researchers aggregate information to establish which users are in communication with other users.[53] However, without testing for the virus, communications between people do not alone provide useful public health information.

Device location data tracks where devices go and how they travel. Assuming the person who owns the device is moving with it, device data location indicates individual movement. Mobile phones use a combination of Global Positioning System (GPS), Bluetooth, and Wi-Fi to determine the "approximate" geospatial location of the device.[54] A mobile device records its location each time it pings a nearby cell phone tower for service or Wi-Fi network.[55] The location of the device is recorded into the phone's operating system.[56] The operating system and third-party apps have access to the device's location data, which indicates where the device has been and the places the owner visited.[57] Device location data can provide a log of individual activity, but testing for the virus is necessary to understand the implications of the device location data. Otherwise, general mobility data may only be valuable

52. *See supra* note 48 and accompanying text.

53. *See* Grantz et al., *supra* note 41, at 2.

54. *About Privacy and Location Services in iOS and iPadOS*, APPLE (Feb. 2, 2021), https://support.apple.com/en-us/HT203033 [https://perma.cc/NSJ4-MG2C].

55. *See* Nield, *supra* note 46 (advising users on how to stop smartphones from "pinging GPS satellites, cell towers, [or] . . . nearby public wifi networks"). Cell phone pings collect data sets that store the precise daily movements of millions of people. *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. While technically sanitized of identifying information, aggregate location pings reveal identities with little effort. *Id.* (quoting Paul Ohm, law professor and researcher at *Georgetown University Law Center* as stating that "[r]eally precise, longitudinal geolocation information is absolutely impossible to anonymize").

56. *See Location Services & Privacy*, APPLE (Sept. 18, 2020), https://support.apple.com/en-us/HT207056 [https://perma.cc/9FH6-6LV8] (notifying users that the operating system "allows Apple and third-party apps and websites to gather and use information based on the current location of your iPhone or Apple Watch to provide a variety of location-based services"). Often, a user's full access of a third-party application is predicated on the user enabling the application to access the user's location. Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, BUS. L. TODAY (Mar. 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy [https://perma.cc/NS6A-3VPM]. In turn, third parties make conclusions or predictions based on the users' location data, forming a profile for each user that can be sold to interested parties. *Id.*

57. *See* Boshell, *supra* note 56.

for understanding adherence to public health guidelines such as shelter-in-place orders.

Another source of pandemic-related mobility data are health-specific smart technologies. Health-related mobile phone apps monitor physical fitness by collecting vital signs such as heart rate, pulse, and oxygen saturation.[58] Smart health devices often also have their own third-party phone apps that interact with existing mobile health data.[59] Apps associated with smart health devices aggregate and analyze trends as well as capture location information.[60] Proponents argued that smart health devices could provide real-time surveillance of COVID-19 outbreaks.[61] Smart thermometer apps claimed to identify unexpected patterns of fever,[62] although regulatory barriers prevented users from sharing real-time data with medical professionals.[63] However, mobile health data sources are particularly susceptible to privacy vulnerabilities.[64]

---

58. *See, e.g.*, Brian Dolan, *Apple Shows off AirStrip's Vital Sign Monitoring Apple Watch App*, MOBIHEALTH NEWS (Sept. 10, 2015, 10:31 AM), https://www.mobihealthnews.com/46687/apple-shows-off-airstrips-vital-sign-monitoring-apple-watch-app (explaining how physicians monitor a patient's vital signs in real time through a smart watch app); Andrew M. Luks & Eric R. Swenson, *Pulse Oximetry for Monitoring Patients with COVID-19 at Home: Potential Pitfalls and Practical Guidance*, 17 ANNALS AM. THORACIC SOC'Y 1040, 1040 (2020).

59. *See, e.g.*, Alicia Phaneuf, *Latest Trends in Medical Monitoring Devices and Wearable Health Technology*, BUS. INSIDER (Jan. 11, 2021, 12:48 PM), https://www.businessinsider.com/wearable-technology-healthcare-medical-devices [https://perma.cc/RA3D-4NDF] (explaining how data can be transferred from a wearable blood pressure monitor to a mobile app).

60. *See, e.g.*, *Mobile Health: Tools, Benefits, and Applications*, UNIV. ILL. CHI. (Oct. 21, 2020), https://healthinformatics.uic.edu/blog/mobile-health [https://perma.cc/AZB8-GKLG] (describing how devices can use GPS and other data to provide users a more comprehensive view of their fitness progress).

61. *See* Warzel, *supra* note 41 (using historical fever data from smart thermometer apps to monitor potential "impending outbreak cluster[s]").

62. Mollie Bloudoff-Indelicato, *This Company Claims Its Smart Thermometer Could Help Detect Coronavirus Hot Spots Faster than the CDC*, CNBC: TECH DRIVERS (Apr. 2, 2020, 10:25 AM), https://www.cnbc.com/2020/04/02/this-smart-thermometer-could-help-detect-covid-19-hot-spots.html [https://perma.cc/BZ2L-MLBU].

63. *See* Anna Wilde Mathews & Melanie Evans, *Sharing Your Digital Health Data: New Rules Ease Access*, WALL ST. J. (Mar. 9, 2020, 7:16 PM), https://www.wsj.com/articles/sharingyourhealthdatanewdigitalrules-11583702453 (noting that regulatory barriers on digital health data frequently compel patients to bring physical copies of records to a new doctor's office).

64. *See, e.g.*, Rosie Spinks, *Using a Fitness App Taught Me the Scary Truth About Why Privacy Settings Are a Feminist Issue*, QUARTZ (Aug. 1, 2017), https://qz.com/1042852/using-a-fitness-app-taught-me-the-scary-truth-about-why-privacy-settings-are-a-feminist-issue [https://perma.cc/2532-937P] (describing the misleading location sharing policies of Strava, a fitness tracking application).

Call logs, device location, and health apps enable the collection and possible aggregation of information.[65] In order to identify which locations are important in the pandemic, the technology would need testing information, which could only be accomplished through mass testing. In the end, many of the digital innovations in health data tracking did not translate into actual treatment.[66]

C. Contact Tracing and Relational Mobility Data

Public health officials limit the spread of the virus by identifying who has been in contact with a positive test case and asking them to isolate.[67] Contacting anyone who may have been exposed to the virus is the traditional method of containing an outbreak.[68] Digital contact tracing attempts to emulate this manual contact tracing process through digital and automated means.[69] Relational mobility data can identify a small group of people who were in the same physical location, and it can indicate the breadth of pathogen spread between individuals.[70] Public health organizations need relational mobility data of small groups in order to make decisions to protect the health of everyone in the area.

---

65. *See Mobile Location Data and Covid-19: Q&A*, HUM. RTS. WATCH (May 13, 2020, 12:01 AM), https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa [https://perma.cc/P9SC-YZWF] (explaining how device location systems and smartphone apps collect data).

66. *See* Gina Neff, *Why Big Data Won't Cure Us*, 1 BIG DATA 117, 118–19 (2013) (discussing why access to health data has not translated to better care).

67. *When You Can Be Around Others After You Had or Likely Had COVID-19*, CTRS. FOR DISEASE CONTROL & PREVENTION (Mar. 12, 2021), https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/end-home-isolation.html [https://perma.cc/JXY8-4PWF].

68. *See Case Investigation and Contact Tracing: Part of a Multipronged Approach to Fight the COVID-19 Pandemic*, CTRS. FOR DISEASE CONTROL & PREVENTION (Dec. 3, 2020), https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html [https://perma.cc/2VJ5-Y783] (noting that contact tracing has been a method used for decades to prevent the spread of viruses).

69. *See Mobile Location Data and Covid-19: Q&A*, *supra* note 65 (defining contact tracing as the "process of identifying individuals who may have come into contact with an infected person"); *see also* 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 [https://perma.cc/XD3T-FP4E] (discussing the mechanics of digital contact tracing).

70. *See* Amy Wesolowski et al., *Connecting Mobility to Infectious Diseases: The Promise and Limits of Mobile Phone Data*, 214 J. INFECTIOUS DISEASES S414, S415–16 (2016) (describing the process of using mobile data to "simulate patterns of spread through space and time by using individual movement traces combined with the pathogen's known biological aspects").

Digital contact tracing leverages mobile phone applications that share networked resources.[71] The contact tracing project released by two Big Tech companies, Google and Apple, used Bluetooth to identify all devices within the vicinity of each other.[72] Despite their initial plans to only provide the technology framework, Google and Apple decided to build the entire application and permit states to use the technology.[73] A central server operated by the Association of Public Health Laboratories in addition to a single application infrastructure can track people across state lines.[74]

Digital contact tracing apps deploy an "exposure notification" strategy.[75] Advocacy groups have collaborated with privacy and technology organizations to develop a set of principles to govern the collection and distribution of user information to alert the user to potential COVID-19 exposure.[76] An exposure is determined by a combination of time and distance between individuals, but the exact cutoffs depend on the country and the app.[77] For example, in Australia, the exposure threshold is 1.5 meters for 15 minutes whereas in Ireland the threshold is set at 2 meters for 15 minutes.[78] The use of Bluetooth to connect with all phones in a 1.5- or 2-meter radius assumes that Bluetooth is specific enough to properly trace exposure. Bluetooth relational mobility data intends to establish when people are breathing the same source of air, which is critical to understanding a respiratory virus.

---

71. *See* Greenberg, *supra* note 69 (explaining how major technology companies worked together to make digital contact tracing possible).

72. *Id.*; Gregory Barber, *Google and Apple Change Tactics on Contract Tracing Tech*, WIRED (Sept. 1, 2020, 2:42 PM), https://www.wired.com/story/google-apple-change-tactics-contact-tracing-tech [https://perma.cc/5R9X-RYFS] (describing plan to alert users to potential exposure using short-range, anonymous Bluetooth signals); *see also* Tony Homm et al., *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, WASH. POST (Mar. 17, 2020, 9:15 PM), https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus (weighing individual privacy rights with urgent public health needs).

73. *See* Barber, *supra* note 72 (offering a centralized technology model available through operating systems to generate exposure notifications).

74. *Id.*

75. *Data Rights for Exposure Notification*, EXPOSURE NOTIFICATION, http://exposurenotification.org [https://perma.cc/PD27-YX6X] (explaining how the exposure notification strategy is used).

76. *See id.* (dictating fourteen principles on individual data rights for developers and public health officials).

77. *See* Mitch Leslie, *COVID-19 Fight Enlists Digital Technology: Contact Tracing Apps*, 6 ENG'G 1064, 1064 (2020).

78. *Id.*

Epidemiological models need proximity data to inform critical allocation decisions and medical responses. For instance, epidemiological models of COVID-19 determined where to concentrate resources for respirators.[79] Predictive data technology for the pandemic has relied on four sources of data: call logs that assess population density,[80] device location tracking from major mobile phone companies to understand population movement,[81] third-party phone apps and health devices that share health and location data,[82] and contact tracing data to estimate proximity to infection.[83] Mobile location sources that track individual and group movements could provide actionable information for epidemiologists during a pandemic with the right assumptions.

D. Social and Technical Assumptions

Individual and relational mobility data expose several social and technical assumptions in addition to privacy concerns. Location data sources yield value insights, yet only for a limited population that own devices or show symptoms.[84] Furthermore, assumptions that location data services have sufficient fidelity and accuracy for virus detection may not reflect reality. Together, these assumptions render some populations and behaviors invisible to public health authorities.

Public health interventions rely on the health of everyone in a community. However, current solutions that rely on data and technology may render some populations invisible and thus have limited application. Specifically, mobile phone adoption can vary greatly.[85] Several factors may correlate with less mobile device adoption, including economic, social, demographic, geographic, or cultural aspects of

---

79. Nuria Oliver et al., *Mobile Phone Data for Informing Public Health Actions Across the COVID-19 Pandemic Life Cycle*, 6 SCI. ADVANCES, at 2 (2020).

80. *See supra* notes 48–53 and accompanying text.

81. *See supra* notes 54–57 and accompanying text.

82. *See supra* notes 58–63 and accompanying text.

83. *See supra* Section I.C.

84. *See Mobile Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile [https://perma.cc/WY42-7MU3] (finding that only eighty-one percent of individuals in the United States own smartphones); *infra* note 89 and accompanying text. Further, even individuals who do own phones do not always have their phones with them while interacting with others. For example, students at school might be required to leave their phones in their lockers, and people entering a courthouse might need to leave their phones in their cars or elsewhere.

85. *See* Pierre Deville et al., *Dynamic Population Mapping Using Mobile Phone Data*, 111 PROC. NAT'L ACAD. SCIS. 15888, 15891 (2014).

communities.[86] Because of systematic social and geographic differences between mobile and non-mobile phone users, mobile phone users reflect a non-representative sample of the population for public health observation.[87] Reliance on expensive digital and internet-connected health devices suffers from the same challenges as reliance on mobile phones.[88] The adoption rates are less likely for people with less disposable income due to more limited knowledge of health systems and mobile applications and lack of trust in the healthcare system..[89] Solutions built on mobile devices will fail to account for areas with lower-income populations or less reliable mobile reception.

The presence of an outbreak in the population of mobile device owners may not be an appropriate proxy variable for a general outbreak. Conversely, an outbreak outside of this biased sample may be invisible within these data sources. A sampling bias means that the results of a study cannot be reliably applied to a general population because there may be something specific about that population that led to the results.[90] Current mobile data solutions suffer from a sampling bias and would only be successful with widespread adoption.

Another reason these technologies have failed are assumptions about the spread of COVID-19. Originally, smart thermometers promised valuable information on the spread of the virus based on the

---

86. *See Mobile Fact Sheet*, *supra* note 84 (explaining, for example, that while ninety-one percent of college graduates own a smartphone, only sixty-six percent of people without high school degrees do).

87. *See, e.g.*, Amy Wesolowski et al., *Heterogeneous Mobile Phone Ownership and Usage Patterns in Kenya*, PLOS ONE (Apr. 2012), at 1, 3 (describing distinct regional, gender, and socioeconomic variations among mobile phone owners in Kenya); Joshua Blumenstock & Nathan Eagle, *Mobile Divides: Gender, Socioeconomic Status, and Mobile Phone Use in Rwanda*, INT'L CONF. INFO. & COMMC'N TECHS. & DEV. 1, 1–2 (2010) (finding that mobile phone users in Rwanda are "disproportionately male, better educated, older, and come from larger households," highlighting the socioeconomic disparities in ownership).

88. *See* Patrick Liu et al., *Use of Mobile Health Applications in Low-Income Populations: A Prospective Study of Facilitators and Barriers*, 13 CIRCULATION: CARDIOVASCULAR QUALITY & OUTCOMES 687, 687, 689 (2020) (describing logistical challenges in enrolling populations in mobile health programs, including technological and economic concerns); Marie McCullough, *Useful Tool: Smart Thermometers Can Help in Tracking, but Many Are Not Used Correctly*, PHILA. INQUIRER, Nov. 18, 2020, at B1 (reporting that Philadelphia gave out 5,000 smart thermometers to low-income families, but ninety percent of the families failed to connect them to the app to enable community data gathering).

89. Liu et al., *supra* note 88, at 687.

90. Daniel Andrés Díaz-Pachón & J. Sunil Rao, *A Simple Correction for Covid-19 Sampling Bias*, 512 J. THEORETICAL BIOLOGY, 1, 1 (2021).

presence of fever.[91] However, a high body temperature, or fever, is not a primary indicator of the coronavirus infection, putting into question the value of aggregate temperature data.[92] As health officials expanded their understanding of COVID-19,[93] it became clear that some carriers could be asymptomatic.[94]

Bluetooth contact tracing applications assume that all physical proximity is a meaningful approximation of air flow.[95] However, location data that indicates the proximity of two devices cannot distinguish between two people in the same room or devices within the same distance between a wall.[96] Relational location sources generated from Bluetooth could be potentially meaningless without adding information that makes a distinction between hazardous and nonhazardous interactions, and relational mobility data alone does not provide that information.

Digital contact tracing fails to reflect the realities of jobs that interact with the public. Some people can avoid contact with people outside their household, and other people cannot. Anyone whose work puts them into contact with hundreds of random people daily could easily be overwhelmed by notifications of possible exposure. Public employees and "essential workers," who may not have the economic choice to

---

91. *Supra* notes 61–62 and accompanying text.

92. Sumanthi Reddy, *Temperature Isn't a Good Litmus Test for Coronavirus, Doctors Say*, WALL ST. J. (Sept. 21, 2020, 2:32 PM), https://www.wsj.com/articles/temperature-isnt-a-good-litmus-test-for-coronavirus-doctors-say-11600713159.

93. *See* Pam Belluck, *C.D.C. Adds New Symptoms to Its List of Possible COVID-19 Signs*, N.Y. TIMES (Aug. 5, 2020), https://www.nytimes.com/2020/04/27/health/coronavirus-symptoms-cdc.html.

94. Lisa Lockerd Maragakis, *Coronavirus Symptoms: Frequently Asked Questions*, JOHNS HOPKINS MED. (Feb. 24, 2021), https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/coronavirus-symptoms-frequently-asked-questions [https://perma.cc/A3ZQ-EXHH]. Sources indicate that anywhere between twenty-five to eighty percent of individuals who contract COVID-19 are asymptomatic. Roz Plater, *As Many as 80 Percent of People with COVID-19 Aren't Aware They Have the Virus*, HEALTHLINE (May 28, 2020), https://www.healthline.com/health-news/50-percent-of-people-with-covid19-not-aware-have-virus [https://perma.cc/795M-DZ4P].

95. *See* Ross Anderson, *Contact Tracing in the Real World*, LIGHT BLUE TOUCHPAPER (Apr. 12, 2020), https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world [https://perma.cc/FS2A-85M9] (describing an interaction that a Bluetooth device would flag as "mutual contact[]" despite a negligible risk of infection due to air flow and standing distance).

96. Douglas J. Leith & Stephen Farrell, *Coronavirus Contact Tracing: Evaluating the Potential of Using Bluetooth Received Signal Strength for Proximity Detection*, ARXIV 1, 5 (May 6, 2020), https://arxiv.org/pdf/2006.06822.pdf [https://perma.cc/F34Z-6Y66].

quarantine, face the extra burden of determining which notifications are viable threats.

Employees face an additional dilemma: health data collected by non-healthcare organizations do not qualify for HIPAA privacy protections.[97] Data collected through third-party apps can be aggregated and provided to employers in de-identified forms without violating HIPAA.[98] This leaves health-related pandemic data open for sharing among organizations that do not have a fiduciary responsibility to those employees.

Indeed, digital responses to the pandemic assume that people are willing to eschew their personal privacy in support of the public health effort. While Big Tech may enable data collection, governments may use those data sources in ways not anticipated by the public. For instance, the government in Singapore granted law enforcement access to contract tracing data to identify relationships between alleged criminals.[99] The reuse of data in both commercial and governmental contexts threatens the privacy of people who willingly volunteer their health data. The collection of data may persist after the emergency ends, further infringing on privacy rights.[100]

The freedom of association, inscribed in the United Nations Declaration of Human Rights, means that there is no penalty for choosing to be with other people.[101] Yet, during a pandemic, monitoring interpersonal associations is critical for public health. This tension

---

97. *See* Lisa Bari & Daniel P. O'Neill, *Rethinking Patient Data Privacy in the Era of Digital Health*, HEALTH AFFS. BLOG (Dec. 12, 2019), https://www.healthaffairs.org/do/10.1377/hblog20191210.216658/full [https://perma.cc/R3E9-JSWM] (arguing for updating HIPAA to ensure that privacy protections apply to all health data instead of only the data entered by specifically covered entities, e.g., healthcare providers).

98. *Id.*; *see, e.g.*, Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think (examining how employers use data from the pregnancy-tracking app Ovia to impact their bottom line). *See generally* 45 C.F.R. § 164.514 (2018) (defining de-identified health information as "[h]ealth information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information").

99. David Pierson, *Singapore Says Its Contact-Tracing Data Can Be Used for Criminal Investigations*, L.A. TIMES (Jan. 5, 2021, 5:17 AM), https://www.latimes.com/world-nation/story/2021-01-05/singapore-coronavirus-contact-trace-data-criminal-investigations.

100. Oliver et al., *supra* note 79, at 5.

101. *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) (affirming the rights of peaceful assembly and association).

between freedom and control underlies the many privacy concerns of deploying relational data solutions.[102]

E. Summary

This extended analysis of call logs, device location tracking, health apps, and digital contact tracing demonstrates flawed social assumptions and technological limitations of these solutions for the pandemic. Although these technologies purport to provide solutions for public health, they generally only work within limited technical and social settings. This alone may be cause for concern, but the organizations representing this interest in pandemic data technology also have conflicts of interest.

II. CONFLICTS OF INTEREST

Proximity and health information is valuable outside of the pandemic context, making it vulnerable to misuse. Many organizations have financial interests that conflict with public health interests. It is plausible that private healthcare organizations and digital platforms would keep pandemic-related information to support their own predictive products. Any public health deployment of pandemic technology must recognize the reuse value of its data and the potential for exploitation.

A. Data Reuse

Data innovation interconnects new digital sources to derive predictive accuracy as a competitive advantage.[103] Drawing on the initial success of segmenting consumers geospatially by postal codes,[104]

---

102. Oliver et al., *supra* note 79, at 1, 4 (describing concerns that the pandemic may be used to "create and legitimize surveillance tools used by government and technology companies that are likely to persist beyond the emergency").

103. Data innovation uses traditional and non-traditional sources of data to obtain novel analyses on otherwise complex or impossible problems. UNITED NATIONS DEV. PROGRAMME, A GUIDE TO DATA INNOVATION FOR DEVELOPMENT: FROM IDEA TO PROOF-OF-CONCEPT (2017) (defining non-traditional sources as digital data from social media, web content, transactions, and GPS devices). This process is commonly referred to as data analytics, which utilizes algorithms to derive conclusions from raw data. *See, e.g.*, Cathy Petrozzino, *Big Data Analytics: Ethical Considerations Make a Difference*, 16 SCITECH LAW. 14, 15 (2020); BROOKINGS INST., *supra* note 43 ("Algorithms are harnessing volumes of macro- and micro-data to influence decisions affecting people in a range of tasks, from making movie recommendations to helping banks determine the creditworthiness of individuals.").

104. *See* Veronica K. McGregor et al., *Big Data and Consumer Financial Information*, BUS. L. TODAY, Nov. 2013, at 1, 2 (explaining that Big Data allows for "customer micro-

digital advertising inevitably will seek to use pandemic mobility data to improve marketing.

The reuse of data for a purpose outside of the original intention touches on many legal and ethical concerns, although it is a common practice. In one example, a DNA sample from a routine medical procedure connected the patient's relative to a crime scene.[105] The Chicago police maintains a database[106] of *potential* gang members based on Facebook friends and photos of teenagers on the social networking site.[107] Free mental health support in New York City funnels data into the algorithms that determine whether children will be removed from

---

segmentation," which divides consumer bases into more granular segments to track their behavior); Angela Byers, *Big Data, Big Economic Impact?*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 757, 758–59 (2015) ("Application of [micro-segmentation] . . . can be revolutionary . . . in the public sector, where tailoring actions or service levels to population segments with different needs can actually make more efficient use of limited resources.").

105. *See* Ellen Nakashima, *From DNA of Family, a Tool to Make Arrests*, WASH. POST, Apr. 21, 2008, at A01 (explaining how law enforcement connected serial killer BTK to several crime scenes by comparing DNA from the crime scenes to DNA from his daughter's routine Pap smear).

106. Annie Sweeney & Paige Fry, *Thousands of Youths in Gang Databases: Critics Say CPD Records Out-of-Date, Skewed, Harmful*, CHI. TRIB., Aug. 9, 2018, at 1. Juveniles who lose a relative or a friend to gun violence are put into the system as potential gang members even if they do not participate in any gangs. *Id.* Similarly, individuals without criminal records may be identified in the database as gang members simply because of where they live. Mick Dumke, *Chicago's Gang Database Is Full of Errors—And Records We Have Prove It*, PROPUBLICA (Apr. 19, 2018, 4:00 AM), https://www.propublica.org/article/politic-il-insider-chicago-gang-database; Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. 192, 208–09 (2019) ("[A] computerized assessment tool . . . identifies and ranks individuals at risk of becoming a victim or possible offender in a shooting or homicide.").

107. *Tracked and Targeted: Early Findings on Chicago's Gang Database*, POLICING IN CHI. RSCH. GRP. 3 (Feb. 2018), http://erasethedatabase.com/wp-content/uploads/2018/02/Tracked-Targeted-0217.pdf; *see* CHI. OFF. INSPECTOR GEN., REVIEW OF THE CHICAGO POLICE DEPARTMENT'S "GANG DATABASE" 4 (2019), https://igchicago.org/wp-content/uploads/2019/04/OIG-CPD-Gang-Database-Review.pdf (finding that the gang database lacks sufficient data maintenance mechanisms, procedural protections, and transparent practices). The Office of Inspector General for the City of Chicago found that Black, African American, and Latinx persons account for ninety-five percent of the 134,242 individuals designated as gang members. *Id.*; *see also* Class Action Complaint at 2–3, Chicagoans for an End to the Gang Database v. City of Chicago, No. 18-CV-4242 (N.D. Ill. 2018) (alleging that the database disproportionately targets Black and Latinx people and that officers abuse their unlimited discretion in a discriminatory manner).

the home.[108] Information that was originally intended to support the needs of newly released prisoners instead calculates a risk assessment score that may curtail their future.[109] In these examples, the original purpose of the data collection was perverted to penalize instead of support. The data from the person seeking services, such as the teenager or the hospital patient, suddenly becomes the vehicle of a punitive system.

The crossover between public health and other uses is not theoretical. While many possible motivations for data reuse exist, it is inevitable that law enforcement, marketers, researchers, and the curious may want to know how people associate with each other. Reuse of pandemic data for financial profit is particularly concerning when it involves private healthcare organizations seeking to minimize costs or digital platforms seeking to improve digital advertising.

---

108. CHAPIN HALL, STRONG FAMILIES NEW YORK CITY: FINAL EVALUATION REPORT 14, 17 (2019) (detailing the "Partnering for Success" initiative, which provides mental health counseling to children and caregivers, and also informs the Strong Families evaluation model). New York City's Administration for Children's Services (ACS) uses numerous public services to evaluate the competence of parents whose children will be put in foster care. *Id.* at 17. Even parents who forgo public services to preserve their privacy run the risk of being turned into ACS as neglectful or incompetent for not using the free city services. Stephanie K. Glaberson, *Coding over the Cracks: Predictive Analytics and Child Protection*, 46 FORDHAM URB. L.J. 307, 350 & n.233 (2019). Child protective agencies nationwide employ similar data analysis programs. Dan Hurley, *Can an Algorithm Tell when Kids Are in Danger?*, N.Y. TIMES (Jan. 2, 2018) https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html.

109. The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) system was originally created within a university to help local communities. *See* Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. The software is used by courts as a risk assessment score to predict a defendant's likelihood to recidivate. *See id.* (analyzing the accuracy of COMPAS's predictive analytics). The tool manipulates the offender's therapeutic *needs* as risks. For instance, if someone needs (or previously needed) addiction services, they are labeled as "at risk." *Measurement & Treatment Implications of COMPAS Core Scales*, NORTHPOINTE, INC. 20 (2009), https://www.michigan.gov/documents/corrections/Timothy_Brenne_Ph.D.__Meaning_and_Treatment_Implications_of_COMPA_Core_Scales_297495_7.pdf [https://perma.cc/STA3-AEG3] ("Have you ever been in formal treatment for alcohol such as counseling, outpatient, inpatient, residential?"); *Practitioner's Guide to COMPAS Core*, NORTHPOINTE, INC. 43–44 (Mar. 19, 2015), http://www.northpointeinc.com/downloads/compas/Practitioners-Guide-COMPAS-Core-_031915.pdf (explaining how inputs affect scores, e.g., past treatment for alcohol will raise an individual's score on the substance abuse scale). Studies have found that the COMPAS tool suffers from analysis bias, scoring Black offenders higher on the risk assessment scale than white offenders with similar or worse backgrounds. Petrozzino, *supra* note 103, at 15–16.

B. Profits and Patients

The U.S. healthcare system is built on a network of private healthcare organizations that bill for each unique health event.[110] This financial model is less than ideal when the volume of events is high with little monetary reward. A global pandemic exacerbates the challenges with the model further because everyone needs to be healthy for anyone to be healthy.

Private hospitals, healthcare maintenance organizations (HMOs), and individual physician practices are for-profit entities that are motivated to limit expenses and increase profits. Private businesses also select clients or market to certain groups over others. Private hospitals and healthcare organizations are motivated to limit access to care in order to manage budgets.[111] Digital mobility data is invaluable for building actuarial models of risk. While all healthcare organizations in the United States are subject to HIPAA laws that limit how they handle patient data,[112] they may use internal data to inform actuarial models.[113] These organizations have a financial motivation, and possibly an obligation, to screen out or limit the number of sick people under their care.[114]

Particularly in the United States, patients with limited access to health insurance may be overrepresented in job categories that are

---

110. *See generally* Terry Gross, *Why an ER Visit Can Cost so Much—Even for Those with Health Insurance*, NAT'L PUB. RADIO (Mar. 13, 2019, 1:27 PM), https://www.npr.org/2019/03/13/702975393/why-an-er-visit-can-cost-so-much-even-for-those-with-health-insurance [https://perma.cc/D9TW-7LRQ] (exploring healthcare expenses in the United States, where an ibuprofen can be a $60 line item on a hospital bill, and comparing the structure to countries where the government is more involved in regulating healthcare prices).

111. *See* EMILY GEE, CTR. AM. PROGRESS, THE HIGH PRICE OF HOSPITAL CARE 1, 10 (2019) (examining healthcare costs and hospital profits in the United States). For example, health insurers use "lifestyle data" from third-party sources to complement actuarial assessments, identify high-risk patients, and maximize profits. *See* Marshall Allen, *Health Insurers Are Vacuuming up Details About You—And It Could Raise Your Rates*, PROPUBLICA (July 17, 2018, 5:00 AM), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates [https://perma.cc/63BB-2M2Z].

112. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 § 221, 110 Stat. 1936, 2009 (1996); *Your Health Information Privacy Rights*, DEP'T HEALTH & HUM. SERVS. OFF. C.R., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf?language=es [https://perma.cc/4G6P-NHBH].

113. 45 CFR §§ 160.103, 164.501, 164.506; *Permitted Uses and Disclosures: Exchange for Health Care Operations*, DEP'T HEALTH & HUM. SERVS. OFF. C.R. (Jan 2016), https://www.hhs.gov/sites/default/files/exchange_health_care_ops.pdf.

114. *Id.*; *see supra* note 112 and accompanying text.

considered essential during the pandemic: delivery services, transportation, education, or healthcare.[115] People in these categories may be reasonably hesitant to share data with a healthcare system that might use a positive status to withhold, limit, or refuse healthcare.[116] This means that the virus might continue in a vicious cycle if the people who interact with a large number of people do not have appropriate healthcare.

C. Advertising Models

All data sources are of interest to marketers and therefore to any large digital platform, including those of two popular mobile device manufacturers: Apple and Google. Digital businesses exploit new verified third-party data sources to improve advertisement delivery.

Advertising ecosystems leverage data to better target ads or find new clients, especially through existing clients. Friend of a Friend (FOAF) information is a mathematical and spatial representation of who is connected to whom.[117] FOAF reveals social connections and interpersonal associations usually based on voluntary data shared on a social networking site.[118] Pandemic proximity sources that describe how people congregate provides valuable new information about interpersonal and FOAF relationships that may not be available elsewhere.[119]

Proximity data might not only be used for digital advertising. Insurance companies, credit reporting agencies, and other organizations that rely on risk calculations may be interested in evaluating who is in proximity to the virus. This might lead to an equivalent of health redlining that isolates neighborhoods deemed to be less profitable and more

---

115. Jennifer Valentino-DeVries et al., *Location Data Says It All: Staying at Home During Coronavirus Is a Luxury*, N.Y. TIMES (Apr. 3, 2020), https://www.nytimes.com/interactive/2020/04/03/us/coronavirus-stay-home-rich-poor.html.

116. *Cf.* Maria Karampela et al., *Connected Health User Willingness to Share Personal Health Data: Questionnaire Study*, 21 J. MED. INTERNET RSCH. 8 (2019) (noting that misuse of information fuels a lack of trust, which decreases willingness to share data).

117. *See* Jennifer Golbeck & Matthew Rothstein, *Linking Social Networks on the Web with FOAF: A Semantic Web Case Study*, ASS'N FOR ADVANCEMENT A.I. 1138, 1138–39 (2008), https://www.aaai.org/Papers/AAAI/2008/AAAI08-180.pdf (describing FOAF as "a framework for representing information about people and their social connections").

118. *Id.* (showing how FOAF systems work across multiple accounts).

119. *See* Stacey Gray, *A Closer Look at Location Data: Privacy and Pandemics*, FUTURE PRIV. F. (Dec. 17, 2020), https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics [https://perma.cc/T8ZZ-RZ48] (explaining that location data needs to be precise to be valuable to researchers studying the pandemic since transmission is related to physical proximity between individuals).

vulnerable to outbreaks.[120] The reuse of pandemic proximity data as a punitive assessment would penalize people who live in densely populated locations or workplaces that interface with the public. Furthermore, this may limit the potential for tourism or locations that rely on positive promotion. For instance, New York City's Chinatown has suffered tremendous financial losses due to a false assumption that it has a risky proximity to the virus.[121]

D. Summary

The financial conflicts of interest of large organizations that may offer pandemic data solutions cannot be ignored. Organizations with access to pandemic proximity information would improve their competitive edge over other businesses.[122] Organizations that share proximity data violate the trust of people whose movements are traced.[123] The tension between valuable data assets and personal empowerment creates little incentive for individuals to share their information, assuming they have a choice.

The effectiveness of digital data is often limited by the effectiveness of public health interventions. Public health officials emphasize the importance of test-trace-treat as the three pillars of handling an infectious disease;[124] however, the data-driven pandemic technology only addresses the trace pillar. Information about positive tests is necessary in conjunction with location data to make digital contact tracing viable.

---

120. *See generally* MEHRSA BARADARAN, THE COLOR OF MONEY: BLACK BANKS AND THE RACIAL WEALTH GAP (2017); KEEANGA-YAMAHTTA TAYLOR, RACE FOR PROFIT: HOW BANKS AND THE REAL ESTATE INDUSTRY UNDERMINED BLACK HOMEOWNERSHIP (2019).

121. *See* Laura Bliss, *Chinatown Businesses Face a Particularly Brutal Winter*, BLOOMBERG (Dec. 7, 2020, 3:54 PM), https://www.bloomberg.com/news/articles/2020-12-07/covid-19-has-been-a-disaster-for-u-s-chinatowns (indicating several reasons why the pandemic has hit Chinatowns across the country especially hard, including xenophobia and the collapse of the tourism industry).

122. This phenomenon is particularly concerning in the context of digital markets. Due to digital markets' complexity and reach, some view the technology industry as above supervision or "too big to audit." David Morar & Anne Washington, *How a Compliance Mindset Undermines Antitrust Reform Proposals*, BROOKINGS INST.: TECH STREAM (Sept. 3, 2020), https://www.brookings.edu/techstream/how-a-compliance-mindset-undermines-antitrust-reform-proposals.

123. *See, e.g.*, *supra* notes 105–09 and accompanying text (providing examples of people who suffer adverse effects when their information is tracked and shared).

124. *E.g.*, Laura Bicker, *Coronavirus in South Korea: How 'Trace, Test and Treat' May Be Saving Lives*, BBC NEWS (Mar. 12, 2020), https://www.bbc.com/news/world-asia-51836898.

Even if all mobile device owners generated location data and chose to share their information, the limited and selective sample may still hamper the technology's full effectiveness. Effective public health monitoring requires acquisition of complete population information, which is the opposite of what occurs under the current system. To the extent that individual choice contributes to the lack of complete data, imposing a fiduciary responsibility upon those who possess proximity is a way to resolve the conflict-of-interest issue.

III. FIDUCIARY POLICY SOLUTIONS

A fiduciary has a legal responsibility to protect client confidentiality and interests. While fiduciaries have long standing in business and law, the concept of an information fiduciary is still hotly debated amongst legal scholars.[125] Pandemic data technology might be an opportunity to move information fiduciary theory into practice. We define trust within the context of pandemic data technology, and outline what issues an information fiduciary could solve.

A. Trust

Without explicit guidelines or regulation, it would be very hard to investigate how data have travelled, to whom, or why. Outside regulators, journalists, or interested citizens should be able to track the flow of public health information. The trust that exists between data aggregators and the public is essential to understanding why fiduciaries are necessary during a public health emergency.

Trust must exist throughout the data supply chain that moves data between organizations. Very often, companies do not share first-party data, but instead bundle interpretations of data, such as categories for

125. *Compare* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016) (stating that information fiduciaries can reconcile the conflicting interests between the "information age requir[ing] regulation of new forms of social and economic power . . . [and] the constitutional freedoms of the First Amendment"), *with* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 500–01 (2019) (questioning whether creating information fiduciaries modeled on fiduciary relationships of professionals like doctors and accountants is sufficient to protect users), *and* Claudia E. Haupt, Response, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 36–37 (2020) (rejecting the professional fiduciary model for the trustee-beneficiary relationship that could provide a more successful model for information fiduciaries).

targeted advertisements.[126] As Mark Zuckerberg testified in response to congressional complaints about Facebook selling data, "Senator, we run ads."[127] As long as data are exchanged within long chains of custody, a duty of care among all who may use the data is necessary to guarantee that trust. When data are held over long periods of time or held by different organizations, the potential for negative use later in the chain grows.

Trust must exist at the ends of the data supply chain as well. People depend on organizations to hold their public health-related data about them in trust. This is not about trust between one individual and one company such as a consumer-business relationship. Rather, people want to trust that organizations will not penalize them or negatively exploit their information.[128] Specifically, people need to be able to trust that organizations are not distracted by financial gain when creating public health solutions.

Trust in the government's ability to safeguard information or hire appropriate contractors is also at stake. Philly Fighting COVID switched from non-profit to commercial status after it obtained a contract with the City of Philadelphia.[129] In its few short weeks as a vaccine distributor, Philly Fighting COVID gathered sensitive health data for thousands of local residents without delivering vaccines or

126. Mae Anderson & Anick Jesdanun, *AP Fact Check: Facebook Doesn't Sell Data but Profits off It*, ASSOCIATED PRESS (Apr. 10, 2018), https://apnews.com/article/6f5156879a3a48218b509c97fcc28e39.

127. Facebook, Social Media Privacy, and the Use and Abuse of Data: J. Hearing Before the S. Comm. on Com., Sci., & Transp. and the S. Comm. on the Judiciary, 115th Cong. 21 (2018) (statement of Mark Zuckerberg of Facebook).

128. *See, e.g.*, Timothy Colman et al., *The Data Is in. People of Color Are Punished More Harshly for Covid Violations in the US*, GUARDIAN (Jan. 6, 2021), https://www.theguardian.com/commentisfree/2021/jan/06/covid-violations-people-of-color-punished-more-harshly (explaining that people of color and immigrants are subject to punitive public health enforcement); PASCAL EMMER, UNMASKED: IMPACTS OF PANDEMIC POLICING 23, 28 (2020), https://communityresourcehub.org/unmasked (discussing how the response to the COVID-19 pandemic has been to enforce public health guidance through policing, surveillance, criminalization and civil fines, and increased data-sharing between public health agencies and the police). *See generally COVID-19: Stay-at-Home and Social Distancing Enforcement*, POLICING PROJECT N.Y.U. SCH. LAW (May 20, 2020), https://www.policingproject.org/news-main/2020/5/20/covid-19-stay-at-home-and-social-distancing-enforcement (outlining a series of proposed best practices for police and local political leaders to appropriately enforce social distancing and mask orders without disparately affecting vulnerable communities).

129. Emily Scott, *What You Need to Know About the Philly Fighting COVID Scandal*, WHYY (Jan. 28, 2021), https://whyy.org/articles/what-you-need-to-know-about-the-philly-fighting-covid-scandal.

appointments.[130] Governments are trusting contractors to not exploit citizen information while delivering technology solutions.[131]

Data aggregation has been one means to protect consumers; however, public health officials need details, not aggregate data. A pandemic requires in-depth analysis to plan hospital allocation patterns, first responder staffing, or vaccine rollout schedules. The technology industry has no interest in sharing detailed information and would violate many laws and conventions if it did share it. Having this wealth of information only in the hands of a few commercial organizations reduces the ability of the data to make an impact on the public health crisis and potentially increases the incentive to profit off that data.

While the legal information fiduciary debate has focused on commercial businesses, the application in the public sector, and for public-private partnerships, has the most promise.

B. Information Fiduciaries

The legal scholar Jack Balkin introduced the concept of an information fiduciary in a 2016 law review article based on three laws of an algorithmic society.[132] An information fiduciary, as Balkin suggests, would resolve potential abuses of power by anyone with the computational power to control large populations.[133] Balkin emphasizes the asymmetries of information that make individuals vulnerable to and dependent on digital companies.[134] In addition to Balkin's three laws,

---

130. *Id.*

131. *See* Cat Ferguson, *What Went Wrong with America's $44 Million Vaccine Data System?* MIT TECH. REV. (Jan. 30, 2021), www.technologyreview.com/2021/01/30/1017086/cdc-44-million-vaccine-data-vams-problems (outlining how the CDC contracted with Deloitte to build a COVID-19 vaccination distribution system).

132. Jack M. Balkin, Lecture, *2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1226–27 (2017) [hereinafter Balkin, *Three Laws of Robotics*] (obligating algorithm users to public duties regardless of whether the user is a public or private actor). Balkin defines the Algorithmic Society as "a society organized around social and economic decision-making by algorithms, robots, and AI agents." *Id.* at 1219. *See generally* Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/64L8-UBMU] (presenting the concept of "information fiduciaries"); Balkin, *supra* note 125, at 1221 (expanding information fiduciary duties to online service providers in the digital age).

133. Balkin, *Three Laws of Robotics*, *supra* note 132, at 1226–27.

134. *Id.* at 1127–29.

Frank Pasquale argued for a fourth law that grapples with issues of power based on the source, creator, or owner of the algorithm.[135]

The legal debate on merits of an information fiduciary has considered the obligation of digital businesses, such as Google, Twitter, Amazon, and Facebook. David Pozen and Linda Khan are skeptical of information fiduciaries, emphasizing that their costs could easily lead to complacency.[136] They argue that information fiduciaries are largely immaterial because there is no way to test or confirm fiduciary responsibilities if a company exercises monopoly power within the industry.[137] In a response to Pozen and Khan's skepticism of information fiduciaries in favor of antitrust actions, Balkin reiterated the importance of building trust between individuals and the institutions that use their data.[138] Antitrust actions would not eliminate the desire of the resultant companies to earn a profit off of their surveillance.[139] We argue that if we cannot imagine information fiduciaries, we will not have successful antitrust. When AT&T split up, one "Ma Bell" dissolved into many "Baby Bells" that implemented similar business models and payment structures while competing for customers with innovations.[140] Trust could be further diminished if more companies repeat the same business models with few internal

---

135. *See* Frank Pasquale, Lecture, *Response: Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society*, 78 OHIO STATE L.J. 1243, 1253–54 (2017) (proposing a fourth law, "[a] robot must always indicate the identity of its creator, controller, or owner"); *see also* FRANK PASQUALE, NEW LAWS OF ROBOTICS: DEFENDING HUMAN EXPERTISE IN THE AGE OF AI 11 (2020).

136. *See* Khan & Pozen, *supra* note 125, at 502, 537 (finding that Balkin's fiduciary approach would "cannibalize rather than complement procompetition reforms" and allow Facebook to become the fiduciary of millions of Americans' personal data without government intervention).

137. *Id.* at 537, 540 ("An entity that is designated by the government as a loyal caretaker for the personal data of millions of Americans is not an entity that is liable to be dismantled by that same government.").

138. *See* Jack M. Balkin, Response, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 11, 13, 22 (2020) ("The goal of the fiduciary models is to require digital companies, which are not trustworthy stewards of the data they collect and use, to become trustworthy and look out for the interests of end users . . . . [T]here is no reason why antitrust should be anti-trust." (quoting Interview by Jack M. Balkin with Neil Richards, Professor, Wash. U. St. Louis, in Palo Alto, Cal. (Mar. 19, 2019)).

139. *Id.* at 22.

140. Jose Pagliery, *How AT&T Got Busted up and Pieced Back Together*, CNN (May 20, 2014, 9:30 AM), https://money.cnn.com/2014/05/20/technology/att-merger-history; *see* United States v. AT&T, 552 F. Supp. 131, 200–01, 225 (D.D.C. 1982), *aff'd sub nom.*, Maryland v. United States, 460 U.S. 1001 (1983) (detailing the terms of AT&T's divestment from its Bell Operating Companies or "Baby Bells").

governance mechanisms and little regulatory oversight.[141] Bringing the information fiduciary concept to the table in advance of antitrust enforcement action may support successful divisions of large companies.

In the case of healthcare, the premise of these arguments shifts. The information needs are by default wide-reaching and have to operate, not at the consumer level, but across the entire population. Information fiduciaries are essential to understanding the issues inherent in digital solutions to public health emergencies. Furthermore, implementing an information fiduciary for pandemic data serves to advance conversations about implementing this concept at a broader scale for social networking sites or other commercial services.

Health information, unlike other personally identifiable information (PII), consists of immutable characteristics that the patient has little control over changing, unlike details such as employment status. One person's health information might also impact the health status of the person's relatives, which escalates the stakes for sharing data. Anyone might naturally feel vulnerable sharing personal health details under these conditions. Vulnerabilities from sharing are exponential in a privatized healthcare system where every change in health status is a financial calculation.[142] Patients who share personal health details are made vulnerable to a host of institutional data systems which have a clear financial conflict of interest.[143]

Could an information fiduciary protect patients' interests during a pandemic?

C. Policy Solutions

We offer two tangible suggestions for implementing the information fiduciary concept in practice: conflict-of-interest notices and third-party stewards for pandemic-related health data.

---

141. *See* Morar & Washington, *supra* note 122 ("[D]ividing a large company into many smaller ones will not address the issue at hand, as the business practices of the dominant player are likely to be replicated throughout the industry . . . [potentially] to the detriment of consumers."). *But see* Robert H. Lande & Richard O. Zerbe, *The Sherman Act Is a No-Fault Monopolization Statute: A Textualist Demonstration*, 70 AM. U. L. REV. 497, 564–66 (2020) (highlighting the innovation boom post-AT&T breakup).

142. *See supra* Section II.B (discussing insurance companies' use of actuarial models).

143. *See supra* Section II.A (providing examples of ways in which law enforcement and others use data outside of its original purpose).

1. Conflict-of-interest notices

Organizations that maintain access to any pandemic-related data must submit a digital public filing of conflict of interest. Journalists, litigators, or the public could use these filings for investigations like any other open data source.[144] Organizations face a reputational cost when conflict-of-interest notices are released publicly.[145] This reduces the burden on the individual for misplaced trust,[146] a known problem in consumer technology. The issue of misplaced trust in pandemic technology is similar to how the third-party doctrine placed the burden on consumers for trusting a deceitful actor with their data and communications.[147] In addition, to prevent the misuse towards surveillance by employers and government, public health officials may use these associations if—and only if—the data does not penalize the subject of the data. Conflict-of-interest notices do not protect data but could be an essential mechanism to build trust.

2. Public health fiduciary

A public health fiduciary would have legal responsibility to protect data relevant to epidemiological outbreaks. It would protect patient interests and maintain confidentiality of location data related to the pandemic. A new public health entity would pledge a fiduciary

144. A wide variety of people are open data consumers. Anne L. Washington, *Who Do You Think We Are? The Data Publics in Digital Government Policy*, HAW. INT'L CONF. SYS. SCI. 3264 (2019).

145. *See, e.g.*, Derek Willis, *New in the Congress API: Lobbying Registrations and More*, PROPOLITICA, (June 6, 2018), https://www.propublica.org/nerds/propublica-congress-api-lobbying-registrations-and-more (including more data in the Congress API which gives information about lobbyists in Congress); Diane Ravitch, *ProPublica Exposes the Big Business of Lobbying*, DIANE RAVITCH'S BLOG, (Jan. 17, 2020), https://dianeravitch.net/2020/01/17/propublica-exposes-the-big-business-of-lobbying (arguing that "[t]o save our democracy, we have to understand who is using big money to buy influence," which involves knowing who is trying to influence certain lawmakers); *see also Series—A Users Guide to Democracy*, PROPUBLICA, https://www.propublica.org/series/a-users-guide-to-democracy (linking to various exposures of conflict-of-interest notifications).

146. *See* Brennan-Marquez, *supra* note 27, at 637 & n.112, 644, 646, 657, 659 (2015) (advocating that doctors, hotel staff, and internet service providers should be designated information fiduciaries in a Fourth Amendment context when sharing trusted user data with law enforcement).

147. Courts have long held that third-party reports to law enforcement do not violate Fourth Amendment protections of consumers who provide a third party with their data. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 111, 125–26 (1984) (private freight carrier reports); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (telephone company reports); United States v. Miller, 425 U.S. 435, 443 (1976) (bank reports).

responsibility to digital public health data and its distribution for only medical necessary reasons. A public health fiduciary would oversee who had access to the data in addition to tracking distribution and use. Active data distribution monitoring would allow for just-in-time access to data and discourage hoarding data for unknown future uses.

We recognize that it might be possible for an existing organization to commit to fiduciary responsibilities. However, large commercial organizations may struggle to establish that trust if they have marketing, risk management, or research teams that could benefit from access to the data. Government organizations may be distracted by politics and elections. Ideally a new public health entity would take on these responsibilities. Even a short-term pandemic-only organization would be useful to consider the impact of this data moving forward.

Regulatory enforcement or legal recourse could hold organizations to account for violating this trust. Additional policy instruments such as fines, organizational restrictions, antitrust, or other existing regulatory tools may enforce a duty of care.

CONCLUSION

Data-centric solutions may not limit the spread of the virus as intended if the technology relies on inaccurate assumptions and the organizations involved have financial interests that override other priorities. Any public health effort must have an ultimate goal of centering patient treatment and wellness.

It is imperative to develop mechanisms to protect the privacy of currently invisible populations, whether through increased political power, better privacy protections, or enhanced oversight. The act of sharing health data makes people vulnerable to institutions that may have interests in opposition to their own. Without the protection of all populations, public health goals using digital technology will fail. The visibility of all members of a community is essential to support public health efforts, but often that requires increasing surveillance with potentially negative consequences.

We believe that technology should be part of the public health solution; however, it should be led by a desire to meet the mission to serve all residents within a geographic area. A public health information fiduciary is the best solution to the conflicts of interest. Valuable proximity information could be used to fight the virus if it were not detrimental to the people whose locations are tracked.