BUT WHAT IF BIG BROTHER'S SURVEILLANCE SAVES LIVES?—COMPARATIVE DIGITAL PRIVACY IN THE TIME OF CORONAVIRUS*

APRIL XIAOYI XU†

"Big Brother Is Watching You."
- George Orwell, *1984*[1]

---

* This Essay was written in mid-April 2020. Due to the rapidly-evolving situation surrounding the novel coronavirus, new data and studies, digital privacy policies, and laws in each jurisdiction may have emerged or altered post-completion of this Essay.

† J.D. Candidate, Harvard Law School (2021); B.A., *summa cum laude*, Pomona College (2018). I would like to thank my family, friends, and professors for their support during this trying period in life. Special thanks go to my parents Amy and Frank, and my grandparents, for always being there for me despite the geographical distance between us, Professor Urs Gasser for all his guidance and expertise that inspired this Essay in invaluable ways, Professor Jeannie Suk Gersen for her mentorship and encouragement, Zahra Takhshid for suggestions for this Essay, Andrew B. Liu (Ph.D. candidate at Harvard Medical School) for his insights on bioinformatics and epidemiology, Kent A. Shikama for kindling my interest in exploring intersections between law and technology, and my classmates for enlightening discussions on comparative digital privacy. I also wish to thank the *Creighton Law Review* editors for their diligence and professionalism throughout the editing process.

1. GEORGE ORWELL, 1984, at 3 (1949).

I. INTRODUCTION AND CONTEXT: CURTAILING DIGITAL PRIVACY RIGHTS AS A NECESSARY EVIL TO END THE DYSTOPIAN NEW NORMAL UNDER THE COVID-19 REGIME

By April 2020, a significant portion of students from across the globe were taking classes online instead of learning with their friends at school.[2] Most working-age adults found themselves at home, many unemployed.[3] Everyone worried every day about the safety and health—the most fundamental needs—of loved ones. Across public spaces, "no entry" signs and posters reminded individuals to stay six feet away from each other to strictly enforce social distancing at all times.[4] Bustling restaurants and bars were ordered to shut down, save for a few diligent takeout and delivery locations.[5] Streets were virtually empty.[6] Travel was effectively out of question, as were wed-

2. *See, e.g.*, *Map: Coronavirus and School Closures*, EDWEEK (Mar. 6, 2020), https://www.edweek.org/ew/section/multimedia/map-coronavirus-and-school-closures.html; Benjamin Herold, *The Scramble to Move America's Schools Online*, EDWEEK (Mar. 27, 2020), https://www.edweek.org/ew/articles/2020/03/26/the-scramble-to-move-americas-schools-online.html.

3. *See, e.g.*, Patricia Cohen & Tiffany Hsu, *'Sudden Black Hole' for the Economy With Millions More Unemployed*, N.Y. TIMES (Apr. 9, 2020), https://www.nytimes.com/2020/04/09/business/economy/unemployment-claim-numbers-coronavirus.html.

4. *See, e.g.*, *COVID-19 Social Distancing Poster*, VT. DEP'T. OF HEALTH, https://www.healthvermont.gov/sites/default/files/documents/pdf/COVID-social-distancing-poster-ltr.pdf (last visited Aug. 30, 2020).

5. *See, e.g.*, *From Pandemic to Protests: How Food Businesses Nationwide Are Responding*, BON APPETIT, https://www.bonappetit.com/story/food-businesses-covid-19 (last visited Aug. 30, 2020).

6. *See, e.g.*, Jessica Snouwaert, *13 photos of New York City looking deserted as the city tries to limit the spread of the coronavirus*, BUS. INSIDER (Apr. 1, 2020), https://www.businessinsider.com/coronavirus-pictures-of-new-york-city-empty-streets-2020-3.

dings, honeymoons, Easter get-togethers, and graduation ceremonies.[7]

As dystopian as these portraits of society may sound, they were, in one way or the other, the new normal as the world confronted a new common enemy in 2020: the novel coronavirus, "COVID-19."[8] Although these curtailments to one's civil liberties appeared extreme and the social changes were drastic,[9] especially in liberal democracies such as the United States, new policies and laws imposed by governments worldwide in response to COVID-19 became the necessary evil to mitigate the consequences of the pandemic and to rid the world of this highly contagious and fatal virus as promptly as possible.[10]

Disease models from epidemiologists including Marc Lipsitch, professor of epidemiology and director of the Center for Communicable Disease Dynamics at Harvard Medical School, demonstrate that intermittent periods of social distancing may be the best option to control the COVID-19 pandemic, for this "on-again, off-again approach" would "protect hospitals from being overwhelmed with sick patients, buy them time to gather adequate medical supplies, and allow the population to slowly gain immunity."[11] In the absence of an effective vaccine

---

7. *See, e.g., Coronavirus disease (COVID-19) travel* advice, WORLD HEALTH ORG., https://www.who.int/emergencies/diseases/novel-coronavirus-2019/travel-advice (last visited Aug. 14, 2020).

8. *See generally Coronavirus disease (COVID-19) pandemic*, WORLD HEALTH ORG., https://www.who.int/emergencies/diseases/novel-coronavirus-2019 (last visited Aug. 14, 2020).

9. *See* Danielle Allen et al., *Securing Justice, Health, and Democracy Against the COVID-19 Threat*, EDMOND J. SAFRA CTR. FOR ETHICS AT HARV. UNIV. WHITE PAPERS 11-20 (2020) (discussing how measures to suppress the spread of COVID-19 can impact civil liberties); Brett Milano, *Restricting Civil Liberties Amid the COVID-19 Pandemic,* HARV. LAW TODAY (Mar. 21, 2020), https://today.law.harvard.edu/restricting-civil-liberties-amid-the-covid-19-pandemic/?utm_source=hltnewsletter&utm_campaign=Mar252020 (providing examples of government-mandated restrictions to civil liberties).

10. *See, e.g.*, GPA Executive Committee, *Statement by the GPA Executive Committee on the Coronavirus (COVID-19) Pandemic*, GLOB. PRIVACY ASSEMBLY (Mar. 17, 2020), https://globalprivacyassembly.org/gpaexco-covid19/ (indicating that members of the Executive Committee of the Global Privacy Assembly ("GPA") support the sharing of personal data by organizations and governments for the purposes of fighting the spread of the COVID-19 pandemic). The GPA brings together data protection regulations from over 80 countries. *Id.*

11. *Coronavirus news – April 2020*, HARV. T. H. CHAN SCH. OF PUB. HEALTH (Apr. 11, 2020), https://www.hsph.harvard.edu/news/hsph-in-the-news/coronavirus-news-april-2020/; *see also* Joel Hellewell et al., *Feasibility of Controlling COVID-19 Outbreaks by Isolation of Cases and Contacts*, 8 LANCET GLOB. HEALTH 488, 489-96 (2020) (containing a mathematical study using a stochastic transmission model that is parameterized to the COVID-19 outbreak). *Accord* Gypsyamber D'Souza & David Dowdy, *What is Herd Immunity and How Can We Achieve It With COVID-19?*, JOHNS HOPKINS BLOOMBERG SCH. OF PUB. HEALTH (Apr. 10, 2020), https://www.jhsph.edu/covid-19/articles/achieving-herd-immunity-with-covid19.html (stating that herd immunity requires "at least 70% of the population" to either get infected or get a protective vaccine to be immune and have herd protection; clearly, the former approach is unrealistic, as getting

and antiviral drugs, governments need to modulate the trajectory of the epidemic "so that the impact on global health is minimized and each epidemic wave does not exceed [ ]healthcare system capabilities."[12]

On a macro level, to slow and contain the spread of COVID-19, governments should have at least three policy and legal objectives in regulating social behaviors while supporting scientific experts with relevant research to the extent possible. Firstly, authorities need to ensure that as many people as possible stay self-isolated at home and practice social distancing if they absolutely need to exit their homes for essential goods or other urgent needs.[13] The less contact there is among the population, the easier and faster it is for the virus to die down.[14] Secondly, for those who have tested positive for coronavirus, governments need to speedily identify individuals who could have gotten COVID-19 from the diagnosed coronavirus carriers due to recent close contact, and begin testing and quarantining those individuals accordingly.[15] Thirdly and equally importantly, leaders around the world need to prioritize protecting the most vulnerable members of society: the elderly, the homeless, the poor, and those with serious existing medical conditions; in countries with one or multiple epicenter(s) of coronavirus, those locations also merit particular attention.[16]

70% of the population infected would overwhelm hospitals and medical staff, and subsequently result in a dauntingly high number of deaths).

12. Didier Raoult et al., *Coronavirus Infections: Epidemiological, Clinical and Immunological Features and Hypotheses*, CELL STRESS 1, 5 (2020).

13. *See* Joseph A. Lewnard & Nathan C. Lo, *Scientific and Ethical Basis for Social-Distancing Interventions Against COVID-19*, 20 THE LANCET: INFECTIOUS DISEASES 631, 632 (2020) (noting evidence supporting the implementation of social distancing measures).

14. *See, e.g.*, RAMESH RASKAR ET AL., APPS GONE ROGUE: MAINTAINING PERSONAL PRIVACY IN AN EPIDEMIC, MIT WHITEPAPERS 4 (2020) ("[The] ultimate effect of R0 with a 10% use and appropriate response to data will hopefully disrupt ongoing chains of transmission, thus effecting the mortality rate and eventually impacting the contact rate and infection curve. However, high enough utilization could reduce contact rate to such a degree as to make the overall R0 < 1[,] which would ideally lead to dying off of the infection entirely.").

15. *See* Lewnard & Lo, *supra* note 13, at 631 ("In the absence of any pharmaceutical intervention, the only strategy against COVID-19 is to reduce mixing of susceptible and infectious people through early ascertainment of cases or reduction of contact.").

16. *Id.* There has also been a movement to include incarcerated populations among the most vulnerable, because prisons and jails tend to have great difficulty enforcing social distancing. *See, e.g.*, *ACLU Letter to DOJ and BOP on Coronavirus and the Criminal Justice System*, ACLU (Mar. 18, 2020), https://www.aclu.org/letter/aclu-letter-doj-and-bop-coronavirus-and-criminal-justice-system (on file with American Civil Liberties Union); *Coronavirus: Iran temporarily frees 54,000 prisoners to combat spread*, BBC (Mar. 3, 2020), https://www.bbc.com/news/world-middle-east-51723398; John Cheves, *Chief justice pleads for Kentucky inmate releases ahead of COVID-19, but progress slow*, LEXINGTON HERALD LEADER (Mar. 23, 2020), https://amp.kentucky.com/news/coronavirus/article241428266.html?__twitter_impression=true.

Among the sacrifices individuals have had to make in order for governments to accomplish these goals, a central tradeoff that citizens in various jurisdictions have experienced is one between individuals' digital privacy and public safety. At least theoretically, one may readily see ways in which taking advantage of technological advances to monitor individuals' compliance with the newly-launched Orwellian laws and policies can make the process more seamless and efficient. Significantly, while big data has proven to be "immensely useful in fields such as marketing and earth sciences," the public health space has yet to see the fruits of a big data revolution.[17] Instead of relying on recent technological advances, public health—at least up until the outbreak of the COVID-19 global pandemic—had been relying principally on traditional surveillance systems.[18] Based on various nations' digital technologies and data sharing strategies to resolve the COVID-19 crisis so far, one may find it likely that COVID-19 is driving major social change in an area that is integral to a healthy society worldwide.

As of early-April 2020, there have been three main ways of collecting and using digital data in order to accomplish the aforementioned goals.[19] First, mobile location data can provide governments with advanced tracking capabilities to help authorities enforce quarantines.[20] Second, facial recognition technology linked with biometric databases is being integrated with digital thermometers to help capture the identity of individuals with coronavirus symptoms, including, notably, a fever.[21] Third, open-source applications such as Nextstrain are using Gisaid, a platform for sharing genomic data, to help researchers

17. Lone Simonsen et al., *Infectious Disease Surveillance in the Big Data Era: Towards Faster and Locally Relevant Systems*, 214 J. INFECTIOUS DISEASES 380, 380 (2016). This paper includes an overview of the history of infectious disease surveillance, a discussion of electronic health records in the context of the big data revolution, a case study on influenza surveillance, an analysis of Google Flu Trends and other social media, and a conclusion advocating for increased use of hybrid systems combining information from traditional surveillance and big data sources, which the authors deem the most promising option moving forward. *See id.*

18. *Id.*; *see also* Alfred Ng, *Coronavirus Pandemic Changes How Your Privacy is Protected*, CNET (2020), https://www.cnet.com/news/coronavirus-pandemic-changes-how-your-privacy-is-protected/ ("At a media briefing on March 16, the WHO's director-general, Tedros Adhanom Ghebreyesus, said there needed to be more technological measures for tracking the coronavirus outbreak.").

19. *See, e.g.*, Samantha Stein, *How to Restore Data Privacy After the Coronavirus Pandemic*, WORLD ECON. FORUM (Mar. 13, 2020), https://www.weforum.org/agenda/2020/03/restore-data-privacy-after-coronavirus-pandemic/.

20. *Coronavirus: Surge in apps tracking spread and symptoms*, SKY NEWS (Mar. 3, 2020), https://news.sky.com/story/coronavirus-surge-in-apps-tracking-spread-and-symptoms-11948411.

21. Martin Pollard, *Even mask-wearers can be ID'd*, REUTERS (Mar. 9, 2020), https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL.

track and study the evolution of coronavirus.[22] This Essay focuses primarily on the first of these methods.[23] Section II of this Essay surveys the main ways in which governments have applied digital technologies and data sharing models to combat COVID-19, with case studies and a closer examination of the key stakeholders involved throughout the process. Section III of this Essay zooms in on the legal questions involved in this pandemic from a comparative digital privacy law angle. Section IV concludes this Essay on a forward-looking note, extending an open invitation for further research on this fast-evolving situation.

II. HOW BIG BROTHER USES DIGITAL DATA TO COMBAT COVID-19: A TYPOLOGY

A. Introducing Three Main Models . . . And Beyond

As of early-April 2020, there have generally been three main ways in which governments have applied digital technologies and data sharing models to achieve the aforementioned goals in putting an end to the novel coronavirus: self-quarantine enforcement, contact tracing, and flow modeling using aggregated, anonymized data.[24] Some countries use a combination of these approaches. For instance, Singapore, which has widely been considered one of the most successful nations in managing the COVID-19 crisis, uses digital data both for quarantine enforcement and contact tracing.[25]

First, multiple jurisdictions have used cellphone location data of specific users to ensure that self-quarantine rules have been properly respected by individual members of society.[26] This approach serves to enforce the aforementioned social distancing and quarantine policies.[27] The Hong Kong government, for example, used location data to track residents' movement during its lockdown period to ensure that

22. Klint Finley, *Data Sharing and Open Source Software Help Combat COVID-19*, Wired (Mar. 13, 2020), https://www.wired.com/story/data-sharing-open-source-software-combat-covid-19/.

23. I made this decision because the first way of using digital data to combat COVID-19 above has the most direct implications on individuals' digital privacy rights. Accordingly, by understanding the main models that different jurisdictions have adopted, we will be in a better position to analyze digital privacy laws and policies during the coronavirus pandemic.

24. *See* Michael Geist, *Canada Should Ensure Cellphone Tracking to Counter the Spread of Coronavirus Does Not Become the New Normal*, Globe & Mail (Mar. 22, 2020), https://www.theglobeandmail.com/business/commentary/article-canada-should-ensure-cellphone-tracking-to-counter-the-spread-of/.

25. Philip J. Heijmans, *Singapore contained Coronavirus. Could other countries learn from its approach?*, World Econ. Forum (Mar. 5, 2020), https://www.weforum.org/agenda/2020/03/singapore-response-contained-coronavirus-covid19-outbreak/.

26. *See* Geist, *supra* note 24.

27. *See supra* Section I.

everyone stayed in his or her quarantine locations if asked to be quarantined.[28] Starting on March 19, when Hong Kong ordered all arriving passengers to be quarantined for two weeks in order to prevent further spread of COVID-19, the government began mandating the use of an electronic wristband, accompanied by a smartphone app, in an effort to enforce the self-quarantine measures.[29]

In Taiwan and India, there have been similar measures where cellphone tracking is used "to warn those self-quarantining that they have travelled too far from home."[30] In Poland, the government launched "Home quarantine," a smartphone application for citizens returning from abroad who have been required to self-isolate for two weeks.[31] The app uses geolocation and facial recognition technologies: users first upload a selfie to the app, then are "randomly prompted throughout the day to submit more selfies"; the authorities will be alerted if a user does not comply with the app's selfie prompt within twenty minutes.[32] To register for the app, users need to upload personal details and a photograph, and the selfies are verified by facial recognition "and its location stamp is checked against the registered address."[33] Some Latin American countries, which were hit by the coronavirus pandemic later than many other countries, started to follow similar strategies.[34] For instance, as of April 2020, "[t]he city of Recife in northeast Brazil ha[d] been tracking 700,000 cellphones to monitor compliance with social isolation measures."[35]

Second, various countries and regions have used cellphone location data of specific users "to identify other people who may have unknowingly been placed at increased risk by coming into close

---

28. Ng, *supra* note 18.

29. Uptin Saiidi, *Hong Kong is putting electronic wristbands on arriving passengers to enforce coronavirus quarantine*, CNBC (Mar. 18, 2020), https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html. Whether there was consent from individuals is debatable. *Id.* The next section of this Essay, Section III, will discuss this matter in greater depth in considering some of the legal questions involved. We will return to this Hong Kong example as a brief case study in Section III(B)(2) of this Essay.

30. Geist, *supra* note 24.

31. Kenneth Garger, *Polish Residents Can Send Government Selfies to Prove Quarantine Compliance*, N.Y. POST (Mar. 24, 2020), https://nypost.com/2020/03/24/polish-residents-can-send-government-selfies-to-prove-quarantine-compliance/.

32. *Id.*

33. Anna Koper & Douglas Busvine, *In Europe, Tech Battle Against Coronavirus Clashes with Privacy Culture*, REUTERS (Mar. 26, 2020), https://www.reuters.com/article/us-health-coronavirus-europe-tech-poland/in-europe-tech-battle-against-coronavirus-clashes-with-privacy-culture-idUSKBN21D1CC.

34. *See, e.g.*, Yasodara Cordova & Beatriz Botero Arcila, *Latin America Hopes Big Data Can Beat the Virus. But There Are Risks*, AM. QUARTERLY (Apr. 22, 2020), https://www.americasquarterly.org/content/latin-america-hopes-big-data-can-beat-virus-there-are-risks.

35. *Id.*

proximity with someone known to have" tested positive for COVID-19.[36] This contact tracing approach helps ensure that authorities can isolate possible victims of COVID-19 transmission as quickly as possible, based on their recent close contact with confirmed COVID-19 carriers.[37]

The World Health Organization states that contact tracing occurs in three steps: contact identification, contact listing, and contact follow-up.[38] Under a traditional medical surveillance regime, this process takes a significant amount of time; however, digital contact tracing makes this process much faster and more efficient.[39]

At its simplest, digital contact tracing might work like this: Phones log their own locations; when the owner of a phone tests positive for COVID-19, a record of his/her recent movements is shared with health officials; owners of any other phones that recently came close to that phone are notified of their risk of infection and advised to self-isolate. But designers of a tracking system will have to work out key details: how to determine the proximity among phones and the health status of users, where that information is stored, who sees it, and in what format.[40]

"Israel has implemented a system that involves the collection and use of cellphone location data to identify at-risk individuals, who may receive text messages warning that they need to self-quarantine."[41] Similarly, Singapore, a country famous for its "efficiency and no-nonsense government," is well known for its "TraceTogether" app, which "exchanges Bluetooth signals between mobile phones in close proximity."[42] TraceTogether stores records of such encounters on the user's

---

36. Geist, *supra* note 24.

37. *See supra* Section I.

38. *Contact Tracing*, WORLD HEALTH ORG. (May 9, 2017), https://www.who.int/news-room/q-a-detail/contact-tracing.

39. *See* Sharon Begley, *Covid-19 spreads too fast for traditional contact tracing. New digital tools could help*, STAT (2020), https://www.statnews.com/2020/04/02/coronavirus-spreads-too-fast-for-contact-tracing-digital-tools-could-help/. One may be concerned about traditional contact tracing, not only because it typically takes three days to complete the interview process, a period during which more people could be infected, but also because many interviewees find it challenging to remember all the people with whom they may have been in physical contact within the span of 14 days—the incubation period of COVID-19. This concern was raised by Satchit Balsari during a virtual roundtable privacy and COVID-19 lecture at Harvard Law School on April 21, 2020.

40. Kelly Servick, *Cellphone tracking could help stem the spread of coronavirus. Is privacy the price?*, SCIENCE (Mar. 22, 2020), https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price.

41. *Episode 44: Michael Birnhack on Israeli Use of Cellphone Tracking to Combat the Spread of Coronavirus*, MICHAEL GEIST (Mar. 23, 2020), http://www.michaelgeist.ca/podcast/episode-44-michael-birnhack-on-israels-use-of-cellphone-tracking-to-combat-the-spread-of-coronavirus/.

42. Yasheng Huang et al., *How Digital Contact Tracing Slowed Covid-19 in East Asia*, HARV. BUS. REV. (Apr. 15, 2020), https://hbr.org/2020/04/how-digital-contact-trac-

phone, so that when the Ministry of Health interviews a user as part of the Singaporean government's contact tracing efforts, he/she can consent to send his/her TraceTogether data to government authorities.[43] This would facilitate the contact tracing procedure by speeding up the process—the sooner users take necessary actions, the earlier the detection of COVID-19 cases, and the greater reduction in the risks of the spread of coronavirus for the community at large.[44] Meanwhile, South Koreans downloaded the "Corona 100m" app over one million times within a few weeks; the app "collects data from public government sources that alert users of any diagnosed [COVID-19] patient within a 100-meter radius along with the patient's diagnosis date, nationality, age, gender, and prior locations."[45]

Third, some countries and regions have aggregated and anonymized data "to identify trends such as community outbreaks."[46] A slightly more sophisticated version of this method is termed "flow-modeling," which uses mobile phone tower data to calculate how many people pass through places, as well as how quickly.[47] For example, in Italy, one of the countries that has suffered most severely from COVID-19, there is "an aggregated and anonymous heat map for the Lombardy region . . . to better understand population movements in order to help thwart the spread of COVID-19."[48]

This approach not only serves to provide valuable information to scientific researchers, but also informs officials about the most vulnerable geographic locations and populations so that they can dedicate

---

ing-slowed-covid-19-in-east-asia; *see also* TRACETOGETHER: A SINGAPORE GOV'T AGENCY WEBSITE, *TraceTogether, Safer Together* (last visited Aug. 14, 2020), https://www.tracetogether.gov.sg (providing access to the "TraceTogether" app).

43. *TraceTogether*, MINISTRY OF HEALTH SING. (last visited Aug. 14, 2020), https://www.healthhub.sg/apps/38/tracetogether-app.

44. *Id.*

45. Huang et al., *supra* note 42.

46. *See* Geist, *supra* note 24.

47. *Countries are using apps and data networks to keep tabs on the pandemic*, ECONOMIST (Mar. 26, 2020), https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic?fbclid=IWAR3RVEv3t1XraqHzT17xBi11peT38m-TN-LsamAz_lsmKk0HhxwYWZiSg1A. This approach should be differentiated from "spying law" regimes such as those in Slovakia and South Korea involving "temporary legislation that would allow individual movements to be tracked for the duration of the pandemic." Koper & Busvine, *supra* note 33. By contrast, "a proposal by German Health Minister Jens Spahn to allow individual smartphone tracking without a judicial order was blocked by the Social Democrats (SPD)." *Id.*

48. Press Release, Vodafone launches five-point plan to help counter the impacts of the COVID-19 outbreak (Mar. 18, 2020), https://www.vodafone.com/news-and-media/vodafone-group-releases/news/vodafone-launches-five-point-plan-to-help-counter-the-impacts-of-the-covid-19-outbreak. Vodafone played an important role in this project. *See id.* The role of private sector actors is discussed in greater detail in the subsection below.

additional resources and adjust their priorities accordingly.[49] As a team of leading scholars in fields as diverse as communicable diseases, quantitative social science, and privacy law opined, "the estimates of aggregate flows of people are incredibly valuable."[50] In their article titled "Aggregated Mobility Data Could Help Fight COVID-19," Professor Caroline O. Buckee and her co-authors shared that a map that examines the impact of social distancing messaging or policies on population mobility patterns "will help county officials understand what kinds of messaging or policies are most effective."[51] According to this research team:

> [c]omparing the public response to interventions, in terms of the rate of movement over an entire county from one day to the next, measured against a baseline from normal times, can provide insight into the degree to which recommendations on social distancing are being followed. We will need these estimates, not only now but also when we need to resume life again without risking a major resurgence.[52]

In addition to these three predominant models, researchers and journalists have identified a few other approaches to using digital data and technologies to combat COVID-19 that they have observed or are predicting to emerge in the coming weeks or months. For instance, *The Economist* identified "social-graph making" as an additional possible application of data tools for the COVID-19 pandemic, but states that nowhere is known to have already implemented this tool.[53] By mapping out which data subjects tend to meet repeatedly based on mobile phone tower data and machine learning, this approach could be an effective tool that unfortunately poses high risk of civil liberties infringements.[54]

Although these three strategies appear to be structurally straightforward in that all three methods are ways for governments to regulate individual citizens, in reality, there are often other stakeholders involved as intermediaries in this process.

---

49. *See supra* Section I.

50. Caroline O. Buckee et al., *Aggregated mobility data could help fight COVID-19*, SCIENCE (Apr. 10, 2020), https://science.sciencemag.org/content/368/6487/145.2. *But see* Scott Berinato, *There's No Such Thing as Anonymous Data*, HARV. BUS. REV. (Feb. 9, 2015), https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data (arguing that there is no such thing as "anonymous data").

51. Buckee, *supra* note 50.

52. *Id.*

53. *Countries are Using Apps and Data Networks to Keep Tabs on the Pandemic*, *supra* note 47.

54. *See id.* (explaining the breadth of information contact tracing apps can collect).

B. The Picture at Large: Big Brother's Helpers and Those Voluntarily Succumbing to His Watch

Because government administrations are not always the most technology-savvy and resource-abundant institutions, technology and telecommunications companies such as Apple, Google, and Vodafone,[55] which possess the relevant experience, expertise, and manpower to quickly invent new public health products, are naturally suitable candidates for transforming ambitious ideas and grandiose theories into reality.

Granted, one may question the incentives for those corporate powerhouses to cooperate with governments, such as prioritizing reputation-building from corporate social responsibility and profit maximization; however, if one were to take a more skeptical lens, one can note further complexities in the privacy-public health tradeoff, because each of the stakeholders has a unique incentive. Governments, especially authoritarian ones, value legitimacy. One way a government shows its legitimacy is through its performance maintaining the welfare and stability of society.[56] The speed at which a country extinguishes the threat of COVID-19 for its constituents can showcase to other states the effectiveness of its leadership and the country's overall strength. On the bright side, the race to kill COVID-19, if only partially driven by this incentive, is beneficial to the world at large, as one country's public health crisis can easily become another country's nightmare due to mobility under the backdrop of globalization. On the other hand, these incentives have also led to attempts to, and accusations of, fabricating data, which creates a vicious cycle of more accusations and hindrances of correctly analyzing the science behind COVID-19.[57]

Meanwhile, individual members of society, who are perhaps the largest group of stakeholders in this global pandemic, most value freedom, coupled with the safety and health of themselves and their loved

---

55. *See, e.g.*, Ina Fried, *Apple, Google team up on coronavirus contact tracing,* Axios (Apr. 10, 2020), https://www.axios.com/apple-google-team-up-on-coronavirus-contact-tracing-6579b80f-f348-4c8e-ac87-d823b9abb4fb.html; *see also* Press Release, *supra* note 48; *see generally* Chris Nuttall, *Tracking Covid-19 Through Your Phone*, Fin. Times (2020), https://www.ft.com/content/5f49f7c4-9b1e-49bc-99d1-8a0d176a9bce.

56. *See* Christian von Soest & Julia Grauvogel, *Identity, Procedures and Performance: How Authoritarian Regimes Legitimize Their Rule*, 3 J. Contemp. Pol. 287, 291 (2017) (discussing six claims to legitimacy, one of which is "performance").

57. *See, e.g.*, Dion Rabouin, *China's V-shaped coronavirus recovery looks too good to be true*, Axios (Mar. 31, 2020), https://www.axios.com/china-coronavirus-economic-recovery-doubts-0e32c3c1-3759-495f-a757-ef8ced031254.html; Kunal Purohit, *Misinformation, Fake News Spark India Coronavirus Fears*, Aljazeera (Mar. 10, 2020), https://www.aljazeera.com/news/2020/03/misinformation-fake-news-spark-india-coronavirus-fears-200309051731540.html.

ones over that of strangers. This explains why many young people chose to continue partying at Florida beaches over spring break despite nationwide social distancing policies that had already been in place in early-to-mid March: they believed themselves to be safe from the fatality of coronavirus due to their youth.[58] Such actions have ironically resulted in further worsening of the spread of the virus: an attempt at gaining freedom in turn resulted in tighter restrictions in one's digital privacy and overall civil liberties.

Despite all these cynicisms that one may have about each stakeholder's incentives and motivations, there have been at least some *positive* mechanisms in which private individuals and technology corporations alike have contributed to governments' realization of their public health and safety goals. Although the three aforementioned methods in which governments use digital technologies and data to combat COVID-19 in this Section may appear to be top-down, there have been concurrent bottom-up efforts, including grassroots movements from individuals, academia,[59] and corporate entities alike.

We can observe a number of cases in which grassroots movements have helped governments monitor the population and ensure that individuals are self-quarantining and social-distancing properly. For instance, there have been a number of Hackathons that specifically focused on tackling issues related to the COVID-19 pandemic.[60] Pre-coronavirus, Hackathons had been "made popular decades ago by the software community as communal, all-night sessions, often powered by pizza and various caffeinated beverages";[61] under the coronavirus backdrop, nothing quite stops the enthusiasm of coders from directing their energy and talent to collectively brainstorm constructive solutions to the pandemic. True to the technology theme, everything is accomplished via online platforms such as Zoom.[62] Among the ideas that emerged in those Hackathons and similar grassroots movements

58. Christopher Brito, *Spring Breakers Say Coronavirus Pandemic Won't Stop Them From Partying*, CBS NEWS (Mar. 25, 2020), https://www.cbsnews.com/news/spring-break-party-coronavirus-pandemic-miami-beaches/.

59. For example, the COVID-19 Mobility Data Network is "a network of infectious disease epidemiologists at universities around the world working with technology companies to use aggregated mobility data to support the COVID-19 response." COVID-19 MOBILITY DATA NETWORK, https://www.covid19mobility.org (last visited Aug. 14, 2020). Its "goal is to provide daily updates to decision-makers at the state and local levels on how well social distancing interventions are working, using anonymized, aggregated data sets from mobile devices, along with analytic support for interpretation." *Id.*

60. *See, e.g.*, Agam Shah, *Hackathons Target Coronavirus*, WALL ST. J. (Apr. 9, 2020), https://www.wsj.com/articles/hackathons-target-coronavirus-11586424603; *Our Story*, CORONAVIRUS HACKATHON, https://hackathon.common.vc/ourstory (last visited Aug. 14, 2020).

61. Shah, *supra* note 60.

62. *Id.*

was "a location-based mobile application to track traffic in grocery stores for effective social-distancing practices."[63]

The actions and behaviors of individual members of society are critical to a speedy return to pre-COVID-19 normalcy because their cooperation is essential to the implementation of government social distancing and quarantine policies. For consent-based approaches such as the German GeoHealth app[64] and Massachusetts Institute of Technology's Private Kit: Safe Paths app,[65] individuals have effectively become Big Brother's willing subjects by providing consent and volunteering to donate data to the apps, although the extent of voluntariness and consent is contentious.[66] After all, "paradoxically, privacy is a public value" that "begins with personal choices about what individuals share, and with whom."[67] As Harvard Law School profes-

63. *Id.*; *see also* Koper & Busvine, *supra* note 33.

64. Servick, *supra* note 40. For GeoHealth, "that data would then be anonymized and stored on a central server." *Id.* "A data analytics platform designed by the software company Ubilabs would compare users' movement history to that of infected people, and the GeoHealth app would show them color-coded alerts based on how recently they may have encountered the virus." *Id.* Through "a combination of GPS tracking, wireless network data, and connections between phones via Bluetooth," the GeoHealth app can "detect when a phone comes within 1 meter of another phone." *Id.*

65. *Id.* (describing how a person who tests positive for COVID-19 could use the app to "donate" or share his or her location history). With regards to MIT's Private Kit: Safe Paths, the app was developed as a team project among MIT, Facebook, Mayo Clinic, and other organizations. Casey Ross, *After 9/11, we gave up privacy for security. Will we make the same trade-off after Covid-19?*, STAT (Apr. 8, 2020), https://www.statnews.com/2020/04/08/coronavirus-will-we-give-up-privacy-for-security/. MIT's app "collects information using a technique known as differential privacy, a way of publicly sharing information gleaned from a data set without identifying the individuals whose activities are represented." *Id.* The MIT app constitutes an example of "human-centered tech," as well as perhaps an illustration of "privacy by design." Margaret Bourdeaux et al., *How human-centered tech can beat COVID-19 through contact tracing*, THE HILL (Apr. 21, 2020), https://thehill.com/opinion/technology/493648-how-human-centered-technology-can-beat-covid-19-through-contact-tracing; Lee A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, 4 OSLO L. REV. 106 (2017).

66. *See, e.g.*, Saiidi, *supra* note 29. One reason why one may argue that some of the perceived voluntariness is not purely voluntary may be attributed to the immense level of shame that some COVID-19 carriers have experienced. According to Lee Su-young, a psychiatrist at Myongji Hospital in South Korea, some coronavirus "[patients] were more afraid of being blamed than dying of the virus." RASKAR ET AL., *supra* note 14, at 2 (alteration in original). Under such circumstances, it is natural that those who test positive for COVID-19 may "volunteer" to report this information as soon as possible, so that by acting as responsible citizens, they may be blamed to a lesser extent if they infect others in the community. *But see* Doug Fraser, *Experts: Coronavirus Pandemic Tests Limits of Privacy Laws*, GOV'T. TECH. (Mar. 24, 2020), https://www.govtech.com/health/Experts-Coronavirus-Pandemic-Tests-Limits-of-Privacy-Laws.html ("Part of the privacy concern is that people could face discrimination, isolation, even retribution if their identity were revealed. . . . [I]t makes it less likely that those who are infected or suspect they are will come forward for testing.").

67. Laurence H. Tribe, *Digital coronavirus data tracing would barter away American liberties: Laurence Tribe*, USA TODAY (Apr. 21, 2020), https://www.usatoday.com/

sor Laurence H. Tribe stated, "the cumulative impact of those judgments far exceeds the sum of their parts."[68]

III. ZOOMING IN ON DIGITAL PRIVACY LAW IN THE TIME OF CORONAVIRUS

Digital privacy law is a constantly-evolving field. The different ways in which Big Brother surveils the masses in an effort to guard them against COVID-19 raises a myriad of legal questions. While current laws generally allow for a public health crisis/emergency exception to otherwise-stricter digital privacy laws, there are still multiple valid legal concerns, including consent, expiration,[69] transparency, and Due Process.[70] Additionally, "[p]rivacy intrusions should be necessary and proportionate," while data collection should be based on science instead of bias.[71] This Section starts with a brief overview of some key laws that govern digital privacy in the public health context in Europe and the United States that have substantial ramifications in other regions, and then analyzes each of the dominant digital surveillance methods identified in Section II of this Essay: (1) modeling using aggregated data and (2) location tracking using cellphone location data, which includes quarantine enforcement and contact tracing.[72]

A. An Overview of the Legal Landscape Relevant to the COVID-19 Context

1. The European Approach to Digital Privacy Governance

The global governance of digital privacy has, until quite recently, been a "near anarchy."[73] However, Europe's General Data Protection

story/opinion/todaysdebate/2020/04/21/coronavirus-data-tracing-barter-away-liberties-laurence-tribe-editorials-debates/3000576001/.

68. *Id.*

69. Under the General Data Protection Regulation ("GDPR"), consent to processing sensitive personal data should be freely given, and there are far-ranging constraints on its use; i.e., data collected over the course of COVID-19 should not be stored indefinitely or used for another purpose. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1.

70. *Accord* Effy Vayena, Comparative Digital Privacy and COVID-19, Presentation at Harvard Law School (Mar. 24, 2020).

71. *Id.*

72. As the field of digital privacy law is greatly complex and involves significant differences across nations, this Essay does not attempt to be comprehensive in its analysis, but instead focuses on the dominant models in Europe and the United States. Due to the two regions' prominent role and leadership in the global economy, I believe this approach is justified. *See, e.g.*, Cordova & Botero Arcila, *supra* note 34 (Latin American countries, such as Mexico, Colombia, and Brazil, have followed European countries' models in terms of digital privacy laws to a great extent).

73. Brian Yost, Note, *Enforcing Digital Privacy*, 33 Harv. J. Law Tech. 311, 311 (2019).

Regulation ("GDPR"), which took effect in May 2018, terminated the previous piecemeal approach, extending European Union jurisdiction far beyond European Union countries.[74]

As a general matter, under Articles 7 ("[r]espect for private and family life") and 8 ("[p]rotection of personal data") of the Charter of Fundamental Rights of the European Union ("CFR"), "personal data must be processed on the basis of 'consent.'"[75] The GDPR offers further specificity, requiring explicit and informed consent to the processing of personal health data.[76]

More specifically, in the fight against the coronavirus pandemic, Andrea Jelinek, who serves as Chair of the European Data Protection Board ("EDPB"), opined that whilst data protection rules such as the GDPR "do not hinder measures taken," "even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects."[77] The EDPB elaborated in a press release that:

> The *GDPR is a broad legislation* and also provides for the rules to apply to the processing of personal data in *a context such as the one relating to COVID-19*. Indeed, the GDPR provides for the legal grounds to enable the employers and the competent public health authorities to process personal data in the context of epidemics, *without the need to obtain the consent of the data subject*. This applies[,] for instance[,] when the processing of personal data is necessary for the employers for reasons of *public interest in the area of public health or to protect vital interests* ([*Articles*] *6 and 9* of the GDPR) or to comply with another legal obligation.
>
> For the processing of *electronic communication data*, *such as mobile location data*, *additional rules apply*. The national laws implementing the ePrivacy Directive provide for the principle that the location data can only be used by the

74. Pam Greenberg, *A Higher Profile for Data Privacy*, 27 LEGISBRIEF 1, 1 (2019) ("Any global business that sells to or has European Union customers is subject to the GDPR, regardless of where that business is based. The GDPR sets forth rules about how companies treat the personal data of EU citizens, even those purchasing U.S. products or services or living in the U.S.").

75. The European Parliament Council and the Commission, *Charter of Fundamental Rights of the European Union*, 2000 O.J. (C 364) 1 (EC), https://www.europarl.europa.eu/charter/pdf/text_en.pdf; Hannah van Kolfschooten, *EU Coordination of Serious Cross-Border Threats to Health: The Implications for Protection of Informed Consent in National Pandemic Policies*, 10 EUROPEAN J. RISK REG. 635, 639-40 (2019).

76. Council Regulation 2016/679, 2016 O.J. (L 119) 1.

77. European Data Protection Board Press Release, Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak (Mar. 16, 2020), https://edpb.europa.eu/sites/edpb/files/files/news/edpb_covid-19_20200316_press_statement_en.pdf.

> operator when they are made *anonymous*, or with the *consent* of the individuals.[78]

During the 2013-2016 outbreak of Ebola, the European Union had introduced several countermeasures against the epidemic, including recommendations on "contact listing, contact tracing, and monitoring of possibly exposed persons."[79] However, at the E.U. level, law and policy do not contain specific safeguards on ways "to properly balance the protection of individual fundamental rights[,] such as the right to informed consent with the protection of public health."[80]

2. The United States Approach to Digital Privacy Governance

In the United States, there is an absence of a federal privacy law, which, according to Omer Tene, who serves as vice president of the International Association of Privacy Professionals, creates "great uncertainty and disarray around the scope of and guardrails around legitimate uses of personal information."[81]

A notable law that was recently passed is California's Consumer Privacy Act ("CCPA"), which "would constitute one of the broadest online privacy regulations in the U.S., affecting businesses across the country."[82] Similar to that of "the GDPR, the CCPA's impact is expected to be global, given California's status as the fifth largest global economy."[83] As an overview, the CCPA:

> [i.] Allows consumers the right to request a business to disclose the categories and specific pieces of personal informa-

78. *Id.* (emphases added). More specifically, data processing in the context of adopting necessary measures to combat COVID-19 and limit its speed has different legal bases under the GDPR. These include Article 6(1)(c), (d) and (e), pursuant to which the processing is necessary i) "for compliance with a legal obligation to which the controller is subject"; ii) "to protect the vital interests of the data subject or of another natural person"; or iii) "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." Further, public authorities may process sensitive personal data based on Article 9(2)(b), (e), (h) and (i), where the data processing is either necessary i) for the purposes of carrying out obligations derived from "employment and social security and social protection law"; ii) "for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee"; iii) "for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health"; or iv) where the processing relates to personal data which is "manifestly made public by the data subject." Council Regulation 2016/679, 2016 O.J. (L 119) 1.

79. van Kolfschooten, *supra* note 75, at 642; *see also The EU's response to the Ebola outbreak in West Africa*, EUROPEAN COMM'N (Oct. 27, 2014), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_599.

80. van Kolfschooten, *supra* note 75, at 643.

81. Ng, *supra* note 18.

82. Greenberg, *supra* note 74.

83. Alice Marini et al., *Comparing Privacy Laws: GDPR v. CCPA*, DATA GUIDANCE & FUTURE OF PRIVACY FORUM, Dec. 2019, at 1, 5.

> tion that have been collected about them, as well as the source of that information and the purpose for collecting it.
> [ii.] Gives consumers the right to request a business' sale[84] of their personal information without being discriminated against for opting out.
> [iii.] Allows consumers to ask businesses to delete personal information that has been collected from them.
> [iv.] Provides for enforcement by the state attorney general and for a private right of action in certain cases of unauthorized access, theft[,] or disclosure of a consumer's personal information.[85]

The CCPA, like the GDPR, defines "personal information" and "personal data" broadly.[86] Under the CCPA, any information that is "reasonably capable of being associated with, or could reasonably be linked with" an individual device or household constitutes "personal information," and this definition specifically includes "geolocation data."[87]

Unlike the GDPR, which "does not exclude specific categories of personal data from its scope of application," "[t]he CCPA specifically excludes from its scope of application collecting and sharing of [certain] categories of personal information," including, notably for our

---

84. The CCPA imposes notice and opt-out requirements on entities that "sell" personal information, where the word "sell" is defined to include disseminating, disclosing, or otherwise "making available" personal information to for-profit third parties in exchange for "monetary or other valuable consideration." Aaron Burstein & Alysa Zeltzer Hutnik, *Data Privacy Considerations for Coronavirus Data Tools*, AD LAW ACCESS (Mar. 28, 2020), https://www.adlawaccess.com/2020/03/articles/data-privacy-considerations-for-coronavirus-data-tools/. While not a "sale," sharing personal information with a government authority "would qualify as a disclosure under CCPA and would need to be accurately disclosed in the privacy policy." *Id.*

85. *Id.* (internal citation added); *see also* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100-1798.198 (West 2018). *But see* George P. Slefo, *Coronavirus may delay enforcement of California's consumer privacy law*, ADAGE (Mar. 19, 2020), https://adage.com/article/digital/coronavirus-may-delay-enforcement-californias-consumer-privacy-law/2245291 ("Multiple trade bodies sent the California attorney general a letter on Thursday asking the Golden State to push back its enforcement of the Consumer Privacy Protection Act from July of this year to January 2021.").

86. Burstein & Zeltzer Hutnik, *supra* note 84.

87. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(b)(o) (2018). This is similar to the GDPR, where:

> personal data is defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Marini et al., *supra* note 83, at 13 (quoting GDPR Articles 4(1), 9, Recitals 26-30). "The GDPR also explains in its recitals that in order to determine whether a person is identifiable, 'account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person' to identify the individual directly or indirectly." *Id.*

purposes, "medical information and protected health information."[88] Instead, one's "medical information and protected health information [ ] are covered by the Confidentiality of Medical Information Act and the Health Insurance Portability and Accountability Act" ("HIPAA").[89]

The HIPAA—the United States' primary health privacy law—punishes any covered entity that knowingly discloses another person's "individually identifiable health information."[90] The language of the HIPAA is sufficiently broad to permit disclosures if one acts "reasonably and in good faith that the disclosure is necessary and to someone who could reasonably lessen the threat."[91] Specific to the public health crisis context, the HIPAA includes language that allows "federal officials to waive privacy rules"; "officials have already exercised those provisions to allow for greater sharing of patient medical records for public health purposes and to support increased access to telemedicine services."[92] However, as this law was passed in 1996, "when health data were primarily in the hands of hospitals, physician offices, and insurance companies—before Apple, Facebook, Amazon, and Google became so pervasive in American life," it is arguably outdated to a certain degree.[93] This may pose "threats to privacy and individual freedoms that lawmakers could not have contemplated at the time."[94]

B. Applying Privacy-Related Legal Concerns to Big Brother's Digital Surveillance Strategies

1. Flow Modeling Using Aggregated, Anonymized Data

Among the predominant ways in which Big Brother has used digital technologies and data to surveil his subjects, the use of aggregated and anonymized data is the least controversial vis-à-vis concerns raised by digital privacy law. As the EDPB shared in its press release statement, "public authorities should first aim for the processing of location data in an anonymous way (i.e., processing data aggregated in a way that it cannot be reversed to personal data)" "to generate

88. Marini et al., *supra* note 83, at 11.

89. *Id.*

90. Ross, *supra* note 65; *see also* 42 U.S.C. § 1320d-6 (2012).

91. Fraser, *supra* note 66.

92. Ross, *supra* note 65.

93. *Id.*; *supra* Section I (discussing possible social changes in the COVID-19 outbreak context, where we are seeing a shift from traditional medical surveillance regimes to one that is driven by the big data revolution).

94. Ross, *supra* note 65.

reports on the concentration of mobile devices at a certain location ('cartography')."[95]

Buckee and her co-authors have advocated against the use of individual data and instead recommend the use of aggregated and anonymized data, believing that there have already been successful precedents in Asia and Europe where governments have managed to juggle the privacy-public health trade-off in aggregating COVID-19 data.[96] Deutsche Telekom, for example, "has shared aggregated data with Germany to help measure social distancing, in compliance with EU laws."[97] According to Buckee and her co-authors, "[t]he more such analyses are initiated and concluded openly, and in accordance with the law, the greater will be the public trust and our ability to produce reliable analytic insights."[98]

However, one still has reasons to remain cautious. As the Electronic Frontier Foundation ("EFF") has warned, "there's a difference between 'aggregated' location data and 'anonymized' or 'deidentified' location data."[99] Information about a person's location is often sufficient by itself to re-identify individual location data, for "[s]omeone who travels frequently between a given office building and a single family home is probably unique in those habits and therefore identifiable from other readily identifiable sources."[100] Indeed, study shows that researchers could uniquely characterize fifty percent of the population using only two randomly selected time and location data points.[101] Despite this, the EFF has also found aggregation to preserve individual privacy to be potentially useful, while it still considers consent to play an important role despite the anonymous and aggregated form of data collection method.[102]

---

95. European Data Protection Board Press Release, *supra* note 77.

96. Buckee et al., *supra* note 50; *see, e.g.*, Shengjie Lai et al., *Assessing spread risk of Wuhan novel coronavirus within and beyond China, January-April 2020: a travel network-based modelling study*, MEDRXIV: THE PREPRINT SERVER FOR HEALTH SCIENCES (Mar. 9, 2020), https://www.medrxiv.org/content/10.1101/2020.02.04.20020479v2.full.pdftml; Elvira Pollina & Douglas Busvine, *European mobile operators share data for coronavirus fight*, REUTERS (Mar. 18, 2020), https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2.

97. Buckee et al., *supra* note 50.

98. *Id.*

99. Jacob Hoffman-Andrews & Andrew Crocker, *How to Protect Privacy When Aggregating Location Data to Fight COVID-19*, ELECTRONIC FRONTIER FOUND. (Apr. 6, 2020), https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19.

100. *Id.*

101. Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The privacy bounds of human mobility*, SCI. REPORTS (Mar. 25, 2013), https://www.nature.com/articles/srep01376.

102. *See* Hoffman-Andrews & Croker, *supra* note 99.

Overall, this data aggregation method, based on our analysis of the GDPR in Section III(A)(1), is generally compliant with European privacy laws. Meanwhile, in the U.S., the CCPA, HIPAA, and other privacy laws also offer "examples of what safeguards are expected to reasonably treat data as anonymized, and employing such standards can help avoid unnecessary privacy mishaps despite well-intentioned efforts."[103] These specificities will hopefully alleviate some of the EFF's concerns. In any case, moving forward, different authorities should, as best practice, keep in mind the relevant consent-based considerations even in the context of aggregated data.

2. The Cellphone Tracking Methods: Quarantine Enforcement and Contact Tracing[104]

Cellphone tracking methods, including quarantine enforcement and contact tracing, are more worrying with regards to privacy concerns. If flow modeling using aggregated data poses low civil liberties risk, quarantine enforcement would rate as "medium" and contact tracing would rate as "high" in terms of the level of risk these methods pose to cellphone users' civil liberties and privacy rights.[105] Although at a glance, the unprecedented crisis caused by the COVID-19 outbreak around the world appears to easily qualify under the exemptions of both the GDPR and HIPAA, as well as similar laws from other regions,[106] in the absence of anonymity,[107] many legal challenges remain, including issues of consent, expiration/deletion, transparency, proportionality, and necessity.[108]

Per Article 15 of Europe's ePrivacy Directive, when it is not plausible to solely process anonymous data, member states may introduce "legislative measures pursuing national security and public secur-

103. Burstein & Zeltzer Hutnik, *supra* note 84.

104. Because of the nature of my legal analysis, I find it easier to group quarantine enforcement and contact tracing in the same sub-sub-section because laws tend to focus on the similarities between them as both are based on cellphone location data tracking.

105. *Countries are Using Apps and Data Networks to Keep Tabs on the Pandemic*, *supra* note 47.

106. *See, e.g.*, Cordova & Botero Arcila, *supra* note 34.

107. Granted, some contact tracing apps under the category of "human-centered tech" arguably does preserve anonymity through putting to practice "privacy by design" principles. *See* Ross, *supra* note 66; Bourdeaux et al., *supra* note 65. However, as much of that type of technology is still a work in progress, this Essay focuses more on the already-widely adopted methods that governments have used.

108. *See supra* Section III(A). This Essay will not address expiration/deletion issues in detail, because as we are still very much in the middle of the pandemic, there has been relatively scarce focus on this longer-term issue, although some apps, including TraceTogether and MIT's app, pride themselves in forward-looking considerations such as the erasure of data after the end of COVID-19. *See, e.g.*, *TraceTogether Privacy Safeguards*, GOV'T OF SING. (last updated June 1, 2020), https://www.tracetogether.gov.sg/common/privacystatement; RASKAR ET AL., *supra* note 14, at 12.

ity."[109] This emergency legislation, however, comes with the caveat that those measures must constitute "a necessary, appropriate, and proportionate measure within a democratic society."[110] Germany, which has some of Europe's most stringent data privacy protections, allows the government to "compel a technology company to share location data on an individual in the interest of national security."[111] However, according to Sebastian Golla, a data protection law scholar at the Johannes Gutenberg University of Mainz, "indiscriminate mass tracking of individuals lacks a legal basis" under German laws: to track cell-phone users who have or might carry "coronavirus, Germany and other European countries would need to pass laws specifying how data collection would be restricted to a certain population, for a certain time, and for a certain purpose."[112]

Further reflecting on the general legal principles of proportionality, necessity, and appropriateness in the COVID-19 context, a number of experts have voiced skepticism regarding the effectiveness of location tracking altogether. Some advise policymakers to exercise caution with these tools, partially because "locational data is not very accurate," as "it can convey that two people a few meters apart crossed paths, but it won't distinguish if they were on the same bus or in two separate cars at a stoplight."[113] Ross Anderson, a professor of security engineering at the computer laboratory at the University of Cambridge, has also raised at least seven concerns about contact tracing, calling into question the extent to which it is as privacy-complying as others may consider it to be.[114] These critiques include this technique's lack of anonymity, the authorities' access to other types of data such as public transport ticketing and credit-card records,[115] the vulnerability of such smartphone apps to trolling or other bad-inten-

109. European Data Protection Board Press Release, *supra* note 77.

110. *Id.*

111. Servick, *supra* note 40.

112. *Id.* In reality, some laws satisfying these criteria are in the making: for instance, in late March, the German Health Ministry had drafted changes to the Infection Protection Act to allow the tracking of individuals who were in contact with those infected with the novel coronavirus. *Id.*; *see also COVID-19: The German Infectious Diseases Protection Act – What Makes You Stay at Home*, GIBSON DUNN (Mar. 20, 2020), https://www.gibsondunn.com/covid-19-german-infectious-diseases-protection-act-what-makes-you-stay-at-home/.

113. Cordova & Botero Arcila, *supra* note 34.

114. Ross Anderson, *Contact Tracing in the Real World*, LIGHT BLUE TOUCHPAPER: SECURITY RSCH., COMPUTER LAB., UNIV. OF CAMBRIDGE (Apr. 12, 2020), https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/.

115. According to Anderson, this accounts for how "a contact tracer in Singapore is able to phone you and tell you that the taxi driver who took you yesterday from Orchard Road to Raffles has reported sick, so please put on a mask right now and go straight home." *Id.*

tioned acts from hackers,[116] and the outdated nature of some of the technologies involved due to the fact that some of the Internet infrastructure from thirty years ago are difficult to update.[117] Given the relative ease at which such technologies can be exploited to "expand mass surveillance, limit individual freedoms and expose the most private details about individuals,"[118] skepticisms and criticisms such as these are valid in casting doubt on the proportionality, necessity, and appropriateness of quarantine enforcement and contact tracing using cellphone tracking technologies.

Partially, the answer would depend on the type of data that is collected from these approaches. Under the GDPR, data can be either related to the health of the data subject or not; the former would be a special category of personal data subject to stricter regulation.[119] While personal data such as one's travel history to a country with a high rate of COVID-19 cases or data that one's relatives or colleagues have been infected by COVID-19 would not constitute this special category of data, whether the data subject has recently received healthcare services does fall within this special category of personal data.[120]

In terms of legal concerns about consent and transparency, we may return to the Hong Kong quarantine enforcement example.[121] Despite that authorities claimed to have obtained consent from individuals under quarantine before tracing them,[122] in practice, it is "un-

116. *See* RASKAR ET AL., *supra* note 14, at 9 ("In South Korea, fraudsters quickly began blackmailing local merchants and demanding ransoms to not (falsely) report themselves as sick and having visited the business. Additionally, bad actors may force individuals to provide their location data for purposes other than disease containment, such as for immigration or police purposes."). Indeed, there are many forms of fraud involved with these digital technologies that skilled fraudsters can exploit. Unfortunately, bad actors can be quite creative.

117. Anderson, *supra* note 114.

118. RASKAR ET AL., *supra* note 14, at 2.

119. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1.

120. Dan Cooper & Spyridon Goulielmos, *Greek Data Protection Authority Issues Guidelines on Data Protection and Coronavirus*, INSIDE PRIVACY (Mar. 30, 2020), https://www.insideprivacy.com/covid-19/greek-data-protection-authority-issues-guidelines-on-data-protection-and-coronavirus/. Cooper and Goulielmos's article uses Greece as an illustration:

> Pursuant to Article 2(1) of the GDPR and Article 2 of Law 4624/2019" of Greece (which implemented the GDPR), "the legal framework for the processing of personal data applies solely in cases where personal data is processed wholly or partly by automated means or where it otherwise forms part of a filing system or is intended to form part of a filing system. As a result, although information provided orally concerning – for example – whether a data subject has been infected by COVID-19 or whether one's body temperature is higher than normal does not fall within the scope of the GDPR, where [sic] it not recorded.

Id.

121. *Supra* Section II(A).

122. *See, e.g.*, *Privacy Commissioner Responds to Privacy Issues Arising from Mandatory Quarantine Measures*, PRIVACY COMM'R FOR PERSONAL DATA, HONG KONG,

clear *how* that consent was obtained."[123] For instance, passenger Declan Chan, whom Saiidi interviewed, "filled out a form which suggested passengers had the option of sharing their location with the government via messaging platforms, like WeChat and WhatsApp, or by agreeing to wearing an electronic wristband."[124] However, Chan "soon learned the messaging apps were not an option and all passengers must wear the wristbands."[125] In other apps, it is also difficult to obtain "real" consent, because signing up to these apps often involves reading and consenting to "incomprehensible" language that a non-lawyer can find daunting, and consider to be a "lack of real choice."[126]

Even if consent was truly obtained to everyone's satisfaction, still, others question the sufficiency of consent. Cordova and Botero Arcila, for instance, commented that "consent is an insufficient protection mechanism" because "[o]nce a citizen gives consent," it would be challenging "for individuals to exercise control about how their information is being used."[127]

All in all, despite the surface-level legal compliance of cellphone location tracking techniques in quarantine enforcement and contact tracing, a more nuanced legal analysis finds that existing strategies may not hold up to closer examinations. The hope would be that "citizen-centric, privacy-first solutions" that are "open source, secure, and decentralized," such as MIT's Private Kit: Safe Paths, will truly "represent the next generation of tools for disease containment in an epidemic or a pandemic," as they claim themselves to be.[128]

(Feb. 12, 2020), https://www.pcpd.org.hk/english/media/media_statements/press_20200211.html. Among other key points, the Commissioner highlights that the collection of location data of persons under quarantine is "for a lawful purpose . . . . for the interest of the persons under quarantine and the general public" alike. *Id.* Regarding consent, the Commissioner underscores that:

> [b]efore the quarantine measures were implemented, the authority has obtained *consent* from the persons under quarantine *in accordance with the law* for access to their relevant personal data, including the situation of the quarantine premises, and for the usage of commonly-used mobile applications and imaging equipment. *These functions can only be activated by the persons under quarantine*, who have a *free choice* as to [under] what circumstances these functions would be activated, and whether the requisite information would be provided via other means.

Id. (emphases added). However, the government did not specify *how* consent was obtained.

123. Ng, *supra* note 18 (emphasis added).

124. Saiidi, *supra* note 29.

125. *Id.*

126. RASKAR ET AL., *supra* note 14, at 8.

127. Cordova & Botero Arcila, *supra* note 34.

128. RASKAR ET AL., *supra* note 14, at 3. It is at least reassuring that designers of these newer apps have had the legal principles in mind from the very get-go—a good illustration of "privacy by design." *See* Ross, *supra* note 65.

IV. COUNTERING THE NOVEL CORONAVIRUS, AND BEYOND: SYNTHESIS AND LOOKING AHEAD

As Winston Churchill once said, "never waste a good crisis."[129] The novel coronavirus appears to have forcefully put an originally vibrant, inter-connected world on halt. It is hardly imaginable that merely months ago, one could easily fly anywhere for business or leisure, and now, countries around the world are beginning to see lockdowns as a new normal of sorts. As we unwillingly confront ourselves with what promises to be an unprecedented global economic crisis that would likely rival the Great Depression,[130] times of crises and uncertainty such as the one we live in at the moment calls for optimism and introspection. This includes thoughtful research and reform on current laws and policies, including the ever-evolving field of digital privacy law. Only through such reflections can society move forward and prepare for any future crises that pose new challenges to the human race, especially as technology becomes an ever-more-omnipotent force that we could harness to counter new challenges.

As of April 2020, in response to the outbreak of COVID-19, twenty-three countries have used contact tracing apps and twenty-two countries have actively used alternative digital tracking measures.[131] As Section II shows, Big Brothers from different jurisdictions have used digital technology and data at an unprecedented scale. This demonstrates the way society has moved past traditional medical surveillance to digital-based surveillance featuring public and private sector players alike.[132] While different digital privacy laws have been overall generous in terms of their public health crisis exceptions, such

129. Andrew Low, *Telling the truth about SME life today*, REAL BUS. (Feb. 25, 2016), https://realbusiness.co.uk/as-said-by-winston-churchill-never-waste-a-good-crisis/. *But see* Jerry Bellune, *NEVER LET A CRISIS GO TO WASTE*, LEXINGTON CTY. CHRONICLE (Mar. 26, 2020), https://www.lexingtonchronicle.com/business/never-let-crisis-go-waste (attributing a similar version of the quote to Rahm Emanuel); Fred Shapiro, *Quotes Uncovered: Who Said No Crisis Should Go to Waste?*, FREAKONOMICS (2009), https://freakonomics.com/2009/08/13/quotes-uncovered-who-said-no-crisis-should-go-to-waste/ (noting the expression has been used in the context of medical emergencies by M.F. Weiner).

130. *See, e.g.*, Natalie Huet & Sasha Vakulina, *IMF: Coronavirus pandemic will cause worst economic slump since Great Depression*, EURONEWS (Apr. 3, 2020), https://www.euronews.com/2020/04/09/imf-coronavirus-pandemic-will-cause-worst-economic-slump-since-great-depression; Peter S. Goodman, *Why the Global Recession Could Last a Long Time*, N.Y. TIMES (Apr. 1, 2020), https://www.nytimes.com/2020/04/01/business/economy/coronavirus-recession.html.

131. Samuel Woodhams, *COVID-19 Digital Rights Tracker*, TOP10VPN (Mar. 20, 2020), https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/ (last updated July 3, 2020). By September 2020, the number of countries using contact tracing apps increased to 50, and the number of countries using alternative digital tracking measures rose to 35. *Id.*

132. *See supra* Sections I and II.

exceptions should constitute no legal loophole for any unnecessary or disproportional intrusion into residents' private lives and personal data.

Many open questions remain: how can governments and private sector cooperators further encourage individuals to download consent-based digital tools at a higher rate?[133] What actions should nations take to assist particularly vulnerable and marginalized groups—such as the homeless, the poor, the elderly, and rural populations, who often lack the technological means of participating in digital governance during COVID-19 that ultimately serves to benefit individuals through information transparency?[134] How can different jurisdictions collaborate together, putting aside non-altruistic political incentives, for the greater good? In what ways can authorities keep private sector actors and themselves accountable for the deletion of private data after this public health crisis ceases?[135] How can authorities further reform privacy laws and policies beyond the immediate duration of the novel coronavirus pandemic?[136]

These call for further studies and discussion much beyond the end of the COVID-19 pandemic. While it is heartening to note many cross-disciplinary collaborations are already underway with an intense fo-

---

133. *See, e.g.*, Kai-Fu Lee (@kaifulee), TWITTER (Apr. 10, 2020, 7:46 PM), https://twitter.com/kaifulee/status/1248774479309766656?s=20 ("Opt-in contact tracing won't work. If 10% people opt-in, 50% always-on bluetooth, 40% people infected voluntarily report, then only 10%*10%*50%*40%=0.2% pairwise contacts get reported."). Lee is an AI entrepreneur and the former president of Google China. According to experts advising the United Kingdom National Health Service ("NHS"), for a contact-tracing app to help stop the coronavirus pandemic, 80% of current smartphone owners would need to use it; however, as of mid-April, only 12% of the Singaporean population downloaded TraceTogther. *See* Leo Kelion, *Coronavirus: NHS contact tracing app to target 80% of smartphone users*, BBC (Apr. 16, 2020), https://www.bbc.com/news/technology-52294896.

134. For instance, according to the Pew Research Center, in India—the second most populous country in the world comprising approximately 17.7% of the global population—only 24% of all adults report owning a smartphone. *India Population 2020 (Live)*, WORLD POPULATION REV., https://worldpopulationreview.com/countries/india-population/ (last viewed Aug. 14, 2020); Laura Silver, *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*, PEW RSCH. CTR. (Feb. 5, 2019), https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/. Meanwhile, in Latin America, "approximately 66% of the population has a smartphone and about 52% has access to mobile Internet." Cordova & Botero Arcila, *supra* note 34.

135. *See generally* Cordova & Botero Arcila, *supra* note 34 (raising five suggestions for lawmakers and policymakers, including: a data minimization policy, limitation of the amount of time the data can be stored to only cover the duration of the COVID-19 pandemic, as well as transparency with the "public and open access to the rules[ ] to allow monitoring and evaluation by the courts and civil society").

136. Some legal scholars have already been working on this matter. *See, e.g.*, Bill Proposal, Lilian Edwards et al., The Coronavirus (Safeguards) Bill 2020: Proposed Protections for Digital Interventions and in Relation to Immunity Certificates (May 6, 2020).

cus on unresolved questions posed by COVID-19,[137] it is a critical goal of this Essay to further encourage such explorations, which will affect global societies and individuals at large, as well as generations to come.

137. *See, e.g.*, Allen et al., *supra* note 9; Buckee et al., *supra* note 50.